جامعـــة بنغـــازي
كليـــة الاقتصـــاد
قسم المحاسبـــة

الرقابة في المنظومة المصرفية الموحدة

"دراسة تطبيقية علي المصارف الليبية"

إعـداد

طارق محمود يونس المزيني

بكالوريوس محاسبة، كلية الاقتصاد، جامعة عمر المختار طبرق، ربيع 2006م

إشـــراف

الدكتور: إدريـــس عبدالحميد الشريـــف

قدمت هذه الدراسة استكمالاً لمتطلبات الحصول على درجة الإجازة العليا (الماجستير)

في المحاسبة بتاريخ 2013/12/19

الفصل الدراسي خريف 2013م.

جامعة بنغـــازي
كليــة الاقتصـــاد
قســـم المحاسبة

الرقابة في المنظومة المصرفية الموحدة

"دراسة تطبيقية علي المصارف الليبية"

إعـداد

طارق محمود يونس المزيني

بكالوريوس محاسبة، كلية الاقتصاد، جامعة عمر المختار طبرق، 2006م

لجنــة الإشـراف والمنــاقشة

د. إدريـس عبدالحميد الشريف مشــرفـــــاً .....

د. فـــاخر مفتـــاح بوفرنـــه ممتحناً داخلياً .....

د. عـادل السيـد أفكيريـــــن ممتحناً خارجياً .....

اعتماد عميد الكلية .....

بسم الله الرحمن الرحيم

"يرفع الله الذين امنوا منكم والذين

أوتوا العلم درجات والله بما تعملون

خبير"

(المجادلة، من الآية 11)

أتوجه بالشكر لله عز وجل الذي أفاض علي من كرمه، فمنحني من العطايا والنعم ما مكنني من إنجاز هذا البحث.

ولا يسعني في هذا المقام إلا أن أتوجه بجزيل الشكر وفائق الاحترام والتقدير إلي أستاذي الفاضل الدكتور/ إدريس عبد الحميد الشريف، لما تكبده من عناء ومشقة في سبيل إخراج هذا البحث في صورته الحالية، ولما شملني به من رعاية وحسن توجيه وإرشاد، وما غمرني به من علم وخلق، فقد كان بحق نعم الأخ وخير معلم، ولا يسعني إلا أن أدعو له بوافر الصحة والعافية ومديد العمر، وأن يثيبه الله من خير الجزاء أحسنة ومن خير العلم أوفره ومن خير الدرجات أعلاها، وليجعله الله نبراساً للعلم، وأسال الله العلي أن يجعل ذلك في ميزان حسناته.

كما أتوجه بالشكر والتقدير إلي زميل الدراسة الأستاذ/ خالد زيدان الفضلي، لما غمرني به من عون وسعة صدر طوال إعداد هذا البحث، فقد كان نعم الأخ وخير العون، ولا أملك إلا أن أدعو له بدوام الصحة والعافية ومديد العمر، وليجعله الله مناراً للعلم.

وأخيراً، اللهم إني قد بذلت ما يسرت لي من الجهد، فإن وفقت فبفضل من عندك، وأن أخفقت فمن نفسي ومن الشيطان، فسبحان من تفرد بالكمال وحده، وما توفيقي إلا بالله العزيز الحكيم.

الباحث

الإهداء

إلى أمي وأبي:

سندي في الشدائد، من يعجز اللسان

أن يوفيهما حقهما بارك الله فيهما

وحفظهما وأنعم عليهما بمديد العمر

ودوام الصحة والعافية.

ملخص الدراســـة

علي الرغم مما تحققه نظم التشغيل الإلكتروني من مزايا متعددة في مجال تشغيل تداول البيانات المحاسبية، إلا أنها أفرزت العديد من المشاكل المتعلقة بالرقابة علي البيانات الإلكترونية، وبكيفية حماية البيانات من الدخول غير المصرح، لذا اهتمت الدراسة بالتعرف علي آليات الرقابة في المنظومة المصرفية الموحدة في المصارف الليبية، من خلال دراسة شملت خمس فصول حيث تناول الفصل الأول مقدمة الدراسة مكونه من مقدمة ومشكلة وأهداف وأهمية ومنهجية ومجتمع وعينة الدراسة، بالإضافة إلي تقسيمات الدراسة.

ثم قدمت الدراسة في الفصل الثاني مفهوم وأهداف وأهمية الرقابة في نظم المعلومات المحاسبية الإلكترونية، بالإضافة إلي المقومات والمبادئ الأساسية للرقابة في نظم المعلومات، ثم التعرف علي تصنيف رقابة نظم المعلومات ومقاييس الأمان ومراحل تطويرها، والمخاطر الرقابية والقانونية المتعلقة بها وأساليب تقييمها والعوامل المؤثرة علي فعاليتها.

أما الفصل الثالث اقتصر علي عرض الإصدارات المهنية الخاصة بالرقابة في نظم المعلومات، والدراسات التي قامت بتحديد آليات رقابة نظم المعلومات والتهديدات التي تتعرض لها مع التغير المستمر والتقدم التكنولوجي السريع.

واحتوى الفصل الرابع علي الدراسة التطبيقية من أجل اختبار الفرضية الرئيسية للدراسة، وتم استخدام قائمة استبيان (وجهاً لوجه)، وتوزيعها علي المراجعين الداخليين ومشرفي المنظومة، بالإضافة إلي الملاحظات من واقع العمل في المصارف الليبية المشاركة في الدراسة، وتمثلت نتائج الدراسة في رفض الفرضية الصفرية وقبول الفرضية البديلة لها للفرضية الرئيسية للدراسة وذلك بالنسبة للمراجعين الداخليين ومشرفي المنظومة، واختلفت نتائج الملاحظات مع نتائج المراجعين الداخليين ومشرفي المنظومة، وأظهرت عدم فعالية آليات رقابة المنظومة المصرفية الموحدة في المصارف الليبية المشاركة في الدراسة.

وأخيراً قدم الفصل الخامس توصيات الدراسة فتمثل أهمها في توعية المراجعين الداخليين ومشرفي المنظومة الموحدة في الصارف الليبية بالدور المنتظر منهم في تقييم نظم الرقابة للمنظومة الموحدة، وتحديد الأخطار التي تهددها، والمشاركة في اختيار الضوابط الرقابية الملائمة لمواجهة هذه الأخطار، وتوفير برامج تدريب مهني متخصص للمراجعين الداخليين وأخصائي تقنية المعلومات في مجال رقابة المعلومات المحاسبية الالكترونية، بهدف إعداد كوادر قادرين علي القيام بالأدوار المطلوبة منهم في مجال رقابة نظم المعلومات المحاسبية الالكترونية.

قائمــة المحتويــات
والجـــــــــداول

قائمــة المحتويـــــــات

الموضـــوع

الفصل الأول

الإطــار العام للدراســة.

الفصـل الثانــي

الرقابــة في نظم المعلومات الالكترونيــة.

الفصل الثالث

مراجعة الدراسات السابقة.

الفصل الرابع

تجميع وتحليل البيانات.

الفصـــل الخامـــس

النتائـــج والتوصيـــــات

قائمـــة المراجـــــع.

الملاحـــــــــق.

قائمـــة الجـــداول

الفصـــــــــل الأول:
الإطار العام للدراســة

1.1 مقدمـــة:

لقد ظهر مصطلح تكنولوجيا المعلومات في السبعينات، وقد دخلت هذه التقنية مختلف الأنشطة والقطاعات ومنها أعمال المحاسبة والمراجعة، ففي البداية أرتبط المراجعين فقط بالرقابة على استخدام الحاسب، وتبع ذلك إدراك المراجعين لأهمية استخدام الحاسب في القيام ببعض إجراءات المراجعة (رضي والسقا، 2005).

وأصبحت تكنولوجيا المعلومات جزءً أساسياً لإنجاز أعمال ومعاملات المؤسسات بمختلف أنواعها وأحجامها، وأصبح النظام المحاسبي بما يتضمنه من قواعد وإجراءات رقابية جزءً من نظام المعلومات الإلكتروني، واستبدل النظام المحاسبي اليدوي بنظام محاسبي ينجزه الحاسب الآلي مع المحافظة على قواعد وإجراءات الرقابة الداخلية من خلال إجراءات وبرامج عالية الدقة (رسلان والشيشنى، 2005).

وأدت التطورات السابقة إلى ظهور أساليب رقابة ومراجعة عديدة، الأمر الذي دعي إلى التساؤل حول مدى كفاءة وفعالية هيكل الرقابة الداخلية، ولاشك أن اختلاف بيئة العمل المحاسبي الإلكتروني عن بيئة العمل المحاسبي التقليدي قد أدت إلى صعوبة الإلمام بكافة مستجدات النظام المحاسبي، وأدى ذلك إلي صعوبة فهم كيفية تدفق البيانات داخل النظام، الأمر الذي تطلب ضرورة حدوث توجه نحو تطوير عملية الرقابة الداخلية (الجبالى، 2002). ومن الطبيعي أن تتأثر مهنة المحاسبة والمراجعة بالتطور التكنولوجي الذي حدث في أساليب تشغيل ومعالجة البيانات، وأن لم يؤثر بالضرورة على المبادئ الرئيسية للمحاسبة والمراجعة، ولذلك فقد أصبح على المحاسب والمراجع أن يكونا ملمين بأساليب التشغيل الإلكتروني للبيانات (طلبه، 2006).

وفي إطار توجه مصرف ليبيا المركزي نحو تفعيل الاستفادة من تطورات تكنولوجيا المعلومات، وتحسين بنية العمل المصرفي، شرع المصرف المركزي والمصارف الليبية الأخرى في تنفيذ برنامج يطمح إلى تطوير أنظمة الخدمات المصرفية بما يتوافق مع التطورات التكنولوجية، وهو ما يعرف **"بمشروع نظام المدفوعات الوطني"** وقد انبثقت من هذا النظام خمس مكونات أساسية وهى، منظومة التسوية الإجمالية الفورية Real Time (RTGS) Gross Settlement، منظومة المقاصة الالكترونية Automated Cleaning (ACH) House، منظومة معالجة الصكوك أليا Automated Checks Processing (ACP)، نظام آلات السحب الذاتي نقاط البيع وإدارة البطاقات Automatic Teller (ATM)

Machine، وأخيراً المنظومة المصرفية الموحدة أو المتكاملة Core (FLEXCUBE) Banking System[1].

وبناءً على إستراتيجية مصرف ليبيا المركزي التي تهدف إلى نشر بيئة مركزية لتقنية المعلومات تم اختيار تطبيق المنظومة المصرفية الموحدة أو المتكاملة، والتي تعتمد في الأساس على مزود لخدمات التطبيقات التي تعمل بها المنظومة، والذي يغطى العمليات المصرفية للإفراد والشركات معاً والخدمات المصرفية الالكترونية، ومن أهم ما يميز هذا النظام هو دعم تعدد الفروع أي إمكانية تنفيذ المعاملات الحالية عن طريق أي فرع دون الرجوع إلى الفرع الذي به حساب العميل ودعم الحسابات بعملات مختلفة ودعم تعدد وسائل الاتصال والدفع ومركزية قواعد البيانات الخاصة بالعملاء والحسابات. كما أدى التقدم الكبير في مجال الاتصالات والتشغيل عن بعد إلى خلق نظم متقدمة للتشغيل الإلكتروني للبيانات تعمل على تلبية احتياجات العديد من المستفيدين بكفاءة وفعالية، وقد ظهرت العديد من المشاكل المتعلقة بالرقابة على تلك النظم، وبكيفية حماية البيانات والمعلومات من الدخول غير المصرح به، وقد ترجع المخاطر الناتجة عن التشغيل الإلكتروني إلى التطورات السريعة في تكنولوجيا المعلومات والتي لم يواكبها تطور موازى في ممارسات الرقابة والتزام ووعى ومهارة ومعرفة العاملين (حسين، 2006).

ولقد تبنت العديد من الجهات المهنية مسعى رقابة البيانات والمعلومات الالكترونية، وقد بين المعيار الصادر عن (اللجنة الفنية المشتركة التي أسستها كل من المنظمة الدولية للمواصفات القياسية واللجنة الإلكترونية الفنية الدولية، International"-27000-2009) (ISO/IEC) Standards Organization and International Electronic Committee"، أن مقومات النظام الجيد لرقابة البيانات والمعلومات تتمثل في توفير مناخ أخلاقي يبعث على الأمن في المؤسسة، ويتمثل كذلك في وجود قسم منفصل لإدارة الرقابة علي المعلومات يتبع للإدارة العليا، وتأسيس مجلس المديرين ولجنة المراجعة تحرص كل هذه الأقسام على توافر نظام جيد لرقابة البيانات والمعلومات الالكترونية، والموازنة بين التكاليف اللازمة والمنافع المترتبة من تطبيق تلك الإجراءات، وتحديد الواجبات والمسؤوليات، والتوافق مع القوانين واللوائح الخاصة بالدولة.

[1]- انظر ملحق رقم (2) لمزيد من الإيضاح حول هذه المنظومات.

وقدم إرشاد (المؤسسة الدولية للمعايير والتكنولوجيا، 2008) (NIST) "National Institute of Standards and Technology" الكيفية التي يتم بها وضع خطط فعالة لرقابة المعلومات، من خلال تحديد مجموعة شاملة من الإجراءات التي يجب تنفيذها للحصول على تأكيد لفعالية الرقابة المطبقة في أنظمة المعلومات.

وهدفت دراسة (مكتب المحاسبة العام، 2003) (GAO) "General Accounting Office" بالولايات المتحدة الأمريكية لدراسة مدى قيام الإدارة المالية بتحديد المخاطر المرتبطة بالمدفوعات التي تتم عن طريق الانترنت، ومدى قيام تلك الإدارة بتوثيق وتطبيق إجراءات رقابية ملائمة لحماية تلك المدفوعات، وتوصلت الدراسة إلى إنه لم يتم تحديد المخاطر المرتبطة بنظام المدفوعات عن طريق الانترنت بصورة شاملة، ويرجع ذلك لعدم اعتقاد المسئولين في تلك الإدارة بأهمية ذلك، وكذلك الإجراءات والسياسات التي تم اتخاذها من قبل الإدارة للحد من مخاطر الرقابة التي لم تطبق بفعالية مما يؤدى إلى وجود العديد من نقاط الضعف في تلك الإجراءات.

وقدم Wayne (2002)، تقريراً يوضح سياسة رقابة المعلومات لأحد المصارف بولاية تكساس الأمريكية، حيث تناول الأهداف الرقابية التي يسعى المصرف لتحقيقها والتهديدات التي تتعرض لها المصارف، وقد أشار التقرير إلى أن سياسة رقابة المعلومات الالكترونية للمصرف تسعى لتحقق ثلاثة أهداف أساسية متمثلة في حماية وسرية بيانات العملاء، وتوثيق التهديدات المتوقعة ومحاولة تقليل احتمال حدوث هذه التهديدات إلى ادني حد، والمتابعة المستمرة للتعرف على التهديدات الجديدة التي قد تطرأ على بيئة الإعمال.

كما أوضحت دراسة Jacobs and Weiner (1997)، دور مراقبي الحسابات في تصميم خطط للتغلب على أثار الكارثة[2]، وإن التحدي أمام المراجعين يتمثل في تحديد خطة شاملة للتغلب على أثار الكارثة القابلة للتطبيق في ظل الموارد المادية المنخفضة للمؤسسات صغيرة ومتوسطة الحجم، وتوصلت الدراسة إلى إحدى عشر[3] عنصر يجب تحديدهن لتصميم خطة فعالة للتغلب على أثار الكارثة والتي تضمن تصميم خطة شاملة وفقاً لأسوأ كارثة يمكن أن تتعرض لها المؤسسة.

---

[2]- المقصود بالكارثة: هو ما تتعرض لها المؤسسات من أضرار ناتجة عن الطبيعة (مثل: الزلازل- البراكين- الفيضانات)، أو ناتجة عن الإنسان مثل الحروب.

[3]-انظر صفحة رقم (51- 52)، للتعرف الأحدى عشر عنصر التي تم تصميمها للتغلب علي آثار الكارثة.

ويعتبر المعيار الصادر عن (اللجنة الفنية المشتركة التي أسستها كل من المنظمة الدولية للمواصفات القياسية واللجنة الإلكترونية الفنية الدولية، ISO/IEC (2005-27000، الإطار الشامل في مجال رقابة المعلومات وهو يقدم توصيات حول الممارسات الجيدة في مجال إدارة رقابة المعلومات موجهة إلى الإطراف المسئولة، وأن مجال الرقابة الداخلية يحتوى على رقابة البيانات والمعلومات الالكترونية وينقسم إلى إحدى عشر مبدأ وهى:

1- سياسة الرقابة: توضح سياسة الرقابة في صورة دليل للمستويات الإدارية المختلفة.
2- الرقابة التنظيمية: توفر التوجيهات وتوضح الالتزامات والمسؤوليات الخاصة بالإفراد.
3- تصنيف الأصول ورقابتها: يحدد المسؤولية عن كل أصل وتصنيفه وفقاً للاحتياجات الرقابية لكل أصل.
4- رقابة الإفراد: إدارة حقوق الوصول للنظام وتوفير برامج الوعي والتدريب للعاملين والتحقق من الخلفية الجنائية للعاملين قبل التعيين.
5- الرقابة المادية والبيئية: حماية معدات الحاسب الهامة مادياً من الإضرار والسرقة والحرارة.
6- إدارة الاتصالات والعمليات: تحديد إجراءات رقابة للأنظمة والشبكات والمسؤوليات التشغيلية لتكنولوجيا المعلومات وإدارة خدمات التعهيد[4].
7- رقابة الوصول: مراقبة الوصول المنطقي ومنع الاستخدام غير المصرح به.
8- تطوير الأنظمة وصيانتها: تحديد المتطلبات الرقابية اليدوية و الإلية اللازمة.
9- إدارة حوادث رقابة المعلومات: تحديد نقاط الضعف وإدارة الحوادث الرقابية وإتباع إجراءات رقابية ملائمة للحد من تلك التهديدات.
10-استمرارية الإعمال: وصف العلاقة بين خطط الطوارئ واستعادة الإعمال إلى مرحلة اختبار الخطط والتنفيذ.
11- الالتزام: يوضح التزام المؤسسة بالالتزامات والمتطلبات القانونية والالتزام بالسياسات والمعايير والالتزامات التقنية والرقابية.

[4]- تتمثل خدمات التعهيد في قيام أحد المصارف بالاتفاق مع المؤسسات التي تعمل في مجال تكنولوجيا المعلومات على توريد خدمات تكنولوجية (مثل: تطوير أنظمة معلومات جديدة- الصيانة الدورية - معالجة المشاكل التي تطرأ نتيجة لاستخدام أنظمة المعلومات).

ويقدم كل مبدأ منها توصيات عامة حول الضوابط التي يمكن الاستعانة بها، وتهدف هذه التوصيات إلى توفير الثقة في التعاملات التي تتم بين المؤسسات، وان الهدف الرئيسي للمعيار هو السرية، والإتاحة، والسلامة للمعلومات الإلكترونية وذلك من خلال تطبيق تسع أهداف فرعية رقابية وهي:

1- رقابة خفض الخطأ والغش: يهدف إلي تخفيض فرص ارتكاب الخطأ والغش وزيادة فرص اكتشافها.
2- رقابة الوصول المادي: يهدف إلي حماية حجرات وأجهزة الحاسب وملحقاتها من الوصول غير المصرح به.
3- رقابة الوصول المنطقي: يهدف إلي حماية أجهزة الحاسب الآلي من الاستخدام غير المصرح به.
4- رقابة أمن البيانات: يهدف إلي حماية البيانات والمعلومات الالكترونية.
5- معايير التوثيق: تهدف إلي تطبيق الإجراءات الرقابية وفقاً لمواصفات التشغيل المعيارية.
6- خطة التغلب على آثار الكارثة: تهدف إلي التحقق من وجود خطة شاملة للتغلب علي آثار أي كارثة محتملة الحدوث.
7- الرقابة الخاصة بالانترنت والاتصالات والمصارف الإلكترونية: يهدف إلي حماية العمليات الإلكترونية.
8- رقابة أمن النتائج: تهدف إلي حماية مخرجات الحاسب الآلي من الوصول غير المصرح به.
9- رقابة خدمات التعهيد: تهدف إلي رقابة الخدمات التي يتم تعهيدها ورقابة أنشطة موفر خدمات التعهيد لضمان سرية وسلامة البيانات والمعلومات الالكترونية.

وتم التوصل إلى الأهداف التسعة الفرعية من خلال دراسة ومقارنة الممارسات المتبعة في عدد من المؤسسات العالمية التي تعد رائدة في مجال أمن المعلومات.

1.2 مشكلة الدراســة:

لقد نتج عن استخدام تكنولوجيا المعلومات ظهور العديد من الصعوبات والتحديات، وهو الأمر الذي تطلب ضرورة دراسة تلك الصعوبات ومحاولة تبويبها وعرضها في إطار علمي

متناسق، للعمل على التغلب عليها، من خلال استحداث أساليب رقابة ملائمة للبيانات والمعلومات في بيئة الأعمال الإلكترونية (الجبالي، 2002).

وضرورة السعي إلى الأخذ بتكنولوجيا المعلومات مواكبة للتطور الفني والتقني في بيئة الإعمال، إلا أن بدء التطبيق قد واجهه بعض العقبات، ومنها ضعف تواجد نظم رقابية لضمان سلامة المعلومات الالكترونية، كما يتطلب استخدام تكنولوجيا المعلومات استثمارات رأسمالية طويلة الأجل واستثمار في الموارد البشرية المؤهلة، ومن أخطر ما تواجهه أنظمة تكنولوجيا المعلومات هو اختراق النظام من خارج المؤسسة، ويتعرض نظام المعلومات للكثير من المخاطر ولكن بمراجعة النظام وتطويره واستخدام إجراءات رقابية جيده يتم القضاء على هذه المخاطر (رسلان والشيشنى، 2005).

وأكد تقرير صادر عن منظمة التعاون الاقتصادي و التنمية Organization of the Cooperation Economic and Promotion (OCEP) إلى أهمية توفير أساليب رقابة محكمة لضمان سلامة البيانات والمعلومات المستقاة من تلك النظم التكنولوجية، وعادة ما يتسبب عدم توافر إجراءات رقابية مناسبة في حدوث جرائم المعلومات (الجبالى، 2002).

وباستخدام المنظومة المصرفية الموحدة في المصارف الليبية ظهرت العديد من المشاكل منها قصور أنظمة الرقابة وعدم تفعيلها بشكل جيد ويتجلى قصور الأنظمة الرقابية للمنظومة الموحدة واضحاً في ثورة (17 فبراير)، مما استدعى الأمر التوقف عن العمل بهذه المنظومة، والرجوع إلى النظم السابقة للمصارف وكذلك حدوث تأخير في استئناف العمل لبعض فروع المصرف التي تقع في المدن التي تضررت بشكل كبير مثل فروع المصارف لمدينة سرت، وتاورغاء وذلك ناتج عن إهمال إدارات المصارف لإجراءات خطة التغلب على أثار الكارثة، بالإضافة إلى وجود قصور في إعداد وتطوير أداء المشرفين على هذه المنظومة[5].

والتهديدات التي تواجه المنظومة المصرفية الموحدة تتطلب انتباه من جانب إدارات المصارف لكي يتم إدراكها وتقليلها إلى الحد الأدنى ويتم ذلك من خلال تبنى إجراءات رقابية فعالة تحقق أهداف المصرف، ولهذا يجب إن يكون المراجع الداخلي قادر على تقييم إجراءات الرقابة للمنظومـــة الموحدة وعرض التوصيات لتقليـــل المخاطر الرقابية، فالتبني السريـع لتكنولوجيـا

[5]- مقابلة مع أ.ميلاد الساحلي، رئيس اللجنة التسييرية المؤقتة لمصرف شمال إفريقيا، في زيارة لمدينة بنغازى، 5 مارس 2012.

المعلومات لم يغير الحاجة الأساسية للرقابة الداخلية، ولكنه وسع دور الرقابة الداخلية المستندة على تكنولوجيا المعلومات (محمود، 2006).

وبرغم هذه التطورات الكبيرة في تكنولوجيا المعلومات إلا أن الباحثين لم يولوا اهتماماً موازياً بدراسة نجاح هذه النظم ومدى تحقيقها لأهدافها، والتعرف على العوامل التي تؤثر على نجاح فعالية الرقابة فإدارة تلك النظم تتأثر بالعوامل التنظيمية والبيئية والشخصية للمستخدمين، وبما أن هذه العوامل عرضه للتغيير المستمر فأن نظم الرقابة تحتاج إلى المتابعة الدائمة لمعرفة مدى نجاحها في تحقيق أهدافها (حسين، 2005).

وفى ضوء ما سبق يمكن صياغة سؤال البحث كما يلي:

س/ هل الرقابة في المنظومة المصرفية الموحدة في ليبيا فعالة[6]؟

1.3 فرضيات الدراســة:

ولغرض الإجابة على سؤال الدراسة تم صياغة الفرضية الرئيسية كالتالي:

الفرضية الرئيسية/ عدم فعالية الرقابة للمنظومة المصرفية الموحدة في ليبيا.

وسيتم قبول أو رفض الفرضية الرئيسية للدراسة وذلك من خلال قبول أو رفض الفرضيات الفرعية التسعة التالية:

الفرضية الأولى/ لا تخفض آليات الرقابة من الخطأ والغش.

الفرضية الثانية/ لا تخفض آليات الرقابة من الوصول المادي.

الفرضية الثالثة/ لا تخفض آليات الرقابة من الوصول المنطقي.

الفرضية الرابعة/ لا تحسن آليات الرقابة من أمن البيانات.

الفرضية الخامسة/ لا تحسن آليات الرقابة من تطبيق معايير التوثيق.

الفرضية السادسة/ لا تمكن آليات الرقابة من التغلب على آثار الكارثة.

---

[6]- فاعلية نظام الرقابة: تتمثل في مدى تحقيق المشروع لأهدافه وأدائه لإعماله وأنشطه بصورة جيدة، أي أن الفعالية تركز كمفهوم عن نوعية وجودة النتائج التي تتحقق من وراء استخدام الموارد بطريقة مثلى (شريهان، 2011: 24).

الفرضية السابعة/ لا تخفض آليات الرقابة من الاختراقات الأمنية في عمليات التجارة الالكترونية والاتصالات والانترنت.

الفرضية الثامنة/ لا تحسن آليات الرقابة من أمن النتائج.

الفرضية التاسعة/ لا تحسن آليات الرقابة من أمن خدمات التعهيد.

1.4 هدف الدراســة:

تهدف الدراسة إلى استكشاف واقع الرقابة في المنظومة المصرفية الموحدة في ليبيا ومعرفة فعالية الرقابة والعوامل التي تؤثر علي نجاحها وتحديد الصعوبات ونقاط الضعف والقوة في أساليب الرقابة المطبقة.

5.5 أهمية الدراســة:

تستمد الدراسة أهميتها من أهمية دور الرقابة في النظم المصرفية الإلكترونية، وكونها أول دراسة من نوعها فيتوقع أن يستفيد من نتائجها ذوي العلاقة من المهتمين سواء في القطاع المصرفي أو الأكاديمي.

1.6 منهجية الدراســة:

بما أن هدف الدراسة هو معرفة واقع الرقابة في المنظومة المصرفية الموحدة فبذلك تصنف الدراسة بأنها دراسة استكشافية من حيث الهدف، وأن البيانات التي تم تجميعها للدراسة وفرضيات الدراسة تم اختبارها إحصائياً فتصنف الدراسة بأنها دراسة كمية بناءً علي أسلوبها، والحقائق التي تسعى الدراسة لتجميعها تتسم بالوجود المادي الظاهر، والمعرفة المتعلقة بها مستقلة عن الإفراد فان الدراسة تقع إلى حد كبير ضمن الـ (Paradigm Functionalist) أي النموذج الوظيفي، وبناءً عليه ستكون المنهجية المتبعة في الدراسة (Nomothetic Methodology) أي المنهجية الطبيعية.

ولجمع البيانات اللازمة للدراسة تم الاعتماد على الاستبيان والملاحظات كأداتين رئيسيتين في الدراسة، وتم تحليل البيانات باستخدام الاختبارات الإحصائية الآتية:

- اختبار الصدق والثبات (Reliability Analysis) للتأكد من مدي صدق وموثوقية الإجابات وثباتها.

- الإحصاء الوصفي (Descriptive Analysis) لاحتساب تكرارات العدد ونسبة الأسئلة المتعلقة بقائمة أسئلة الاستبيان والملاحظات وذلك بهدف وصف بعض خصائص عينة الدراسة ومعالمها.
- اختبار الفرضيات الفرعية للدراسة باستخدام اختبار (One Sample T- Test (T، عند مستوى الثقة 95%.

1.7 مجتمع وعينة الدراسة:

يتمثل مجتمع الدراسة في المصارف الليبية التي تطبق المنظومة المصرفية الموحدة من مختلف المصارف في البيئة الليبية، وقد شملت الدراسة مصرف شمال إفريقيا ومصرف الوحدة ومصرف الجمهورية، وقد تم استبعاد المصارف التي رفضت إجراء هذه الدراسة باعتبار إن هذه الدراسة تمثل تهديداً لأنظمة الرقابة الخاصة بها، مثل بعض فروع مصرف الوحدة والجمهورية، والمصارف التي أوقفت العمل بالمنظومة المصرفية الموحدة مثل مصرف التجاري الوطني، وكذلك المصارف التي لم تعمل بهذه المنظومة، مثل مصرف الصحاري ومصرف التجارة والتنمية ومصرف الأمان ومصرف الإجماع العربي.

ولاختبار فرضيات الدراسة تم استخدام عينة من الإطراف التي تهتم بمشكلة الدراسة وهم **المجموعة الأولى** مكونة من المراجعين الداخليين، **والمجموعة الثانية** مكونة من مشرفين المنظومة، نظراً لعلاقتهما المباشرة بموضوع الدراسة.

1.8. تقسيمات الدراســة:

تم تقسيم الدراسة إلي خمس فصول كالأتي:

الفصل الأول: الإطار العام للدراسة.

الفصل الثاني: الرقابة في نظم المعلومات الالكترونية.

الفصل الثالث: مراجعة الدراسات السابقة.

الفصل الرابع: تجميع وتحليل البيانات.

الفصل الخامس: النتائج و التوصيات.

الفصـــل الثانـــــي:
الرقابـة في نظـم المعلومات الالكترونيـــة

2.1 مقدمـــة:

أدى التطور السريع في استخدام أساليب تكنولوجيا المعلومات إلي زيادة إمكانية التلاعب في نظم المعلومات الالكترونية دون ترك أي أثر، علاوة علي صعوبة اكتشافها في ظل عدم وجود مستندات خاصة بها، مما أدي إلي ضرورة الاهتمام بنظم الرقابة علي البيانات والمعلومات في ظل بيئة تكنولوجيا المعلومات نظراً لتزايد المخاطر التي تهدد أمن وسلامة نظام المعلومات (كامل وشحاتة، 2008).

ويستعرض هذا الفصل رقابة المعلومات في بيئة تكنولوجيا المعلومات من حيث مفهومها، ومقوماتها، وأهميتها، وأهدافها، والإجراءات الرقابية اللازمة لحماية نظم المعلومات الالكترونية.

2.2 مفهوم وأهداف الرقابة في نظم المعلومات الإلكترونية:

تشكل رقابة نظم المعلومات الالكترونية علي مستوى العالم هاجساً وقلقاً بالنسبة للقائمين علي إدارة الأنظمة المعلوماتية المختلفة، لاسيما في ظل تنامي عمليات الجرائم المعلوماتية في ظل تطور التقنية وانتشار المخاطر التي تكتنف استخدامها وتطبيقاتها المختلفة، وسنتناول بعض مفاهيم الرقابة في نظم المعلومات الالكترونية وأهدافها.

2.2.1 مفهوم الرقابة في نظم المعلومات الإلكترونية:

اهتم العديد من البحُاث والجهات المهنية في مجال الرقابة علي المعلومات الإلكترونية بتحديد ماهية نظم رقابة المعلومات، وفيما يلي بعض التعريفات الخاصة بنظم وآليات رقابة المعلومات الالكترونية.

عرف الإصدار الأخير للمعيار الدولي (ISO- IEC 27000- 2009: 4)، رقابة المعلومات بأنها *"نظم إدارة أمن نظم المعلومات هي جزء من نظم الإدارة تستند علي مدخل خطر الإعمال لوضع وتطبيق وتشغيل ومتابعة وفحص وتحسين رقابة وأمن المعلومات"* .

وعرف (نصر والسيد، 2008: 222)، رقابة المعلومات بأنها *"مجموعة من الإجراءات والأساليب التي تهدف إلي تحقيق الحماية للنظام من أي أحداث مستقبلية تهدد النظام وتؤدي إلي فقد المعلومات أو عدم دقتها أو فقد سريتها"* .

وقد عرف المعهد الدولي للمعايير والتكنولوجيا (National Institute of Standard Technology ، 2008: 4)، رقابة المعلومات بأنها *"أجراء الوقاية أو الإجراءات المضادة التقنية والتشغيلية والإدارية التي تهدف إلي حماية سرية وإتاحة النظام والمعلومات"*.

وعرف (الشريف، 2006: 175)، رقابة المعلومات بأنها *"عملية جمع وتقييم الأدلة لتحديد ما إذا كان استخدام تكنولوجيا المعلومات تساهم في حماية أصول المؤسسة، ويؤكد سلامة بياناتها، ويحقق أهدافها بفعالية، ويستخدم مواردها بكفاءة"*.

وكما عرف (حسين والسيد، 2003: 21)، رقابة المعلومات بأنها *"عملية منظمة لجمع وتقييم موضوعي للأدلة الخاصة بمزاعم الإدارة بشأن الإحداث والتصرفات الاقتصادية للمشروع لتحديد مدى تمشى هذه النتائج مع المعايير القائمة وتوصيل النتائج إلي مستخدميها المعنيين بها"*.

يتضح من التعريفات السابقة إن الهدف الأساسي من رقابة البيانات والمعلومات الالكترونية هو تحقيق السرية والسلامة وتوافر المعلومات بالإضافة إلي توفير إجراءات تضمن استعادة البيانات والمعلومات بسرعة في حالة حدوث أي كارثة تؤدي إلي فقد أو تلف البيانات مما يتيح استعادة الإعمال بسرعة.

ويتضمن مفهوم رقابة أمن وسلامة المعلومات كافة الإبعاد المتعلقة بالحفاظ علي السرية Confidentiality، والسلامة Integrity، والإتاحة Availability، وإمكانية المراجعة Audibility، والتوثيق Authenticity.

كما يقول (نصر والسيد، 2003: 222) أن اعتبارات أمن وسلامة المعلومات تتمثل في العناصر التالية:

1- **سرية المعلومات Confidentiality:** تعني عدم إتاحة المعلومات أو اطلاع الإطراف غير المصرح لها علي تلك المعلومات، أو عدم حصول الإطراف غير المصرح لهم عليها.
2- **سلامة المعلومات Integrity:** وتعني أن المعلومات لم يتم إجراء تغيير بها أو تدميرها أو تحريفها، ويعني ذلك ضمان أن تكون المعلومات دقيقة وصحيحة ومكتملة أثناء تخزينها وأثناء نقلها، وان يتم تشغيلها بطريقة صحيحة.

3- **الإتاحة Availability:** تعني إمكانية الوصول إلي المعلومات وتوفرها واستخدامها عند طلبها في الوقت الملائم من جانب المستخدمين المصرح لهم، أو ضمان أن تكون المعلومات متاحة للأطراف المصرح لها في الوقت المناسب والمكان المناسب.
4- **إمكانية المراجعة Audibility:** تعني القيام بفحص معين يضمن أن أفعال وعمليات وتصرفات مؤسسة معينة يمكن ردها إلي تلك المؤسسة فقط.
5- **التوثيق Authenticity:** وتعني التحقق من سلامة هوية الشخص أو الجهة التي يتم التعامل معها، والتأكد من أنه طرف مصرح له بالدخول إلي موقع أو نظام معلومات المؤسسة والاطلاع علي معلومات المؤسسة.

2.2.2 أهداف الرقابة في نظم المعلومات الالكترونية:

إن الأهداف الأساسية لأساليب وإجراءات الرقابة هي التحقق من سلامة تنفيذ سياسات وإجراءات المؤسسة التشغيلية، وإن هذه الإجراءات ملائمة وكافية لتحقيق فعالية التشغيل وشمولية معالجة البيانات، ولكي تكون إستراتيجية رقابة المعلومات ناجحة وفعالة وقابلة للتطبيق لا بد أن يشارك في إعدادها وتنفيذها جميع المستويات الوظيفية التي لها علاقة بتلك الإستراتيجية بحيث تسعي هذه المستويات إلي إنجاح تلك الإستراتيجية من خلال تحقيق أهداف إستراتيجية رقابة المعلومات تتمثل في الأتي (الشريف، 2006):

1- تعريف مستخدمي تكنولوجيا المعلومات ومختلف الإداريين بالتزاماتهم وواجباتهم المطلوبة لحماية نظم المعلومات الإلكترونية بكافة إشكالها وفي مختلف مراحل جمعها وإدخالها ونقلها عبر الشبكات وإعادة استرجاعها عند الحاجة.
2- تحديد وضبط الإجراءات التي يتم من خلالها تحقيق وتنفيذ الواجبات المحددة لكل من له علاقة بنظم المعلومات وتحديد المسؤوليات عند حصول الخطر.
3- بيان الإجراءات المتبعة لتفادي التهديدات والمخاطر وكيفية التعامل معها عند حصولها والجهات المكلفة بالقيام بذلك.

2.3 أهمية الرقابة في نظم المعلومات الإلكترونية:

تعمل معظم المؤسسات في الوقت الحاضر علي استخدام تكنولوجيا المعلومات (IT) "Information Technology" المعتمدة علي الحاسبات الالكترونية في تشغيل بياناتها وتوصيلها إلي مستخدميها في الوقت المناسب، وقد أدى ذلك إلي تزايد أهمية أمن وسلامة

المعلومات الإلكترونية، وأن المتطلبات الأساسية التي يجب توافرها في أنظمة تكنولوجيا المعلومات كما تناولها (كامل والسيد، 2008)، تتمثل في العناصر الثلاث التالية:

1- تكامل المعلومات Information Integration: بمعني تبادل الخدمات والمعلومات بين العديد من أنظمة المعلومات.
2- تبادل المعلومات بين العديد من أنظمة المعلومات في الوقت المناسب Timeliness of Information Exchange .
3- خلق عدد كبير من مستخدمي النظام في العالم من عملاء وموردين Creating Global Communities Of Users.

ومن ناحية أخري فأن استخدام أدوات تكنولوجيا المعلومات في تشغيل نظام المعلومات المحاسبي أدي إلي ضرورة الاهتمام بالرقابة علي أمن وسلامة المعلومات وذلك لعدم وجود سجلات مادية، مما أدي إلي أمكانية حدوث أي تلاعب في البيانات دون ترك أي أثر، وكذلك صعوبة اكتشافها مما يتطلب ضرورة وجود نظام جيد وفعال للرقابة الداخلية يعمل على تحقيق أمن وسلامة المعلومات في ظل بيئة تكنولوجيا المعلومات المعتمدة علي استخدام الحاسبات الآلية (نصر والسيد، 2003)، وكما أشار (صندوق النقد العربي، 1994)، بأن رقابة نظم المعلومات الإلكترونية لها أهمية كبيرة وتحقق فوائد عديدة منها ما يلي:

1- كشف المخالفات والنواقص في وقت مبكر.
2- مرجع إرشادي لعمليات المصرف.
3- تقليل التكلفة.
4- تقليل الخسائر.
5- تقليل إعمال المراجعة وكذلك الوقت الضائع.
6- تحسين نوعية التقارير المالية.

2.4 المبادئ الأساسية للرقابة في نظم المعلومات الإلكترونية:

قدم الإرشاد الدولي الأول لتكنولوجيا المعلومات (IFAC, 1998)، التابع للاتحاد الدولي للمحاسبين ثمانية مبادئ أساسية لرقابة المعلومات الإلكترونية هي: المساءلة، الوعي، تعدد المجالات، فعالية التكلفة، التكامل، إعادة التقييم، التوقيت الملائم، والعوامل المجتمعية. وفيما يلي توضيح لكل مبدأ من تلك المبادئ.

1- **المساءلة Accountability:** يشير هذا المبدأ إلي ضرورة تحديد المسؤوليات الخاصة برقابة المعلومات بصورة صريحة وموثقة.

2- **الوعي Awareness:** يشير هذا المبدأ إلي ضرورة الوعي بتهديدات أمن المعلومات، والإجراءات التي تم وضعها لمواجهة تلك التهديدات من الإطراف ذات المصلحة بالمعلومات الخاصة بالمؤسسة.

3- **تعدد المجالات Multidisciplinary:** يشير هذا المبدأ إلي ضرورة التعامل مع رقابة المعلومات عن طريق الاهتمام بكل من الموضوعات التكنولوجية وغير التكنولوجية، فلا يجب أن يقتصر فقط على الموضوعات التكنولوجية ولكن يجب أن يغطي الموضوعات الإدارية والتنظيمية والتشغيلية والقانونية.

4- **فعالية التكلفة Cost Effectiveness:** يشير هذا المبدأ إلي ضرورة مراعاة اعتبارات المنفعة والتكلفة عند السعي إلي تحقيق رقابة المعلومات، ولتحقيق ذلك يجب الأخذ في الاعتبار درجة اعتماد المؤسسة على المعلومات، وقيمة البيانات والمعلومات في حد ذاتها، بالإضافة إلي أهمية التهديدات التي تتعرض لها المعلومات واحتمال تحققها.

5- **التكامل Integration:** يشير هذا المبدأ إلي ضرورة تحقيق التكامل بين السياسات وإجراءات رقابة المعلومات الخاصة بالمؤسسة من جهة، وكل السياسات والإجراءات الأخرى الخاصة بالمؤسسة ذاتها، والسياسات والإجراءات الخاصة بالمؤسسات المتعامل معها من جهة أخري، وذلك لبناء نظام متناسق لرقابة المعلومات.

6- **إعادة التقييم Reassessment:** يشير هذا المبدأ إلي ضرورة مراجعة وتقييم نظم الرقابة بصورة دورية، وذلك نتيجة للتغيرات المستمرة في تكنولوجيا المعلومات وبالتالي ظهور تهديدات جديدة تحتاج إلي إجراءات رقابية متطورة.

7- **التوقيت الملائم Timeliness:** يشير هذا المبدأ إلي ضرورة وضع الإجراءات التي تضمن القدرة علي متابعة الحوادث والتهديدات الفعلية والمحتملة، والاستجابة لها في الوقت المناسب.

8- **العوامل المجتمعية Societal Factors:** يشير هذا المبدأ إلي ضرورة التأكيد علي أهمية الأخلاق، واحترام الآخرين ومصالحهم عند استخدام المعلومات الخاصة بهم، أو عند عرض معلومات تهمهم.

2.5 مقومات النظام الجيد للرقابة في نظم المعلومات الإلكترونية:

ظهرت الحاجة لوجود نظام جيد لحماية البيانات والمعلومات الإلكترونية، نتيجة لكبر حجم المؤسسات وانتشار فروعها، بالإضافة إلي أن نجاح المؤسسة يعتمد بصورة كبيرة علي درجة حمايتها لأنظمة المعلومات الخاصة بها، وأصبح مبدأ توافر مقومات رقابة المعلومات من المبادئ الأساسية في تصميم النظم، حتى يخرج ذلك النظام محكم الحلقات، يحوي في داخله عناصر الضبط والرقابة التي تكفل له أسباب النجاح في تحقيق أهدافه، وقد تناول المعيار الدولي (ISO-IEC 27000 2009: 11)، وكذلك (صندوق النقد العربي، 1994: 9)، تلك المقومات المتمثلة في الأتي:

1- **دعم الإدارة:** لابد من توفير مناخ أخلاقي يبعث علي الأمن في المؤسسة ويمكن تحقيق ذلك من خلال زيادة وعي العاملين برقابة المعلومات ومتابعة تنفيذ الإجراءات الرقابية وتوفير قنوات اتصال جيدة بالعاملين، وتوفير الدعم والالتزام من كافة المستويات الإدارية وبصفة خاصة الإدارة العليا.
2- **هيكل المؤسسة:** المقصود به وجود قسم منفصل لرقابة نظم المعلومات يتبع مباشرة الإدارة العليا، مع التوضيح الجيد لسلطات ومسؤوليات هذا القسم حيث يعمل هذا القسم علي إدارة رقابة المعلومات تحديد المتطلبات الرقابية اللازمة توفيرها لحماية أصول المعلومات أدارة الحوادث الأمنية وتوفير مدخل فعال لإدارة استمرار الإعمال.
3- **لجنة المراجعة:** لابد أن تحرص لجنة المراجعة علي توافر المعرفة والخبرة اللازمة لدي كل من المراجع الداخلي والمراجع الخارجي، حيث يقوم المراجع الداخلي بإعداد تقارير دورية للجنة المراجعة عن نظام رقابة نظم المعلومات، بينما يتم استشارة المراجع الخارجي لتقييم أداء مدير أمن المعلومات وتقييم الإجراءات الرقابية المطبقة.
4- **إدارة أنشطة الرقابة:** من المهم وضع إجراءات رقابية ترتبط مباشرة باستخدام الموارد المرتبطة بالحاسب الآلي وأمن المعلومات مع الأخذ في الاعتبار الموازنة بين التكاليف اللازمة لتطبيق تلك الإجراءات والمنافع المترتبة عليها.
5- **المراجعة الداخلية:** يجب أن يقوم المراجع الداخلي بمراجعة الإجراءات الرقابية المطبقة بصورة دورية وذلك لإجراء التعديلات اللازمة لمقابلة الاحتياجات المتغيرة.

2.6 تصنيف الرقابة في نظم المعلومات الالكترونية:

تشير الرقابة في نظم المعلومات إلي طريقة اكتشاف أو منع أو تقليل الخسائر المرتبطة بتهديدات نظم المعلومات ويمكن تصنيف هذه الآليات بعدة طرق كما يلي:

2.6.1 رقابة نظم المعلومات علي أساس الهدف:

يمكن تصنيف رقابة نظم المعلومات من حيث الهدف إلي تسع مجموعات بحيث تحتوي كل مجموعة علي عدد من الآليات التي تحقق نفس الهدف (ISO- IEC 27000 2005) كما يلي:

1- **رقابة خفض الخطأ والغش:** تهدف إلي تخفيض فرص ارتكاب الغش وزيادة فرص اكتشاف الغش عن طريق استخدام مجموعة من الآليات الملائمة مثل فصل الواجبات، والتدوير الوظيفي.
2- **رقابة الوصول المادي:** تهدف إلي حماية حجرات وأجهزة وتجهيزات الحاسب الآلي من الوصول غير المصرح به وتتمثل في تزويد حجرات الحاسب الآلي بأقفال وكاميرات مراقبة وأجهزة إنذار وتوفير سجل لتسجيل كافة الزيارات لحجرات الحاسب الآلي وأسباب تلك الزيارات.
3- **رقابة الوصول المنطقي:** تهدف إلي حماية الحاسب الآلي من الاستخدام غير المصرح به من خلال تزويد كل جهاز بكلمات مرور يصعب التنبؤ بها مع مراعاة تغييرها بصورة دورية، وفرض رقابة محكمة علي تشغيل الحاسب بنظام اقتسام الوقت وذلك من خلال الإغلاق اليدوي أو من خلال الإغلاق الآلي للملفات والسجلات.
4- **رقابة أمن البيانات:** تهدف إلي حماية البيانات والمعلومات سواء كانت علي أجهزة الحاسب الآلي أو محفوظة في صورة رقمية أو في صورة ورقية، بالإضافة إلي توفير آليات لحماية البيانات من المحو أو التعديل سواء بشكل متعمد أو غير متعمد، واستخدام البرامج المضادة للفيروسات والتي تعمل علي منع دخول الفيروسات.
5- **معايير التوثيق:** تهتم الرقابة علي معايير التوثيق ببناء نظام يتضمن الإجراءات الرقابية الملائمة لبيئة النظام وتطبيقاته، ويعمل وفقاً لمواصفات التشغيل المعيارية ويمكن اختباره ومراجعته بسهولة، وتوثيق البرامج وتعليمات التشغيل اللازمة لمساعدة مشغلي الحاسب علي القيام بعمليات التشغيل، وتوثيق الإجراءات اللازمة لمناولة وتخزين البيانات والمعلومات.

6- **خطة التغلب علي آثار الكارثة:** تهدف إلي التحقق من مدى وجود خطة للتغلب علي آثار الكارثة تتضمن كل التطبيقات والبرامج والأجهزة الضرورية للحفاظ علي تشغيل المؤسسة في الحالات الطارئة ومسؤولية كل فرد في عملية التغطية بالإضافة إلي تحديد الوقت اللازم لاستعادة الأعمال عند المستوى الطبيعي لها.
7- **رقابة عمليات التجارة الالكترونية والاتصالات والانترنت:** تهدف إلي حماية العمليات التي تتم بصورة إلكترونية والاتصالات الإلكترونية وخدمات الانترنت وتتضمن تلك الآليات برامج مقاومة الفيروسات التي تحمي رسائل البريد الالكتروني وبرامج الجداران النارية لحماية الاتصالات وتوفير حد للصفقات النقدية الإلكترونية في اليوم الواحد.
8- **رقابة أمن النتائج:** تهدف إلي حماية مخرجات الحاسب الآلي من الوصول غير المصرح به، وتتضمن هذه الآليات قائمة فحص التوزيعات لضمان توزيع المخرجات علي الأشخاص المصرح لهم بذلك، وجداول التوزيع للتأكد مما إذا كانت كافة التقارير والمستندات قد تم تسليمها في التوقيت المحدد لها.
9- **رقابة أمن خدمات التعهيد:** تهدف إلي حماية نظم المعلومات من المؤسسة المتعهد معها في توفير خدمات النظم الإلكترونية وتتضمن هذه الآليات تحديد واضح لمسؤوليات والتزامات كلا الطرفين التي تتعلق بالأمن في تعاقدات خدمات التعهيد، وتوثيق متطلبات الأمن المستهدفة من قبل المؤسسة والتي يجب أن يلتزم بها موفر خدمات التعهيد.

2.6.2 رقابة نظم المعلومات علي أساس ارتباطها بمراحل تشغيل البيانات:

تصنف رقابة نظم المعلومات من حيث ارتباطها بمراحل تشغيل البيانات إلي رقابة المدخلات، رقابة التشغيل، رقابة المخرجات، ورقابة التخزين (الفرطاس، 2006; الشريف، 2006)، وهي كما يلي:

1- **رقابة المدخلات:** تهدف إلي رقابة العمليات التي يتم إدخالها إلي النظام للتأكد من حصولها علي التصريحات الملائمة لها.
2- **رقابة التشغيل:** تهدف إلي ضمان صلاحية ودقة العمليات التي يتم إدخالها وتشغيلها.
3- **رقابة المخرجات:** تهدف إلي ضمان عدم وجود نسخ غير مصرح بها من المخرجات وأن المعلومات التي يتم طباعتها توجه إلي الأشخاص المصرح لهم فقط وبصورة مباشرة.
4- **رقابة التخزين:** تهدف إلي حماية سرية وسلامة البيانات والبرامج المخزنة من الوصول إليها أو التلاعب بها أو الإفصاح غير المصرح به.

2.6.3 رقابة نظم المعلومات علي أساس الغرض:

تصنف رقابة نظم المعلومات علي أساس الغرض إلي الرقابة المانعة، والرقابة الكاشفة، والرقابة التصحيحية (صندوق النقد العربي، 1994)، وهي كما يلي:

1- **الرقابة المانعة:** تهدف إلي منع حدوث الأخطاء والتلاعب قبل حدوثها.
2- **الرقابة الكاشفة:** تهدف إلي اكتشاف الأخطاء والتلاعب بعد حدوثها.
3- **الرقابة التصحيحية:** تهدف إلي تصحيح الأخطاء والتلاعب بعد حدوثها.

2.6.4 رقابة نظم المعلومات علي أساس المجال:

تصنف رقابة نظم المعلومات علي أساس المجال إلي الرقابة العامة، والرقابة التطبيقية (الفرطاس،2007)، وهي كما يلي:

1- **الرقابة العامة:** وهي مجموعة من السياسات والممارسات والإجراءات التي يجب توافرها بصفة عامة وهي إجراءات ذات تأثير عام، وهي تهدف إلي منع واكتشاف الأخطاء والتلاعب، وهي تنقسم إلي أربعة أنواع أساسية رقابة تشغيل مركز البيانات، رقابة امتلاك برامج وصيانة النظام، رقابة أمن الوصول، رقابة تطوير وصيانة تطبيقات النظام.
2- **الرقابة التطبيقية:** وهي مجموعة السياسات والممارسات والإجراءات التي ترتبط باستخدام الحاسب الآلي في مجال تطبيق معين، وتنقسم إلي ثلاثة أنواع أساسية هي: الرقابة علي المدخلات، الرقابة علي التشغيل، الرقابة علي المخرجات.

2.6.5 رقابة نظم المعلومات من حيث هيراركية[7] الرقابة:

تصنف رقابة نظم المعلومات من حيت هيراراكية الرقابة إلي الرقابة الإجرائية، والرقابة المحاسبية (حسين عبيد وشحاتة السيد، 2007: 28)، وهي كما يلي:

1- **الرقابة الإجرائية:** هي إجراءات وأساليب رقابة نظم المعلومات الالكترونية وهي تشمل:

أ- خطة التنظيم.

ب- أساليب وإجراءات الكفاءة التشغيلية.

[7]- هيراركية: هي كلمة من أصل يوناني وتعني تفاوت المراتب والأدوار أو التدرج الوظيفي.

جـ- الالتزام بالسياسات والأساليب والإجراءات الإدارية.

2- **الرقابة المحاسبية:** وهي الإجراءات والأساليب الرقابية المحاسبية لنظم المعلومات الإلكترونية وهي تشمل:

أ- خطة التنظيم .

ب- أساليب وإجراءات حماية الأصول.

جـ- دقة وإمكانية الاعتماد علي طرق وإجراءات البيانات المحاسبية.

د- الخصائص الأساسية وتشمل:

كفاءة العاملين، الفصل بين المهام، تنفيذ العمليات كما تم اعتمادها، التسجيل الصحيح للعمليات، مراقبة حيازة الأصول، المقارنة الدورية بين الأصل وسجل الأصل.

2.7 مقاييس الأمان في نظم المعلومات الالكترونية:

يتوقف اعتماد البيانات التي يقدمها نظام التشغيل، علي مدى فعالية إجراءات الرقابة علي أمن ذلك النظام، فضعف الرقابة علي أمن النظام يؤدي إلي التشغيل غير المصرح به للعمليات، وعدم دقة تقارير وسجلات البيانات، وفقد الأصول والبيانات الهامة، وانتهاك سرية البيانات، تشمل مقاييس الأمان علي الإجراءات الآتية:

2.7.1 المقاييس التي تهدف إلي حماية الأجهزة الخاصة بالحاسب (الأصول المادية):

إن معظم هذه المقاييس تقوم أساساً علي وضع إجراءات لضمان وصول المخولين فقط لأماكن الحاسبات من خلال وضع مجموعة من الإجراءات تصمم لتوفير الحماية المادية للحاسب، ووضع الحاسب في مكان يبعد عن مستوى طفح المياه، ووجوده في مكان يمكن التحكم فيه من حيث درجة الحرارة والرطوبة اللازمة أو المناسبة للحاسب عن طريق استخدام أجهزة التكييف المناسبة، وأن تكون نقاط العبور للحاسبات مراقبة من موظفي الحماية والحراسة، من خلال أجهزة إنذار، أو كاميرات الرقابة.

وتزداد أهمية إجراءات الأمن المادية في حالات الاتصال عن بعد، والتي يتم فيها الإدخال والمعالجة في مكان والاسترجاع في مكان أخر، لذلك وجب وضع إجراءات أمنية يعتمد عليها

للحفاظ علي أمن المعلومات والمعدات من خلال منع الأشخاص غير المخول لهم بالتعامل مع هذه الأجهزة، والحد من استخدام الأجهزة إلا في الأنشطة المخول بها، وفي ألأوقات المسموح بها.

2.7.2 المقاييس التي تهدف إلي حماية البرامج والبيانات:

تهتم مقاييس الأمان بحفظ سرية البيانات، وعدم تعرضها للتلاعب أو التغيير من قبل الأشخاص غير المصرح لهم، وأن البيانات بنظام الحاسب الآلي تعني الملفات المرتبطة بالحاسب الآلي أو الموجودة بمكتبة الملفات، أو البيانات المخزنة في قاعدة البيانات المرتبطة بالحاسب، كما إن البيانات تشمل البرامج التطبيقية المرتبطة بالحاسب الآلي (الفرطاس، 2006)، وتقدم مقاييس الأمان للبيانات أساليب الحماية الآتية:

2.7.2.1 الحماية ضد حصول الأشخاص غير المصرح لهم علي البيانات:

إن الحد من الحصول علي البيانات إلا للأشخاص المصرح لهم من الأمور المهمة، بالإضافة إلي عدم تعرض البيانات للتغيير المتعمد يحقق الحد من الحصول علي بيانات، وهناك عدة وسائل لتحقيق هذه الحماية من أهمها:

1- **عزل البيانات:** يجب عزل البيانات والملفات والبرامج التي تحتوي علي بيانات مهمة وحفظها في مكتبة البيانات دون التصريح لغير المختصين بالحصول عليها، ووضع حدود فاصلة بحيث لا يستطيع الموظف المختص التعامل إلا مع البيانات التي يصرح له التعامل معها فقط.
2- **التعرف علي الأشخاص المصرح لهم:** يجب تحديد الموظفين الذين يسمح لهم باستخدام البيانات أو إدخال التعديلات عليها، ويمكن وضع قائمة تظهر الأشخاص المصرح لهم بالتعامل مع البيانات بالحاسب، ونطاق هذا التصريح، وزمن تحديد الأشخاص المصرح لهم بالتعامل مع البيانات، والأرقام السرية، والكروت الممغنطة.

2.7.2.2 الحماية ضد فقد أو تعديل البيانات:

هناك العديد من الوسائل لحماية البيانات من الفقد أو التعديل، فهناك سجل العمليات الذي يقوم بحصر كافة العمليات التي تم تشغيلها في نظام الحاسب، ويحتوي هذا السجل علي كافة البيانات التي تم إدخالها، واختبارها، كما يستخدم كأداة لتحديد مسار المراجعة في نظام التشغيل المباشر لبيانات خاصة في حالة عدم وجود مستندات أولية للبيانات.

2.7.2.3 استعادة البيانات:

قد يحدث لسبب أو لأخر الخطأ في التشغيل أو عطل مفاجئ في الأجهزة، أو تلف في وحدات التخزين، أو فقد البيانات، لابد في هذه الحالة إيجاد وسيلة لاستعادة هذه البيانات فوراً، لذلك يجب دائماً الاحتفاظ بنسخة احتياطية من ملفات البيانات، والبرامج، والوثائق الموجودة في الحاسب، وهناك مدخل أخر يساعد علي استعادة البيانات بسرعة أكبر، وهو عدم الانتظار حتى تنتهي عملية التشغيل كلية، بل يمكن أثناء التشغيل حفظ النتائج، ونقلها إلي الملف الاحتياطي علي وحدة تخزين ثانوية أخري، وبذلك إذا حدث فقد للبيانات (مثل: انقطاع التيار الكهربائي)، فيكون المطلوب هو استعادة نتائج عن الفترة من أخر حفظ حتى لحظة فقد البيانات بدلاً من الحاجة إلي إعادة التشغيل كلية من البداية.

2.8 مراحل تطوير الرقابة في نظم المعلومات الإلكترونية:

قدم الإرشاد الدولي الأول لتكنولوجيا المعلومات (IFAC, 1998)، التابع للاتحاد الدولي للمحاسبين ست خطوات لتطوير نظام متكامل لرقابة نظم المعلومات علي النحو التالي:

1- **تطوير السياسة Policy Development:** تهدف إلي تطوير الإجراءات الرقابية قي إدارة أمن المعلومات، ويجب أن تدعم وتكمل السياسة الرقابية السياسات التنظيمية، ويجب أن تصف هذه السياسة أهمية رقابة المعلومات في المؤسسة ولمسؤولياتها مع الأخذ في الاعتبار الفصل الجيد للواجبات والالتزام بمعايير تصنيف الأصول، وأمن البيانات، وأمن العاملين، والأمن المادي، والبيئي والمنطقي، والمتطلبات التشريعية والتنظيمية.
2- **المهام والمسؤوليات Roles and Responsibilities:** يهدف إلي تحديد المهام والمسئوليات، والسلطات الفردية، وتوصيلها إلي جميع العاملين بالمؤسسة، وضمان فهمها لها، حيث تكون الإدارة مسئولة بشكل عام عن تحقيق أمن المعلومات، بينما أخصائيين أمن المعلومات مسئولين عن تصميم، وتطبيق، وإدارة، وفحص سياسة أمن المعلومات، وإجراءات الرقابة، وتتمثل مسؤولية مراجعي أنظمة المعلومات في توفير تأكيد معقول للإدارة عن مدي ملائمة الأهداف الرقابية ومدى توافق السياسة الأمنية والمعايير الرقابية والممارسات مع الأهداف الأمنية للمؤسسة.
3- **التصميم Design:** يتمثل في تطوير إطار الرقابة والذي يتكون من المعايير، والممارسات، والإجراءات اللازمة لإدارة أمن المعلومات، ولتحقيق ذلك لابد من الأخذ في الاعتبار متطلبات الإعمال ومخاطر الإعمال والمخاطر التقنية وتحليل الأهداف

الرقابية والمعايير والتقنيات اللازمة لتوفير إطار متكامل للرقابة يتوافق مع احتياجات المؤسسة ويراعي اعتبارات التكلفة والمنفعة.

4- **التطبيق Implementation:** يتم تطبيق إطار الرقابة في الوقت الملائم والحفاظ عليه.

5- **المتابعة Monitoring:** تهدف إلي وضع مقاييس لمتابعة الحوادث الأمنية، والكشف عنها بسرعة، وضمان تصحيحها، وذلك لضمان الالتزام المستمر بسياسة الرقابية ومعاييرها.

6- **الوعي والتدريب والتعليم Awareness Training and Education:** يهدف إلي نشر الوعي بأهمية رقابة المعلومات، وبكيفية تشغيل أنظمة المعلومات بطريقة آمنة.

2.9 مخاطر الرقابة في نظم المعلومات الإلكترونية:

"يعتبر موضوع رقابة البيانات من الأمور الواجب الاهتمام بها في كافة مراحل إعداد نظم المعلومات وأن رقابة البيانات والمعلومات أصبحت من أهم عناصر الرقابة الواجب تطبيقها علي المعلومات من خلال التخطيط المستمر خلال دورة حياة نظم المعلومات المستخدمة، وتعتبر المخاطر المقصودة اشد خطراً علي أداء فعالية النظم وتزداد تلك الخطورة في النظم الإلكترونية، وتكمن خطورة مشاكل رقابة المعلومات في عدة جوانب منها تقليل أداء الأنظمة الإلكترونية أو تخريبها بالكامل مما يؤدى إلي تعطيل الخدمات الحيوية للمؤسسة، أما الجانب الأخر فيشمل سرية وتكامل المعلومات حيث قد يؤدي الاطلاع علي المعلومات السرية أو تغييرها إلي خسائر مادية أو معنوية كبيرة، وهناك العديد من المخاطر نتيجة استخدام تكنولوجيا المعلومات في الرقابة منها (نصر والسيد، 2003: 220):

1- الاعتماد علي البرامج والأنظمة التي يتم من خلالها تشغيل البيانات بشكل غير حقيقي وغير دقيق أو قد تكون عدم الدقة في البيانات ذاتها.
2- تغيير البيانات بشكل غير مصرح به في الدفتر أو الملف الرئيس أي إمكانية التلاعب في البيانات.
3- فقدان محتمل للبيانات، أو حذفها بطريقة خاطئة.
4- الفشل في أجراء تغييرات لازمة في الأنظمة والبرامج.
5- تغيير بشكل غير مصرح به في البرامج أو الأنظمة.
6- دخول غير مصرح به إلي البيانات والذي يؤدي إلي تدمير البيانات أو تغييرها.

7- تضخم أثر الأخطاء التي تحدث أثناء التشغيل حيث يتم تشغيل البيانات بصورة متماثلة مما يؤدي إلي تراكم الأخطاء بصورة كبيرة.
8- الحاسب الآلي غير قادر علي التفكير أو الحكم الشخصي وبالتالي فأن هناك العديد من الأخطاء التي يمكن حدوثها ما لم توجد إجراءات رقابية علي البرامج المستخدمة.
9- الحاسب الآلي يقوم بالعديد من المهام التي تتعارض مع مبدأ الفصل بين المهام.

10- تتطلب بيئة تكنولوجيا المعلومات ضرورة توافر خبرات ومؤهلات علمية وعملية في الأفراد القائمين علي التشغيل مع ضرورة التدريب المستمر لهؤلاء الإفراد لمواكبة التطورات الحديثة في مجال تكنولوجيا المعلومات.

وتصنف مخاطر نظم المعلومات الإلكترونية من وجهات نظر مختلفة إلي عدة أنواع وهي (الشريف، 2006؛ الدرسي، 2009؛ كامل والسيد، 2008):

أولاً: من حيث مصدرها The Source of Threats:

1- مخاطر داخلية.
2- مخاطر خارجية.

ثانياً: من حيث المتسبب بها The Perpetrator:

1- مخاطر ناتجة عن العنصر البشري.
2- مخاطر ناتجة عن العنصر غير البشري.

ثالثاً: من حيث أساس العمد Intention:

1- مخاطر ناتجة عن تصرفات متعمدة.
2- مخاطر ناتجة عن تصرفات غير متعمدة.

رابعاً: من حيث الآثار الناتجة عنها Consequences:

1- مخاطر ينتج عنها أضرار مادية.
2- مخاطر فنية ومنطقية.

خامسا: من حيث علاقتها بمراحل النظام:

1- مخاطر المدخلات.

2- مخاطر التشغيل.

3- مخاطر المخرجات.

وفيما يلي توضيح لتلك المخاطر:

2.9.1 من حيث مصدرها The Source of Threats:

وتنقسم إلي نوعين مخاطر داخلية ومخاطر خارجية:

1- **مخاطر داخلية:** يعتبر موظفي المؤسسات هم المصدر الرئيسي للمخاطر الداخلية التي تتعرض لها نظم المعلومات الإلكترونية وذلك لأن موظفي المؤسسات علي علم ومعرفة بمعلومات النظام وأكثر دراية من غيرهم بالنظام الرقابي المطبق لدي المؤسسة، ومعرفة نقاط القوة والضعف ونقاط القصور لهذا النظام ويكون لديهم القدرة علي التعامل مع المعلومات والوصول إليها من خلال صلاحيات الدخول الممنوحة لهم، ولذلك فأن موظفي المؤسسة غير الأمناء يستطيعون الوصول للبيانات وإمكانية تدميرها أو تحريفها أو تغييرها.

2- **مخاطر خارجية:** وتجرى من أشخاص خارج المؤسسة ليس لهم علاقة مباشرة بالمؤسسة مثل قراصنة المعلومات والمنافسين الذين يحاولون اختراق الضوابط الرقابية والأمنية للنظام بهدف الحصول علي معلومات سرية عن المؤسسة أو قد تتمثل في كوارث طبيعية مثل الزلازل والبراكين والفيضانات والتي قد تحدث تدمير جزئي أو كلي للنظام في المؤسسة.

2.9.2 من حيث المتسبب لها The Perpetrator:

وتنقسم إلي نوعين وهي مخاطر ناتجة عن العنصر البشري ومخاطر ناتجة عن العنصر غير البشرية:

1- **مخاطر ناتجة عن العنصر البشري:** وهي تلك الأخطاء قد تحدث من قبل أشخاص بشكل مقصود وبهدف الغش والتلاعب أو بشكل غير مقصود نتيجة الجهل أو السهو أو الخطاء.

2- **مخاطر ناتجة عن العنصر غير البشري:** وهي تلك المخاطر التي قد تحدث بسبب كوارث طبيعية ليس للإنسان علاقة بها مثل حدوث الزلازل والبراكين والفيضانات والتي قد تؤدي إلي تلف النظام ككل أو جزء منه.

2.9.3 من حيث العمد:

وتنقسم إلي نوعين مخاطر ناتجة عن تصرفات متعمدة ومخاطر عن تصرفات غير متعمدة:

1- **مخاطر ناتجة عن تصرفات متعمدة:** وتتمثل في تصرفات يقوم بها الشخص متعمداً مثل إدخال بيانات خاطئة وهو يعلم ذلك، أو قيامة بتدمير بعض البيانات متعمداً ذلك بهدف الغش أو التلاعب أو السرقة، وتعتبر هذه المخاطر من المخاطر المؤثرة جداً علي النظام.
2- **مخاطر ناتجة عن تصرفات غير متعمدة:** وتتمثل في تصرفات يقوم بها الأشخاص نتيجة الجهل وعدم الخبرة الكافية كإدخالهم لبيانات بطريقة خاطئة بسبب عدم معرفتهم بطرق إدخالها أو السهو في عملية التسجيل.

2.9.4 من حيث الآثار الناتجة عنها Consequences:

وتنقسم إلي نوعين مخاطر ينتج عنها أضرار مادية ومخاطر فنية ومنطقية:

1- **مخاطر تنتج عنها أضرار مادية:** وهي المخاطر التي تؤدي إلي حدوث أضرار بأجهزة الحاسب أو تدمير وسائل تخزين البيانات والتي قد يكون سببها كوارث طبيعية لا علاقة للإنسان بها أو قد تكون بسبب البشر بطريقة متعمدة أو عفوية.
2- **مخاطر فنية ومنطقية:** وهي المخاطر الناتجة عن أحداث قد تؤثر علي البيانات وإمكانية الحصول عليها للأشخاص المخول لهم بذلك عند الحاجة لها أو إفشاء بيانات سرية لأشخاص غير مصرح لهم بمعرفتها وذلك من خلال تعطيل في ذاكرة الحاسب أو دخول فيروسات للحاسب قد تفسد البيانات أو جزء منها.

2.9.5 من حيث علاقتها بمراحل النظام:

وتنقسم إلي ثلاث أنواع مخاطر المدخلات ومخاطر التشغيل ومخاطر المخرجات:

1- **مخاطر المدخلات:** وهي المخاطر الناتجة عن عدم تسجيل البيانات في الوقت المناسب وبشكلها الصحيح أو عدم نقل البيانات بدقة خلال نقلها، وتنقسم المخاطر المتعلقة برقابة المدخلات إلي أربعة أقسام أساسية وهي:

- **إدخال بيانات غير سليمة:** ويتم ذلك من خلال إدخال بيانات غير حقيقة ولكن بواسطة مستندات صحيحة يتم وضعها داخل مجموعة من العمليات دون أن يتم اكتشافها، مثل إدخال فواتير وهمية باسم احد الموردين.
- **تعديل أو تحريف بيانات المدخلات:** ويتم ذلك من خلال التلاعب في المدخلات والمستندات الأصلية بعد اعتمادها من قبل المسئول وقبل إدخالها إلي النظام، وذلك عن طريق تغيير في أرقام مبالغ بعض العمليات لصالح المحرف، أو تغيير أسماء بعض العملاء أو معدلات الفائدة.
- **حذف بعض المدخلات:** يحدث ذلك من خلال حذف أو استبعاد بعض البيانات قبل إدخالها إلي الحاسب الآلي، أما بشكل متعمد ومقصود أو بشكل غير متعمد وغير مقصود، مثل تعديل تفصيلات حساب المصرف.
- **إدخال البيانات أكثر من مرة:** المقصود بذلك قيام الموظف بتكرار إدخال البيانات إلي الحساب أما بطريقة مقصودة أو غير مقصودة، ويتم ذلك من خلال إدخال بيانات بعض المستندات أكثر من مرة إلي النظام قبل أوامر الدفع وذلك أما بعمل نسخ إضافية من المستندات الأصلية وتقديم كل من الصورة والأصل أو أعادة إدخال البيانات مرة أخري إلي النظام.

2- **مخاطر التشغيل:** يقصد بها المخاطر المتعلقة بالبيانات المخزنة في ذاكرة الحاسب والبرامج التي تقوم بتشغيل تلك البيانات وتتمثل مخاطر التشغيل في الاستخدام غير المصرح به لنظام وبرامج التشغيل وتحريف وتعديل البرامج بطريقة غير قانونية أو عمل نسخ غير قانونية أو سرقة البيانات الموجودة على الحاسب الآلي، مثل قيام الموظف بإعطاء أوامر للبرامج بأن لا يسجل أي قيود في السجلات المالية تتعلق بعمليات البيع الخاصة بعميل معين من اجل الاستفادة من مبلغ العملية لصالح المحرف نفسه.

3- **مخاطر المخرجات:** يقصد بها المخاطر المتعلقة بالمعلومات والتقارير التي يتم الحصول عليها بعد عملية تشغيل ومعالجة البيانات، وقد تحدث تلك المخاطر من خلال طمس أو تدمير بنود معينة من المخرجات أو خلق مخرجات زائفة وغير صحيحة أو سرقة مخرجات الحاسب أو إساءة استخدامها أو عمل نسخ غير مصرح بها من المخرجات أو الكشف غير المسموح به للبيانات عن طريق عرضها علي شاشات العرض أو طبعها علي الورق أو طبع وتوزيع المعلومات بواسطة أشخاص غير مسموح لهم بذلك، كذلك توجيه تلك المطبوعات والمعلومات خطأ إلي أشخاص

ليس لهم الحق في الاطلاع علي تلك المعلومات أو تسليم المستندات الحساسة إلي أشخاص لا تتوافر فيهم الناحية الأمنية بغرض تمزيقها أو التخلص منها مما يؤدي إلي استخدام تلك المعلومات في أمور تسئ إلي المؤسسة وتضر مصالحها.

2.10 المخاطر القانونية المرتبطة بنظم المعلومات الإلكترونية:

إن شبكة الانترنت قد تخطت جغرافيا الحدود، كونها فضاء افتراضي لا يعير الأوراق أي أهمية بل تعتمد في مراسلاتها واتصالاتها علي تقنيات عديدة دون وجود مستندات أصلية أو توقيعات يدوية، مما يلقي علي المحاكم مهمة تحديد القواعد القانونية التي تنطبق عليها، سواء بالنسبة إلي حجية العقود وأثارها، أو بالنسبة إلي الاختصاص القضائي العائد لهذه الدولة أو تلك، وبالتالي إلي القانون الواجب تطبيقه في هذا النطاق، وهناك العديد من الشكوك التي تحوم حول مدي الأمان الذي توفره شبكة الانترنت، والتي في الغالب تتعرض لمحاولات اعتداء وقرصنة من شأنها تكبيد المتعاقدين خسارة كبيرة غير معاقب عليها في القوانين النافذة حالياً، ومن أهم المخاطر القانونية المتعلقة بنظم المعلومات الإلكترونية (الدرسي، 2009)، ما يلي:

2.10.1 مشاكل الإثبات الإلكتروني:

1- **مدى حجية الكتابة الإلكترونية:** لا يوجد مجال للشك في أن الكتابة تحتل المرتبة الأولى في إثبات التصرفات القانونية، خصوصاً أمام عدم توافر الثقة الكافية في شهادة الشهود كوسيلة للإثبات في العصر الحالي، ولكن مع ظهور وسائل اتصال حديثة قد دفع المؤسسات إلي استخدام هذه الوسائل لمواكبة التطور التكنولوجي، ومن أهم النقاط التي تثير الجدل بالمستندات الإلكترونية مقارنة بالمستندات الورقية ما يلي:

أ- السند الورقي يستند إلي أساس مادي مكتوب وهو الورقة ذاتها، أما السند الإلكتروني فيستند إلي نظام إلكتروني مما يؤدي إلي آثار خطيرة تبدو في إمكانية تعديل أو تغيير مضمون المستند الإلكتروني دون أن يبقي أثر، بينما يصعب هذا الأمر في حالة المستندات الورقية.

ب- احتمال حدوث خطأ عند استخدام السند الإلكتروني أكبر بكثير منه في السند الورقي، مما يعني أن السند الإلكتروني قد لا يكون بنفسه دليلاً كافياً لإثبات المعاملات.

2- **مدى حجية التوقيع الإلكتروني:** يمكن تعريف التوقيع الإلكتروني بأنه "رقم أو رمز سري ينشؤه صاحبة باستخدام برنامج حاسب آلي، عن طريق معادلة رقمية مرمزة كرسالة إلكترونية يجري تشفيرها بأحد خوارزميات المفاتيح" (الدرسي، 2009: 66).

ويؤدي التوقيع الإلكتروني نفس وظائف التوقيع التقليدي (الكتابي) فهو أداة للتعبير عن إرادة الشخص في قبول الالتزام بمضمون العقد، ووسيلة لتوثيق العقد وتأمينه من التعديل كما أنه يميز الشخص ومن أهم أنواع التوقيع الإلكتروني (التوقيع الكودي، التوقيع البيومتري، التوقيع الرقمي، التوقيع بالقلم الإلكتروني)[8].

خلاصة القول فيما يتعلق بمجال الإثبات والتوقيع الإلكتروني أنه يجب علي المؤسسات اتخاذ الإجراءات القانونية والإدارية الكفيلة بحماية حقوقها وحقوق عملائها، وذلك بالعمل علي تنظيم عملية الإثبات، بمقتضى أتفاق واضح وصريح في العمليات الإلكترونية.

2.10.2 مشاكل الإخلال بالالتزامات التعاقدية الإلكترونية:

1- **المسؤولية عن الحفاظ علي السرية:** بما أن العمليات الإلكترونية بين العميل والمؤسسة تتم باستعمال وسائل إلكترونية حديثة وعبر شبكة اتصال مفتوحة يمكن للغير الدخول لها، مما يعرض الحسابات المصرفية لخطر القراصنة الذين لا يترددون بالتلاعب بهذه الحسابات سواء بالسحب أو التحويل المالي أو غير ذلك، ويكفي الاطلاع علي حسابات العملاء لانتهاك السرية، ويعد التزام المؤسسة بالحفاظ عل السر من قبيل الالتزامات القانونية، وإذ يجب علي المؤسسة مراعاة السرية التامة لجميع حسابات العملاء وودائعهم وأماناتهم وخزائنهم لديه.

2- **المسؤولية عن التحويل الإلكتروني:** تنشأ مسؤولية المؤسسة التعاقدية عند قيامها بتنفيذ أمر تحويل مزور ليس صادراً عن العميل، لذا من واجبات المؤسسة التحقق من هوية الأمر وصحة التوقيع الإلكتروني، والمؤسسة تعتبر مسئولة دائماً ألا إذا استطاع دفع المسؤولية نتيجة خطأ العميل كثبوت فقدانه أمر التحويل الإلكتروني وإطلاقه في التداول بعد توقيعه علي بياض، أو إهمال في المحافظة علي المعلومات المتعلقة بحسابه، ولا يعتبر العميل مسئولاً عن أي قيد غير مشروع علي حسابه بواسطة التحويل الإلكتروني تم بعد تبليغه للمؤسسة عن إمكانية دخول الغير إلي حسابه، أو فقدان بطاقته، أو احتمال معرفة الغير لرمز التعريف المتعلق به، وتعفى المؤسسة من المسؤولية في حالة ثبوت إهمـال العميـل في الحفاظ على سرية وخصوصية المعلومات والبيانـــــات المسلمة له،

---

[8]- يقصد بالتوقيع الكودي: هو التوقيع باستخدام بطاقات الائتمان الممغنطة ذات الرقم السري الذي لا يعلمه إلا صاحبة، ويقصد بالتوقيع البيومتري: وهو التوقيع باستخدام الخواص الذاتية للإنسان مثل: البصمة الشخصية ومسح العين البشرية ومستوى دائرة الصوت والتعرف علي الوجه البشري، كما يقصد بالتوقيع الرقمي: وتعني منظومة بيانات في صورة شفرة وهي توقيعات قائمة علي ترميز المفاتيح العمومية والخاصة، والتوقيع بالقلم الالكتروني: يقصد به وهو توقيع باستخدام قلم الكتروني حساس يمكنه الكتابة علي شاشة الحاسب الآلي.

كالرقم السري، وبطاقة الصراف الآلي وغيرها، كما لابد من إثبات أن المؤسسة قد بذلت تقصى الجهد للحيلولة دون أي استعمال غير مشروع للحسابات الموجودة لديها (امراجع، 2009).

2.11 أساليب تقييم الرقابة في نظم المعلومات الالكترونية:

توجد العديد من الأساليب التي يمكن استخدامها من قبل المراجعين لتقييم رقابة نظم المعلومات وهي:

2.11.1 فحص النظام:

يقوم المراجع بالفحص الدوري لأنظمة رقابة المعلومات للوصول إلي فهم عام عن النظام قبل القيام باختبار إجراءات الرقابة، ويمكن تحقيق ذلك من خلال ثلاث أساليب وهي:

1- **المقابلات الشخصية:** يقوم المراجع بعقد مجموعة من المقابلات الشخصية مع العديد من الأشخاص بهدف فهم وظائف النظام والتعرف علي آليات الرقابة المطبقة.
2- **التعقب:** يهدف هذا الأسلوب إلي تعقب عملية ما عبر القسم من بداية دخولها وحتى مغادرتها أو تسجيلها في الدفاتر وحفظها، وهذا يمكن من فحص وتقييم فعالية آليات الرقابة التطبيقية القائمة بالنظام موضوع الفحص والتقييم.
3- **قوائم الاستقصاء:** تتضمن قائمة الاستقصاء مجموعة من الأسئلة التي تغطي خصائص النظام الجيد لرقابة نظم المعلومات، ويتطلب تصميم قوائم الاستقصاء وجود تصور مسبق للتهديدات الأمنية المحتملة، ثم تصور لآليات الرقابة الكفيلة بمنع هذه التهديدات أو الكشف عنها، ثم التعبير عن هذه الآليات في صورة أسئلة، مما يتيح للمراجع تحديد نقاط الضعف والقوة في نظام رقابة نظم المعلومات، ويمكن للمراجع الإجابة عن أسئلة قائمة الاستقصاء من خلال سؤال العاملين أو الاطلاع علي التقارير الوصفية وخرائط سير العمليات الموجودة بالمؤسسة (الفرطاس، 2006).

2.11.2 برامج المراجعة العامة:

عبارة عن حزم من البرامج المطورة من قبل شركات متخصصة في مجال البرمجيات تساعد المراجع في أداء المهام الشائعة في المراجعة وبصفة خاصة في جمع الأدلة الإلكترونية، وتمتاز تلك البرامج بالسرعة والدقة العالية في أداء المهام مما يزيد من فعالية عملية المراجعة ويزيد أيضاً من استقلال المراجع، بالإضافة إلي ذلك تتيح تلك البرامج فحص ملفات بيانات المؤسسة بدون استخدام برامج المؤسسة، أيضاً تمتاز تلك البرامج بسهولة تعلمها وتشغيلها ولكن

يعاب عليها احتياجها إلي أجهزة وبرامج محددة ومساحات تخزينية كبيرة علي وحدة التخزين الرئيسية.

2.11.3 النظم الخبيرة:

النظم الخبيرة هي نظم تعمل علي استخلاص المعرفة من خبير بشرى ماهر، وإدخالها للحاسب الآلي بشكل يسمح للنظام بتقديم نصحه أو اتخاذ قرار سليم فيما يتعلق بمشكلة معينة، ويتضمن أي نظام للخبرة عدد ست مكونات أساسية هي: قاعدة بيانات المعرفة، قاعدة بيانات المجال، نظم إدارة قاعدة البيانات، أداة الاستدلال، برامج اتصال المستخدم بالنظام، برامج اقتناء المعرفة، ويمكن استخدام تلك النظم وما تتيحه من مزايا في تطوير نظم خبيرة قادرة علي تقييم الرقابة لنظم المعلومات المحاسبية.

2.12 العوامل المؤثرة علي فعالية نظم المعلومات الالكترونية:

"يتوقف تحقيق نظم المعلومات الالكترونية لأهدافها علي مجموعة من العوامل والمتغيرات التي تحيط بالمؤسسة والمتمثلة في النظام السياسي، والنظام الاقتصادي، والاجتماعي، والتكنولوجيا، والزبائن أو العملاء، أي أنها تمثل كافة العوامل التي تؤثر علي مدى نجاح نظم المعلومات الالكترونية وهي نوعين من العوامل، عوامل داخلية، وعوامل خارجية (فطناني، 2007: 5)، وهي كما يلي:

2.12.1 العوامل الداخلية:

تتمثل في كافة الإمكانيات والموارد المادية والبرمجية والبشرية المتوفرة في النظام بالإضافة إلي البيانات المتاحة والإجراءات المستخدمة، وهي عوامل تتصف بإمكانية التحكم بها والسيطرة عليها كونها تنتج عن القرارات الصادرة عن الإدارة لذا يطلق عليها متغيرات القرار.

2.12.2 العوامل الخارجية:

وهي عوامل يصعب أو لا يمكن التحكم بها والسيطرة عليها وتنتج عن البيئة الخارجية التي تحيط بالنظام والتي يتم في إطارها ممارسة الأنشطة والعمليات، وعلي الرغم من صعوبة وضع حد بين العوامل الداخلية والخارجية التي تؤثر علي مستوي فعالية نظم المعلومات حيث أنها عوامل متداخلة فيما بينها في كثير من المجالات وتتشابك العلاقات بينها في نقاط ومراحل عديدة إلا أنه يمكن قياس تأثير العوامل الخارجية من العوامل التالية:

1- **العوامل القانونية والتشريعات المهنية:** تتمثل في تحديد أثر تطبيق التشريعات القانونية ذات العلاقة بالمصارف علي نظم المعلومات سواء كان بصورة مباشرة كقانون المصرف المركزي وقانون المصارف بصورة غير مباشرة كالتعليمات المنصوص عليها في قانون الشركات وقانون السوق المالي وغيرها من التشريعات، وبالإضافة إلي قياس أثر تطبيق المبادئ والمعايير المحاسبية المتعارف عليها ومعايير المراجعة الدولية وغيرها من القواعد والمعايير المهنية ذات العلاقة والإعمال المصرفية علي نظم المعلومات.

2- **العوامل الاقتصادية:** تتمثل في طبيعة الوضع الاقتصادي السائد وانعكاساته علي الأنشطة وأنظمتها المعلوماتية والذي يمكن قياسه من خلال مؤشرات الاستقرار والنمو الاقتصادي، ودرجة تباين الأسواق التي يتعامل معها القطاع المصرفي، ودرجة المنافسة والقدرة علي التنبؤ بتصرفات المنافسين وردود أفعالهم.

3- **العوامل التنظيمية:** يمثل الهيكل التنظيمي الإطار الذي يتم بموجبة ترتيب وتنسيق جهود الإفراد والعاملين لتنفيذ الأنشطة اللازمة لتحقيق الأهداف باستخدام الموارد المتاحة، ويمكن قياس مدى تأثير العوامل التنظيمية علي نظم المعلومات الالكترونية من خلال قياس درجة المركزية أو اللامركزية والتي تشير إلي مدى تدخل الإدارة العليا ودرجة تفويض السلطات والصلاحيات إلي المستويات الإدارية الأخرى، وقياس درجة تحقيق التكامل بين الأقسام والإدارات المختلفة في المؤسسة لضمان اكتمال العمل وتجنب التعارض بين الأقسام المختلفة، وقياس مدى تطبيق محاسبة المسؤولية علي جميع العاملين في المستويات الإدارية المختلفة، وقياس درجة البيروقراطية ومدى تركيز العمل في أيدي إفراد محدودين ودرجة تعقد أداء الإعمال وتنفيذ الأنشطة.

4- **العوامل السلوكية:** تتمثل في أنماط السلوك الثقافية والاجتماعية للبيئة المحيطة بالمؤسسة والتي ينعكس أثرها علي نظم المعلومات، كمقاومة التجديد والخوف مما ستفرضه نظم المعلومات من تغيير في نمط العلاقات الاجتماعية بين العاملين والرغبة في استمرار العمل وفقاً للروتين المعهود، والقلق والصراع الداخلي الناتج عن الشعور بفقدان الأمن والاستقرار الوظيفي ومخاطر الإحلال الوظيفي وفقدان فرص الترقية، ونقص الإدراك والخوف من التكنولوجيا وعدم القدرة علي فهمها والتعامل معها.

5- **العوامل التقنية وتكنولوجيا المعلومات:** ويمكن قياس تأثير تكنولوجيا المعلومات علي نظم المعلومات الإلكترونية من خلال قياس مدى توفر الوسائل التقنية الملائمة لتشغيل البيانات إلكترونياً وإنتاج المعلومات، وقياس مدى ضوابط وأدوات الرقابة الادارية في تحقيق الرقابة علي المكونات المادية، وأيضاً قياس مدى إسهام تكنولوجيا المعلومات في

تحقيق التكامل والترابط بين أنشطة الأقسام والإدارات المختلفة ومدى إسهامها في تعزيز التوجه نحو بناء النظم المتكاملة للمعلومات.

2.13 الخلاصة:

تناول الفصل الثاني سرد نظري لرقابة نظم المعلومات الإلكترونية، وتم عرض بعض التعريفات المرتبطة برقابة نظم المعلومات الإلكترونية، والتي تعتبر نظاماً فرعياً داخل المؤسسة يتضمن آليات الرقابة التقنية والتشغيلية والإدارية التي تهدف إلي حماية سرية وسلامة المعلومات من المخاطر المرتبطة بأنظمة المعلومات الالكترونية، وتم عرض المبادئ الأساسية لرقابة نظم المعلومات الإلكترونية المتمثلة في المساءلة، والوعي، وتعدد المجالات، وفعالية التكلفة، والتكامل، وإعادة التقييم، والتوقيت الملائم، والعوامل المجتمعية، كما تم تناول أهداف وأهمية رقابة نظم المعلومات وكيفية تطوير تلك النظم داخل المؤسسة والمقومات التي يجب توافرها لتطوير نظم رقابة جيدة تواجه المخاطر والتهديدات الأمنية، وتم أيضاً توضيح آليات رقابة نظم المعلومات الإلكترونية والتصنيفات المختلفة لها وأساليب التقييم التي يمكن الاستعانة بها عند تقييم تلك النظم.

ويخلص هذا الفصل إلي أن رقابة نظم المعلومات الإلكترونية تحقق أهداف الرقابة الداخلية المتمثلة في حماية أصول المؤسسة، والدقة في المعلومات والبيانات والاعتماد عليها، وتعتبر المعلومات من أهم أصول المؤسسة في الوقت الحاضر وهي عرضة للاحتيال، والسرقة، والتعدي، والتخريب، ومع زيادة أهمية المعلومات تزداد الحاجة إلي حمايتها وحفظها، وبالتالي فأنه يلزم حمايتها من الاختراق، والعبث بها، أو تخريبها، أو إتلافها، أو سرقتها، ويتم ذلك من خلال تبني آليات فعالة لرقابة تلك المعلومات مع ضرورة تقييم تلك الآليات بصورة دورية لتحديد نقاط الضعف والعمل علي تحسينها لتحقيق مستوى رقابي جيد لتلك المعلومات، أما الفصل التالي يستعرض أهم الإصدار المهنية والدراسات السابقة المرتبطة بالرقابة في نظم المعلومات الإلكترونية.

الفصـــل الثالـــث:

مراجعة الدراسات السابقة

3.1 مقدمــة:

استعرض الفصل السابق مقدمة عن الرقابة في نظم المعلومات الإلكترونية من حيث مفهومها، وأهدافها، ومبادئ ومقومات النظام الجيد، ومخاطرها التشغيلية والقانونية، والعوامل المؤثرة علي فعالية نظم المعلومات، أما في هذا الفصل سيتم مراجعة الدراسات السابقة، حيث تناولت العديد من البحُاث والجهات المهنية الضوابط الرقابية في نظم المعلومات الإلكترونية وتحديد وتحليل التهديدات والمخاطر الرقابية التي تتعرض لها نظم المعلومات الالكترونية، وعلاقتها بتطوير فعالية وجودة الرقابة علي البيانات وموثوقيتها وتم تقسيم أدبيات الدراسة إلي جزئين كالتالي:

- الإصدارات المهنية المرتبطة بالرقابة في نظم المعلومات الإلكترونية.

- الدراسات المرتبطة بالرقابة في نظم المعلومات الإلكترونية.

3.2 الإصدارات المهنية المرتبطة بالرقابة في نظم المعلومات الإلكترونية:

تتناول هذا الجزء أهم الإصدارات المهنية المرتبطة بالرقابة في نظم المعلومات الالكترونية وهي كما يلي:

- المعيار الصادر عن (اللجنة الفنية المشتركة التي أسستها كل من المنظمة الدولية للمواصفات واللجنة الإلكترونية الفنية الدولية 27000-2005)، (ISO/IEC)، "International Standards Organization and International Electronic Committee":

يعتبر المعيار (ISO/IEUC 27002-2005)، الإطار الشامل للرقابة والذي يقدم توصيات حول الممارسات الجيدة في مجال إدارة رقابة المعلومات موجهة إلى الأطراف المسئولة عن تحقيق رقابة المعلومات والحفاظ عليه في المؤسسة، وتهدف تلك التوصيات إلى توفير الثقة في التعاملات التي تتم بين المؤسسة، حيث تم التوصل إلى تلك التوصيات من خلال دراسة ومقارنة الممارسات المتبعة في عدد من المؤسسات العالمية التي تعد رائدة في مجال رقابة المعلومات.

وقدم المعيار تسعة أهداف فرعية لحماية أصول المعلومات ضد المخاطر المحتملة للسرية والسلامة والإتاحة، والتي تمثل متطلبات وظيفية شاملة محددة للبيئة الأساسية لإجراءات الرقابة في إدارة رقابة المعلومات ويقسم المعيار مجال الرقابة على المعلومات إلى أحدى عشر مبدأ هي سياسة الرقابة، الرقابة التنظيمية، تصنيف الأصول ورقابتها، رقابة الأفراد، الرقابة المادية والبيئية، إدارة الاتصالات والعمليات، رقابة الوصول إلى المعلومات، تطوير الأنظمة وصيانتها، إدارة استمرارية الأعمال، إدارة حوادث رقابة المعلومات، والالتزام، وفيما يلي توضيح لكل مبدأ من تلك المبادئ.

المبدأ الأول سياسة الرقابة: يجب أن تحدد سياسة واضحة توضح اتجاهاتها ودعمها لرقابة المعلومات، حيث يتم وضع سياسة رقابية عامة موجزة للمستويات الإدارية العليا في المؤسسة بالإضافة إلي وضع مجموعة من السياسات الرقابية التفصيلية في صورة دليل لسياسة رقابة المعلومات للمستويات الإدارية الأخرى.

المبدأ الثاني الرقابة التنظيمية: يجب أن تمتلك المؤسسة هيكل إدارة لرقابة المعلومات لتوفير التوجيهات وتوضيح الالتزامات، كما يجب توضيح الأدوار والمسؤوليات الخاصة بالوظائف الرقابية وتأسيس قنوات الاتصال مع الإطراف الأخرى و إجراء المتابعة والمراجعة المستمرة.

المبدأ الثالث تصنيف الأصول ورقابتها: علي المؤسسة أن تفهم طبيعة أصول المعلومات المملوكة لديها وكيفية إداراتها رقابياً، وتحديد المسئول عن كل أصل وتصنيف تلك الأصول وفقاً للاحتياجات الرقابية المطلوبة لكل أصل.

المبدأ الرابع رقابة الإفراد: يجب علي المؤسسة إدارة حقوق الوصول للنظام وتوفير برامج الوعي والتدريب الملائمين للعاملين والتحقق من الخلفية الجنائية للعاملين قبل التعيين وإلغاء امتيازات الإفراد الذين يتم الاستغناء عنهم.

المبدأ الخامس الرقابية المادية والبيئية: يجب حماية معدات الحاسب الهامة مادياً من الأضرار المتعمدة أو غير المتعمدة، بالإضافة إلى الحماية من السرقة والحرارة المرتفعة، وينقسم هذا البعد إلى جزئيين: الجزء الأول يهدف إلى حماية مناطق تواجد الأجهزة من الوصول غير المصرح به، والجزء الثاني حماية معدات الحاسب الهامة والكابلات من الأضرار المادية والحرائق والفيضانات والسرقة سواء كانت داخل أو خارج المؤسسة.

المبدأ السادس إدارة الاتصالات والعمليات: يهدف هذا البعد إلى تحديد إجراءات الرقابة للأنظمة وإدارة الشبكات، حيث يجب توثيق الإجراءات والمسؤوليات التشغيلية لتكنولوجيا المعلومات وإدارة خدمات التعهيد وإدارة النسخ الإحتياطية وإدارة تبادل المعلومات والخدمات الإلكترونية.

المبدأ السابع رقابة الوصول: يجب مراقبة الوصول المنطقي لأنظمة تكنولوجيا المعلومات والشبكات والبيانات لمنع الاستخدام غير المصرح به، ولابد من تحديد متطلبات الأعمال لرقابة الوصول وإدارة وصول المستخدم وتحديد مسؤوليات وأدوار المستخدمين ورقابة الوصول للشبكات.

المبدأ الثامن تطوير الأنظمة وصيانتها: يجب على المؤسسة إدارة رقابة المعلومات في دورة حياة الأنظمة (التطوير، الاختبار، التطبيق والصيانة)، من خلال تحديد وتحليل المتطلبات الرقابية اليدوية والإجراءات اللازم دمجها في مرحلة التطوير.

المبدأ التاسع إدارة حوادث رقابة المعلومات: يهدف هذا البعد إلى تقديم تقرير عن الأحداث والحوادث الرقابية وإدارتها بشكل ملائم، ولابد من التقرير عن نقاط ضعف وأحداث رقابة المعلومات والاستجابة الملائمة لكل حدث والإجراءات التي لابد من إتباعها لتصعيد تلك التقارير للمستويات الإدارية العليا.

المبدأ العاشر استمرارية الأعمال: يهدف هذا البعد إلى وصف العلاقة بين خطط الطوارئ واستعادة الأعمال من بداية التحليل والتوثيق للظروف الطارئة إلى مرحلة اختبار الخطط والتنفيذ.

المبدأ الحادي عشر الالتزام: يهدف هذا البعد إلى توضيح التزام المؤسسة من خلال تحديد الالتزامات والمتطلبات القانونية والالتزام بالسياسات والمعايير والالتزامات التقنية والرقابية.

إما الأهداف الفرعية التسعة التي قدمها المعيار لحماية أصول المعلومات ضد المخاطر المحتملة للسرية والسلامة والإتاحة، تتمثل في: خفض الخطأ والغش، رقابة الوصول المادي، رقابة الوصول المنطقي، رقابة أمن البيانات، معايير التوثيق، خطة التغلب علي آثار الكارثة، رقابة العمليات الخاصة بالإنترنت والاتصالات والمصارف الإلكترونية، رقابة أمن النتائج، وأخيراً أمن خدمات التعهيد وفيما يلي تفاصيل هذه الأهداف:

الهدف الفرعي الأول خفض الخطأ والغش: يهدف إلي تخفيض فرص ارتكاب الخطأ والغش وزيادة فرص اكتشافها ويتم ذلك من خلال إتباع الإجراءات الرقابية التالية:

1- الفصل بين وظائف تطوير نظم المعلومات (مثل: الفصل بين وظائف التحليل والبرمجة والتشغيل) والوظائف المحاسبية.
2- تناوب الواجبات لتقليل فرص حدوث الغش وزيادة فرص اكتشاف الخطأ.
3- إعطاء أجازات إجبارية للعاملين لتخفيض احتمال الغش.
4- التأكد من الصحيفة الجنائية للعاملين المصرح لهم بالوصول للبيانات الهامة.
5- وجود إشراف ملائم علي كل الوظائف الرقابية.

الهدف الفرعي الثاني رقابة الوصول المادي: تهدف إلي حماية حجرات وأجهزة وتجهيزات الحاسب الآلي من الوصول غير المصرح به ويتم ذلك من خلال إتباع الإجراءات الرقابية التالية:

1- وضع جهاز الخادم (Server) والمعدات الهامة في حجرات مغلقة بإحكام.
2- تسجيل الدخول إلي حجرات الحاسب الآلي ومتابعة سجلات الدخول من خلال موظف مختص.
3- حصر الوصول المادي إلي حجرات الحاسب الآلي التي تحتوي موارد تكنولوجيا المعلومات الخاصة بالمصرف لإفراد محددين ومراقبة تلك الحجرات بكاميرات مراقبة.
4- وجود سجلات للزائرين تحتوي علي البيانات الكافية وأسباب الزيارة.
5- تركيب أجهزة إنذار بصفة خاصة علي معدات أجهزة الحاسب الآلي.
6- وجود تامين ضد السرقة والمخاطر الأخرى يغطي أجهزة الحاسب الآلي.

الهدف الفرعي الثالث رقابة الوصول المنطقي: يهدف إلي حماية أجهزة الحاسب الآلي من الاستخدام غير المصرح به ويتم ذلك من خلال إتباع الإجراءات الرقابية التالية:

1- كل مستخدم له الهوية (ID)، وكلمة المرور الخاصة به التي يصعب تخمينها.
2- تغيير كلمات المرور بصورة دورية (علي الأقل كل 90 يوم).
3- احتواء كلمة المرور علي الأقل (6) حروف واحدهما علي الأقل رقمي.
4- وضع شاشات توقف بكلمات مرور (Screen saver).
5- توعية العاملين بضرورة عدم كتابة كلمات المرور أو إظهارها علي الشاشة أو تداولها فيما بينهم.
6- تحديد الأشخاص المصرح لهم منح أو تغيير هويات التعرف وكلمات المرور.

7- تحديد الأشخاص المفوض لهم الوصول إلي معلومات المؤسسة وتوفير الهويات اللازمة لذلك.

8- منع النسخ غير المصرح به لرخص البرامج.

9- منع استخدام نسخ غير أصلية من البرامج.

10- توفير آليات رقابة لحماية أشرطة الأمن المخزنة في النظام والتي تستخدم من قبل النظام للتحقق من الصحة (مثل: رقابة ملفات كلمات المرور).

11- منع الدخول غير المصرح به علي البيانات وملفات نظم المعلومات المحاسبية (مثل: استخدام أسلوب إعادة الطلب الهاتفي والذي يعمل علي منع الاتصال الهاتفي غير المصرح به بنظم شبكات الحاسبات).

12- استخدام برنامج ربط الشبكات الخاص الافتراضي (Virtual Private Networking)، لمنع الوصول غير المصرح به، تعطيل خدمات الشبكة غير الضرورية في خدمات المصرف.

13- استخدام أنظمة تعقب المتطفلين لتوفير متابعة مستمرة لشبكة المصرف والاكتشاف المبكر للاختراقات الرقابية المحتملة.

14- إجراء فحوصات رقابية وتقييم للمخاطر المحتملة بصورة دورية والتقرير عن تلك المخاطر ونتائج الفحص للإدارة العليا لاتخاذ الإجراءات التصحيحية.

15- استخدام إجراءات التحقق من المسلك لضمان عدم إرسال الرسائل الالكترونية إلي عناوين خاطئة.

16- استخدام تقنيات التقرير عن الرسائل لإعلام الراسل أن الرسائل المرسلة تم استلامها.

17- التحديد الالكتروني لكل الشبكات الطرفية.

18- عند الحاجة إلي تجاوزات الإجراءات رقابية الوصول المنطقي لإجراء أي صيانة أو عمليات إصلاح ضرورية لابد من التأكد من توافر التصريح الملائم لذلك التجاوز وإعادة تشغيل تلك الآليات مرة أخري بعد الانتهاء من إجراء العمليات الضرورية.

الهدف الفرعي الرابع رقابة أمن البيانات: تهدف إلي حماية البيانات والمعلومات سواء كانت هذه البيانات موجودة علي أجهزة الحاسب الآلي أو محفوظة في صورة رقمية أو في صورة ورقية ويتم ذلك من خلال إتباع الإجراءات الرقابية التالية:

1- تخزين الملفات في أماكن محمية من الحريق والأتربة وإي ظروف ضارة.
2- إعداد واستخدام دليل جيد للبيانات.
3- تقسيم البيانات علي حسب أهميتها وتحديد مستوى الحماية المطلوب لكل نوع.
4- تشفير البيانات الهامة.
5- تحديد المستخدم المصرح له بالحصول علي كل نوع من المعلومات، وتحديد التوقيت الملائم للحصول علي المعلومات، ومكان تواجد المعلومات في نظام المعلومات.
6- توفير إجراءات الحماية من الكتابة لضمان عدم إعادة الكتابة علي البيانات المخزنة أو حذفها سواء بصورة متعمدة أو غير متعمدة.
7- توفير جداول زمنية لإعداد نسخ احتياطية من البيانات وحفظها بصورة جيدة.
8- اتخاذ الإجراءات اللازمة لتجنب النسخ غير المصرح به للبيانات.
9- منع استخدام لغات البرمجة المتقدمة التي قد تغير من البيانات مع تسجيل إي محاولة لاستخدام تلك اللغات لمتابعتها.
10- تطبيق الإجراءات الرقابية الملائمة عند المناولة اليدوية للبيانات بين الأقسام المختلفة وبين المركز الرئيسي والفروع.
11- طباعة البيانات الهامة بصورة دورية.
12- اتفاقيات الخصوصية الملزمة قانونياً يجب كتابتها من قبل الإدارة العليا وإعلام مستخدمي الحاسب الآلي الذين لديهم حق الوصول إلي البيانات الهامة بهذه الاتفاقيات.
13- حماية الأقراص المغناطيسية للنسخ الاحتياطية وحفظها في خزائن آمنة.

الهدف الفرعي الخامس معايير التوثيق: تهدف إلي بناء نظام يتضمن الإجراءات الرقابية الملائمة لبيئة النظام وتطبيقاته، ويعمل وفقاً لمواصفات التشغيل المعيارية ويمكن اختباره ومراجعته بسهولة ويتم ذلك من خلال إتباع الإجراءات الرقابية التالية:

1- تحديد المعايير والإجراءات الخاصة بعمليات البيانات بما فيها السماح والتفويض للأنظمة الجديدة وإجراء التغيرات في الأنظمة ومعايير تحليل النظام والبرمجة وإجراءات تخزين ومناولة البيانات.
2- توفير الوثائق التي تؤكد تدريب العاملين.
3- تزويد المستخدمين بالتوجيهات اللازمة للتبليغ عن إي اختراقات رقابية لفريق أمن المعلومات حتى يتم متابعة تلك الاختراقات.
4- تحديد الإجراءات المتبعة في حالة عدم الالتزام بالسياسات الرقابية مع تحديد الإجراءات العلاجية التي تتخذ في الوقت الملائم للتعامل مع حالات عدم الالتزام.

الهدف الفرعي السادس خطة التغلب علي آثار الكارثة: يهدف إلي تحقق من مدى وجود خطة شاملة للتغلب علي آثار إي كارثة محتملة الحدوث وتتضمن تلك الخطة كل التطبيقات والبرامج والأجهزة الضرورية للحفاظ علي تشغيل المصرف في الحالات الطارئة ومسئولية كل فرد في عملية التغطية بالإضافة إلي تحديد الوقت اللازم لاستعادة الإعمال عند المستوى الطبيعي لها وتتمثل إجراءات التغلب علي آثار الكارثة في:

1- تحديد التطبيقات والأجهزة والبرامج الضرورية للحفاظ علي استمرار المصرف في حالة حدوث إي حالات طارئة.
2- تحديد لكل الأنشطة اللازمة لاستعادة الأعمال وتتابع تنفيذ تلك الأنشطة والوقت اللازم لتنفيذ كل نشاط، تحديد طريقة الحصول علي الأجهزة والبرامج الضرورية لاستعادة الأعمال.
3- الأماكن التي يمكن من خلالها متابعة مزاولة نشاط المصرف في حالة ما إذا كان الضرر يلحق بمباني المصرف.
4- إجراء فحص واختبار دوري لخطة التغلب علي آثار الكارثة للتأكد من إمكانية تنفيذها في الواقع العملي.
5- الاحتفاظ بالبرامج الأصلية في أماكن آمنة خارج المصرف حتى يمكن الاستفادة من تلك البرامج مرة أخرى عند حدوث الكارثة.
6- توفير نسخ احتياطية من كل الملفات والبرامج مخزنة خارج المصرف لتمكين المصرف من استعادة الملفات والبرامج المدمرة أو التي تم فقدها عند حدوث الكارثة.
7- توفير إجراءات رقابة ملائمة تطبق علي خروج وعودة ملفات البيانات والبرامج من أماكن تخزينها إلي أماكن استخدامها.

8- التحديد الواضح للأشخاص المسئولين عن تنفيذ خطة التغلب علي آثار الكارثة مع تحديد مسؤولية كل فرد من هؤلاء الأشخاص.
9- توفير وحدات قوة الإمداد المتتابعة لتوفير الطاقة خلال فترات انقطاع الطاقة.

10- توافر بوليصة تأمين شاملة تغطي تكاليف أجهزة ومعدات الحاسب الآلي بالإضافة إلي تكاليف انقطاع الإعمال الذي قد ينتج من حدوث كوارث بالحاسب الآلي.

الهدف الفرعي السابع رقابة عمليات التجارة الالكترونية والاتصالات والانترنت: تتمثل في الآليات التالية:

1- وضع برامج الحماية ضد الفيروسات بما فيها البرامج الخاصة بفحص رسائل البريد الالكتروني الوارد بالإضافة إلي التحديث المستمر لتلك البرامج.
2- استخدام حوائط النار (أجهزة - برامج)، لرقابة وحماية الاتصالات بين الشبكة الداخلية والشبكات الخارجية مثل الانترنت.
3- وضع حد للصفقات النقدية الالكترونية التي تتم في اليوم الواحد علي نفس الحساب.
4- توفير بطاقة هوية (ID)، لكل مستخدم لعمليات المصرف الالكتروني الأولى تستخدم في الاستعلامات العامة إما الثانية فتستخدم في إجراء التحويلات والصفقات النقدية.
5- تنشيط الحسابات الالكترونية يتم بعد التسجيل علي الموقع ويستطيع المستخدم الخروج باستخدام الخاصية الملائمة (Sign out)، أو بعد مرور (10) دقائق من التوقف عن الاستخدام.
6- حصر التحويلات النقدية علي الحسابات في نفس المصرف (المرسل والمرسل إليه في نفس المصرف).
7- يتم وقف التعامل علي إي حساب غير مستخدم لمدة (6) أشهر.
8- يتم منع الدخول علي إي حساب بعد ثلاث محاولات غير ناجحة لإدخال الهوية مع تسجيل تلك المحاولات حتى يتم متابعتها.
9- وضع خطوط الاتصالات (الكابلات)، في أماكن خارج منطقة تواجد الأجهزة لمنع رصدها من قبل الأجهزة والمعدات.

10- استخدام التشفير لتشفير المعلومات السرية والخاصة علي الشبكات العامة بما فيها هويات المستخدمين وكلمات المرور.

الهدف الفرعي الثامن رقابة أمن النتائج: تهدف إلي حماية مخرجات الحاسب الآلي من الوصول غير المصرح به وتتمثل في:

1- حصر مخرجات أنظمة المعلومات الهامة يتم الاحتفاظ بها في حجرات مقفلة.
2- الدخول المصرح به للمعلومات الهامة يجب أن يتم مراقبته وتحديده للمستخدمين المصرح لهم خلال فترة التصريح.
3- النسخ الورقية لمخرجات أنظمة المعلومات يتم ختمها بالوقت واليوم.
4- طباعة وتوزيع البيانات والمعلومات يتم في ظل الإشراف الملائم من قبل الأشخاص المصرح لهم في المصرف.
5- يتم استخدام الآلات المخصصة للتخلص من الأوراق التي تم الانتهاء منها.
6- إجراء مراجعة عشوائية منتظمة للمدخلات والمخرجات للتحقق من التشغيل الصحيح (مثل: فحص دفتر أوامر الطباعة مع الملفات المطبوعة).

الهدف الفرعي التاسع رقابة خدمات التعهيد: تتمثل خدمات التعهيد في قيام احد المصارف بالاتفاق مع إحدى المؤسسات التي تعمل في مجال تكنولوجيا المعلومات علي توريد بعض الخدمات التكنولوجية (مثل: تطوير أنظمة معلومات جديدة - إجراء صيانة دورية لأنظمة المعلومات المطبقة لدى المصرف - معالجة المشاكل التقنية التي تطرأ نتيجة لاستخدام أنظمة المعلومات)، وذلك لعدم توافر الخبرات المؤهلة للقيام بتلك الخدمات لدى المصرف، لذلك فأن هدف رقابة الخدمات التي يتم تعهيدها ورقابة أنشطة موفر خدمات التعهيد لضمان سرية وسلامة نظم المعلومات المحاسبية وتتمثل تلك الإجراءات في:

1- وجود تحديد لمسؤوليات والتزامات كلا الطرفين التي تتعلق بالأمن في تعاقدات خدمات التعهيد.
2- إتاحة موفر خدمات التعهيد إمكانية التعرف علي مستوي الأداء الأمني وتقييم المستوى من قبل المصرف.
3- توفير التصريحات اللازمة لمقدم خدمات التعهيد حتى يتمكن من أداء الإعمال المكلف بها.
4- توثيق متطلبات الأمن المستهدفة من قبل المصرف والتي يجب أن يلتزم بها موفر خدمات التعهيد.

- **إرشاد (المؤسسة الدولية للمعايير والتكنولوجيا، 2008)، (NIST) National Institute of Standards and Technology:**

يهدف هذا الإرشاد إلى توضيح الكيفية التي يتم بها وضع خطط فعالة لتقييم الرقابة من خلال تحديد مجموعة شاملة من الإجراءات التي يجب تنفيذها للحصول على تأكيد لفعالية الرقابة المطبقة في أنظمة المعلومات، لما يوفره هذا التأكيد من تقييم لجودة عمليات إدارة المخاطر والتعرف على نقاط الضعف المتواجدة في إجراءات الرقابة المطبقة على نظم المعلومات المحاسبية.

والتقييم الجيد لإجراءات الرقابة يتضمن القيام بجمع الأدلة الكافية لتحديد ما إذا كانت الرقابة المطبقة فعالة في مواجهة المخاطر المحتملة، كما تتضمن تقديم هذه الأدلة بصورة يمكن استخدامها من قبل متخذي القرارات، وللحصول على تلك الأدلة توجد ثلاثة طرق تختلف فيما بينها من حيث مستوى التأكيد المطلوب توفيره وهي: الفحص والمقابلات والاختبار مع إمكانية تطبيق كل طريقة من تلك الطرق بمستويات مختلفة من التفصيل والشمولية يمكن توضيحها كما يلي:

1- **الفحص:** يتمثل في فحص ومراجعة وملاحظة ودراسة وتحليل أحد موضوعات التقييم، ويمكن إجراء الفحص بثلاث مستويات مختلفة من التفصيل هي الفحص العام، والفحص المركز، والفحص المفصل، حيث يقتصر الفحص العام على فحص الوثائق العامة لإجراءات الرقابة لتوفير مستوى محدود من الفهم لإجراءات الرقابة، بينما الفحص المركز يعتمد على القيام بمزيد من التحليل لتوفير مستوى الفهم الضروري لتحديد مدى صحة تطبيق إجراءات الرقابة في بيئة التشغيل، في حين يمتد الفحص المفصل بمزيد من التحليل ليوفر أدلة توضح مدى الاستمرارية في تطبيق إجراءات الرقابة ومدى توافر الدعم الملائم من الإدارة العليا لتحسين مستوى فعالية إجراءات الرقابة المطبقة.
2- **المقابلة:** هي عملية تتم من خلال مناقشة مجموعة من الأفراد المسئولين عن الإجراءات الرقابية لتوفير فهم عام عن الإجراءات الرقابية وتحديد طرق الحصول على الأدلة الملائمة لتوفير تأكيد معقول بشأن فعالية الإجراءات الأمنية المطبقة.

ويمكن إجراء تلك المقابلات بثلاث مستويات مختلفة من التفصيل هي المقابلات العامة والمقابلات المركزة والمقابلات المفصلة، حيث تستند المقابلات العامة على مجموعة من الأسئلة العامة التي توفر مستوى معقول من الفهم لتحديد ما إذا كانت إجراءات الرقابة تطبق بصورة

سليمة أم لا، بينما تعتمد المقابلات المركزة على مجموعة من الأسئلة العامة بجانب أسئلة أخرى محددة تهتم بأجزاء محددة من إجراءات الرقابة وذلك لتوفير مستوى معقول من الفهم والثقة لتحديد ما إذا كانت إجراءات الرقابة تطبق بشكل سليم، في حين أن المقابلات المفصلة تستند على مجموعة من الأسئلة العامة والأسئلة المحددة للتقصي عن إجراءات الرقابة المطبقة لتحديد ما إذا كانت الإجراءات الرقابية المطبقة تطبق بصورة سليمة خالية من الأخطاء ويتوافر لها الدعم الملائم من جانب الإدارة للتحسين المستمر.

3- **الاختبار:** يتم من خلال إجراء مجموعة من الاختبارات لأحد أو لمجموعة من موضوعات التقييم في ظل ظروف محددة لمقارنة النتائج الفعلية بالنتائج المتوقعة، وذلك لتحديد ما إذا كانت آليات الرقابة تطبق بشكل سليم خالي من الأخطاء، وتحديد مدى اكتمالها وصحتها وإمكانية التحسين مع مرور الوقت.

ويمكن إجراء تلك الاختبارات من خلال ثلاث مستويات مختلفة من التفصيل هي الاختبار العام، الاختبار المحدد، والاختبار المفصل، حيث تعتمد منهجية الاختبار العام على عدم وجود أي معرفة مسبقة بالهيكل الداخلي، ويطلق على هذه المنهجية "اختبار الصندوق الأسود" ويتم هذا الاختبار باستخدام المواصفات الوظيفية لأنشطة عمليات المستويات العليا في الهيكل الداخلي وذلك بهدف توفير مستوى الفهم الضروري لآليات الرقابة المطبقة واللازم للحكم على مدى سلامة تطبيق آليات الرقابة.

بينما تعتمد منهجية الاختبار المحدد على توافر درجة معقولة من الفهم والمعرفة بالهيكل الداخلي، ويطلق عليه "اختبار الصندوق الرمادي" ويستخدم هذا الاختيار المواصفات الوظيفية لأنشطة عمليات المستويات العليا في الهيكل الداخلي بجانب المعلومات الخاصة بتركيبة النظام وكيفية دمجها في بيئة التشغيل الخاصة بالأنشطة، وذلك لتوفير مستوى الفهم الضروري لإجراءات الرقابة اللازمة لتحديد ما إذا كانت آليات الرقابة تطبق بشكل سليم، ومدى توفير الثقة بالتطبيق السليم والصحيح لإجراءات الرقابة.

بينما تعتمد منهجية الاختبار المفصلة على المعرفة الكاملة والواضحة بالهيكل الداخلي، ويطلق عليها (اختبار الصندوق الأبيض)، ويتم إجراء هذا الاختبار باستخدام المواصفات الوظيفة لأنشطة عمليات المستويات العليا في الهيكل الداخلي بجانب المعلومات التفصيلية الخاصة بتركيبة النظام وكيفية دمجه في بيئة التشغيل الخاصة بالأنشطة، وذلك لتوفير مستوى الفهم الضروري

لإجراءات الرقابة اللازمة لتحديد ما إذا كانت إجراءات الرقابة تطبق بشكل سليم ومدى توافر الثقة بالتطبيق السليم والصحيح إجراءات الرقابة والتأكد من توافر الدعم اللازم للتحسين المستمر.

كما أشار الإصدار إلى أن عملية تقييم الرقابة تتطلب التحضير والاستعداد سواء من جانب المؤسسة أو من جانب الفريق القائم بالتقييم، يلي ذلك تطوير خطة لإجراءات الرقابة ثم تنفيذ التقييم لإجراءات الرقابة والتحليل والتوثيق وإعداد التقارير، وأخيراً تحليل التقارير للقيام بالخطوات اللازمة للتحسين، وفيما يلي توضيح لتلك الخطوات .

1- **التحضير لتنفيذ تقييم إجراءات الرقابة:** عملية التحضير يجب أن تتناول العديد من الأمور سواء من جانب المؤسسة أو من جانب الفريق القائم بالتقييم ، فعلى المؤسسة أن تضمن وضع سياسة ملائمة تتناول تقييم إجراءات الرقابة وتوصيل تلك السياسة إلى كل الأطراف المعنية بذلك في المؤسسة وضمان القيام بجميع خطوات إدارة المخاطر والتي تشمل تطوير خطة الرقابة وتحديد إجراءات الرقابة الخاصة بالمؤسسة وتقييم هذه الخطة للتأكد من اكتمالها وصحتها وتوافقها مع المتطلبات التنظيمية والحصول على التصديق الملائم لتطبيق تلك الخطة، كما يجب أن تحدد المؤسسة هدف ونطاق عملية التقييم مع تحديد إطار زمني لإكمال عملية التقييم، واختيار فريق العمل المؤهل للتقييم مع توفير الاستقلالية الكاملة لهذا الفريق.
2- **تطوير خطة الرقابة:** خطة تقييم الرقابة توفر أهداف تقييم إجراءات الرقابة وخريطة تفصيلية عن كيفية إجراء التقييم ولذلك يجب أن تتضمن التحديد الواضح لنطاق وغرض تقييم إجراءات الرقابة، والإجراءات التي يتم تقييمها وإجراءات التقييم الملائمة وترتيب تنفيذ تلك الإجراءات بعد ذلك يتم صياغة خطة التقييم النهائية والحصول على الموافقات اللازمة للبدء في تنفيذ التقييم لإجراءات الرقابة.
3- **تنفيذ تقييم إجراءات الرقابة وتوثيق نتائج التقييم:** يجب توثيق نتائج التقييم بمستوى ملائم من التفصيل وفقاً لهيكل التقرير من قبل المؤسسة كما يجب أن يلاءم هذا التوثيق نوع إجراءات الرقابة التي يتم تقييمها، بالإضافة إلى توفير توصيات محددة عن كيفية تصحيح نقاط الضعف الموجودة بإجراءات الرقابة لتخفيض أو الحد من المخاطر المحتملة.
4- **تحليل التقرير:** على المؤسسة فحص نتائج التقييم مع الأقسام التنظيمية المختصة برقابة المعلومات لتحديد الخطوات الملائمة والمطلوبة لتصحيح نقاط الضعف التي تم تحديدها في التقييم وفقاً لإمكانيات وموارد المؤسسة.

ويوضح الجدول رقم (1-3) ملخص الإصدار المهنية المرتبطة بالرقابة في نظم المعلومات الالكترونية كما يلي:

جدول رقـم (1-3)

ملخص الإصدارات المهنية المرتبطة بالرقابة في نظم المعلومات الالكترونية

م	الإصدار	هدفه	توصياته
1	**معيار الصادر عن اللجنة الفنية المشتركة التي أسستها كل من المنظمة الدولية للمواصفات القياسية واللجنة الإلكترونية الفنية الدولية 2005-27000.** **(ISO/IEC2700,2005)**	تقديم توصيات حول الممارسات الجيدة في مجال إدارة رقابة المعلومات موجه إلى الأطراف المسئولة عن تحقيق رقابة وأمن نظم المعلومات والحفاظ عليه في المؤسسات.	مجال الرقابة نظم المعلومات الهدف الرئيسي هو سرية، وسلامة، وإتاحة المعلومات المحاسبية. ويتحقق ذلك من خلال تحقيق تسعة أهداف فرعية هي: خفض الخطأ والغش، رقابة الوصول المادي، رقابة الوصول المنطقي، رقابة أمن البيانات، معايير التوثيق، خطة التغلب علي اثار الكارثة، رقابة العمليات الخاصة بالانترنت والاتصالات والمصارف الالكترونية، رقابة أمن النتائج، وأخيراً رقابة أمن خدمات التعهيد.
2	**إرشاد المؤسسة الدولية للمعايير والتكنولوجيا، 2008** **(NIST, 2008)**	يوضح الكيفية التي يتم بها وضح خطط فعالة لتقييم الرقابة من خلال تحديد مجموعة شاملة من الإجراءات التي يجب تنفيذها للحصول على تأكيد لفعالية إجراءات الرقابة المطبقة في أنظمة المعلومات.	عملية وضع وتقييم إجراءات الرقابة تتطلب التحضير والاستعداد سواء من جانب المنظمة أو من جانب الفريق القائم بهذه العملية، يلي ذلك تطوير خطة تقييم إجراءات الرقابة ثم تنفيذ التقييم لإجراءات الرقابة والتحليل والتوثيق وإعداد التقرير وأخيراً تحليل التقرير للقيام بالخطوات التصحيحية اللازمة للتحسين.

يوضح هذا الجدول ملخص الإصدارات المهنية المرتبطة بالرقابة في نظم المعلومات الالكترونية.

3.3 الدراسات المرتبطة بالرقابة في نظم المعلومات الإلكترونية:

يتناول هذا الجزء أهم الدراسات السابقة التي اهتمت بدراسة رقابة نظم المعلومات الالكترونية وهي كما يلي:

- دراسة Jacobs and Weiner (1997):

هدفت الدراسة إلى توضيح دور مراقبي الحسابات في تصميم وتقييم خطط التغلب على آثار الكارثة للمؤسسات الصغيرة والمتوسطة الحجم في الولايات المتحدة الأمريكية، فقد أوضحت الدراسة أن التحدي أمام المراجعين يتمثل في تحديد خطة شاملة للتغلب على آثار الكارثة تكون قابلة للتطبيق في ظل الموارد المادية المنخفضة للمؤسسات الصغيرة والمتوسطة الحجم .

وقد أشارت الدراسة إلى أن المؤسسات كبيرة الحجم والقطاع المصرفي يقومون بتصميم خطط التغلب على آثار الكوارث الملائمة لطبيعة الأعمال وبيئة التشغيل نتيجة لتوافر الموارد المادية، أما المؤسسات الصغيرة والمتوسطة الحجم تقوم بالاعتماد على البرامج الجاهزة المتخصصة لهذا الغرض والتي قد لا تتوافق مع بيئة التشغيل الخاصة بتلك المؤسسات وبالتالي لا توفر احتياجات تلك المؤسسات كما أنها لا تساعد على اكتشاف الإجراءات والسياسات غير الملائمة المتبعة في المؤسسة.

وأوضحت الدراسة أن الخطوات التي يجب أن يقوم بها مراقب الحسابات عند تصميم خطط التغلب على آثار الكارثة هي توثيق كل الوظائف والأفراد والمعدات اللازمة لاستعادة الأعمال بعد حدوث الكارثة، وتحديد وظيفة كل فرد في خطة التغلب على آثار الكارثة وكيفية قيامه بهذه الوظيفة، وتحديد الموردين القادرين على إمداد المؤسسة بالمعدات والأجهزة اللازمة لاستعادة الأعمال، وتحديث خطة التغلب على آثار الكارثة باستمرار في حالة حدوث أي تغيير في الأفراد أو المعدات.

وتوصلت الدراسة إلى أحدى عشر عنصراً يجب تحديدهم لتصميم خطة فعالة للتغلب على آثار الكارثة والتي تضمن خطة شاملة وفقاً لأسوأ كارثة يمكن أن تتعرض لها المؤسسة وهي تحديد الوظائف الهامة والحيوية في المؤسسة وإعداد هيكل هرمي يوضح تسلسل تلك العمليات، وتحديد الأفراد اللازمين لاستعادة الأعمال والوظائف التي سيقومون بتأديتها، وتحديد المعدات والأجهزة اللازمة لاستعادة الأعمال، وتحديد الموقع البديل الذي سيتم من خلاله تأدية الأعمال، وتحديد قائمة بتسلسل المهام التي سيتم القيام بها لاستعادة الأعمال، وتحديد طرق استعادة الملفات

الإلكترونية، وتحديد المستندات المطبوعة الهامة للمؤسسة التي لا يمكن استعادتها إلكترونياً مثل العقود والبيانات المالية، وتحديد المهام الحيوية في عمليات المؤسسة والتي يلزم استعادتها، وتشكيل لجنة طوارئ هي المسئولة عن تنفيذ خطة التغلب على آثار الكارثة، وتحديد قنوات الاتصال مع العاملين والموردين في حالة حدوث الكارثة، وأخيراً تحديد جدول دوري لتحديث خطة التغلب على آثار الكارثة.

- دراسة Wakefield (2000):

استهدفت الدراسة تحديد الإجراءات التي يجب أن تتضمنها السياسات الرقابية حتى يمكن تطويرها مع التغيرات المستمرة في تكنولوجيا المعلومات والتي تمكن المؤسسات المالية في الولايات المتحدة الأمريكية من تحديد التهديدات والمخاطر سواء كانت داخلية أو خارجية، وتحديد الإجراءات التي يجب تطبيقها لتحقيق أمن الشبكات.

وقد أشارت الدراسة إلى أن الاستخدام المتزايد لتكنولوجيا الإنترنت وما ينتج عنها من اختراقات رقابية مثال إنكار الخدمات التي تتعرض للهجوم أو الإفصاح العام عن المعلومات السرية وانتشار فيروسات الحاسب، وهو ما يتسبب في النهاية إلى إحداث خسائر مالية كبيرة يوضح أهمية وضع سياسات رقابية تتضمن الإرشادات الكافية للحد من المخاطر والتهديدات الرقابية على أن يتم مراجعة تلك السياسات والتأكد من التزام العاملين بها.

وتوصلت الدراسة إلي أن السياسة الرقابية لابد وأن تتناول ستة مجالات هي الوصول إلى المعلومات لابد وأن توضح السياسة الرقابية الأشخاص الذين لهم حق الوصول على قواعد بيانات أو ملفات محددة وكيفية تحديد امتيازات الوصول إلى تلك المعلومات وكيفية إدارة الوصول إلى المعلومات (مثال ذلك استخدام كلمات المرور، المكان المادي، فصل الواجبات)، واستدعاء المعلومات لابد وأن توضح السياسة الرقابية الأشخاص الذين لهم حق نسخ المعلومات السرية والإجراءات اللازمة لنسخ المعلومات السرية وما هي الوسائل المصرح بها لاستدعاء المعلومات (مثال ذلك الفاكس، النسخ الورقي، مشاركة الملفات File Sharing)، ونقل المستندات لابد وأن توضح السياسة الرقابية الكيفية التي يتم بها نقل الملفات (مثال ذلك: الإنترنت، الفاكس، نسخ ورقية)، بالإضافة إلى تحديد الأشخاص المسئولين عن نقل المستندات والإجراءات اللازمة للتصريح بنقل المستندات، وكلمات المرور لابد وأن توضح السياسة الرقابية الأشخاص الذين لهم حق الوصول إلى كلمات المرور وتغييرها بالإضافة إلى تحديد الملفات الهامة التي تحتاج إلى تأمينها بكلمات مرور، وتحديد الوقت اللازم لتحديث كلمات المرور، والتقرير عن الحوادث

الأمنية لابد وأن توضح السياسة الرقابية الكيفية التي يتم بها توثيق الحوادث الأمنية والأشخاص الواجب إعلامهم بتلك الحوادث وطرق العلاج المتوفرة للحد من تأثير تلك الحوادث في حالة حدوثها، وأخيراً المراجعة والفحص الدوري لسياسة وإجراءات الرقابة لابد وأن توضح السياسة الرقابية الأشخاص الذين سيقومون بعملية المراجعة وتوقيت الفحص الدوري ونطاق هذا الفحص.

- دراسة Luehlfing (2000):

استهدفت الدراسة أهم تهديدات أمن الحاسب الآلي في المؤسسات المالية لتحديد إجراءات الرقابة التي يمكن استخدامها لمواجهة تلك التهديدات، بالإضافة إلى تحديد الإجراءات التي يمكن من خلالها تحديد المنافع الرقابية.

أوضحت الدراسة أن تهديدات أمن الحاسب تتمثل في خمس أنواع من التهديدات الرقابية هي: كوارث الطبيعة، العاملين غير الشرفاء، العاملين الساخطين على المؤسسة، اختراق الأنظمة من قبل أشخاص خارج المؤسسة، والأخطاء والحذف غير المتعمدة، حيث يتم مواجهة تلك التهديدات من خلال برامج رقابة الأنظمة المتعمدة على خمس خطوات هي تطوير برامج الرقابة في أسرع وقت ممكن للمؤسسة فعلى المؤسسة تطوير الرقابة الخاص بها والاستعداد للاستجابة السريعة لأي انقطاع محتمل للأعمال، مستخدمي أنظمة المعلومات هم العنصر الأساسي لعمليات رقابة الأنظمة لذلك لابد من توضيح الهدف من منع الاختراقات الرقابية، بالإضافة إلى توفير الدعم الكامل من قبل الإدارة العليا للسياسة الرقابية، وتحليل الاختراقات الرقابية وتحديد أسباب هذه الاختراقات هل هي ناتجة عن فشل الأجهزة والبرامج أم هي ناتجة عن انقطاع متعمدة من قبل المؤسسات المنافسة، وعلى المؤسسات الاستعداد للمخاطر الرقابية من خلال تقييم نظم الرقابة لتحديد نقاط الضعف في إجراءات الرقابة والتي يمكن استغلالها في تنفيذ الاختراقات لتحديد إجراءات الرقابة التصحيحية لكل النقاط، وأخيراً الحذر الشديد عند شراء البرامج الجاهزة لان الوضع الرقابي للبرامج الجاهزة يتمثل في قبول كافة الأوامر التي توجه إلى تلك البرامج لذلك يجب تعديل تلك الأوامر لتستجيب إلى امتيازات الوصول التي تحددها المؤسسة لكل مستخدم.

وقد توصلت الدراسة إلى أن وجود هيكل فعال للرقابة يمكن المؤسسة من مواجهة تهديدات أمن الحاسب الآلي ويزيد من أمكانية الاعتماد على الأنظمة، يعتمد نظام الرقابة الفعال لأمن الحاسب الآلي على كلمات المرور، حوائط النار، وتشفير البيانات، وفهم مقاومة الفيروسات مع ضرورة إجراء تقييم مستمر لنظم الرقابة لتحديد نقاط الضعف في تلك النظم وطرق تصحيحها.

أيضاً توصلت الدراسة إلى إمكانية حساب منافع رقابة الأنظمة من خلال حساب الخسائر المحتملة في حالة تدمير تلك الأنظمة، ويتم تحقيق ذلك من خلال تحديد كافة الأنظمة الموجودة بالمؤسسة، يلي ذلك تصنيف تلك الأنظمة من حيث أهميتها في الحفاظ على استمرار عمليات المؤسسة اليومية، حساب الخسائر النقدية المحتملة في حالة فقد كل نظام من أنظمة المؤسسة، وأخيراً مقارنة الخسائر النقدية المحتملة مع تكلفة البرامج لكل نظام معلومات.

- دراسة Fredrik (2001):

هدفت الدراسة إلى تحديد عوامل النجاح اللازمة لتطبيق أنظمة إدارة رقابة المعلومات في بيئة العمل السويدية، وذلك من خلال تطوير مجموعتين من قوائم الاستقصاء إحداهما موجهة إلى المراجعين والثانية إلى أخصائي رقابة المعلومات، وطلب من المراجعين وأخصائي رقابة المعلومات تحديد عوامل النجاح اللازمة لرقابة المعلومات وأهمية تلك العوامل.

وتوصلت الدراسة إلى أن عوامل النجاح اللازمة لتطبيق أنظمة رقابة المعلومات من وجهة نظر المراجعين تتمثل في ستة عوامل هي: التزام الإدارة برقابة المعلومات، وإعداد هيكل جيد لتطبيق نظم رقابة المعلومات، وتوعية جميع العاملين في المؤسسة بالمخاطر الرقابية، وفهم أسباب احتياج المؤسسة لرقابة المعلومات، وقدرة المؤسسة على الاستعانة بخبراء تكنولوجيا المعلومات، بالإضافة إلى تحفيز العاملين على تطبيق سياسات وإجراءات الرقابة. بينما تتمثل عوامل النجاح من وجهة نظر أخصائي أمن المعلومات في ثلاثة وعشرين عاملاً تم تصنيفهم إلى ست مجموعات هي: قدرة المؤسسة على توفير إدارة جيدة لرقابة المعلومات، قدرة المؤسسة على تفويض السلطة اللازمة لإدارة رقابة المعلومات، قدرة المؤسسة على توفير المتطلبات المالية اللازمة لتطبيق نظم رقابة المعلومات، قدرة المؤسسة التحليلية حتى تتمكن الإدارة من تحليل المواقف الرقابية، قدرة المؤسسة على الاتصال المستمر بالعاملين والأطراف الخارجية، وقدرة المؤسسة على تنفيذ السياسات والخطط الموضوعة.

- تقرير Wayna (2002):

استهدف التقرير توضيح سياسة رقابة المعلومات لأحد المصارف بولاية تكساس الأمريكية، حيث تناول الأهداف الرقابية التي يسعى المصرف لتحقيقها والتهديدات الرقابية التي يتعرض لها المصرف، بالإضافة إلى احتمال حدوث كل تهديد من هذه التهديدات والرقابة المطبقة للحد من هذه التهديدات.

وقد أشار التقرير إلى أن السياسة الرقابية للمصرف تسعى لتحقيق ثلاثة أهداف أساسية تتمثل في حماية، وسرية، وإتاحة بيانات العملاء، وتوثيق التهديدات الرقابية المتوقعة في محاولة لتقليل احتمال حدوث هذه التهديدات إلى أدنى حد، بالإضافة إلى المتابعة المستمرة للتعرف على التهديدات الجديدة التي قد تطرأ على بيئة الأعمال.

وقد أوضح التقرير أن التهديدات الرقابية التي تواجه المصرف يمكن حصرها في: سرقة معلومات العملاء السرية، وتدمير بيانات العملاء من قبل مخترقي أنظمة الحاسب، وحدوث صفقات غير مصرح بها في حساب العملاء تمثل اختلاسات من جانب العاملين بالمصرف، وانتهاك سلامة كلمات المرور أما بسبب تبادلها بين العاملين أو بسبب انتهاكات لأمن النظام، بالإضافة إلى فقد بيانات العملاء نتيجة لحدوث حوادث طبيعية وفي ضوء هذه التهديدات تم الإضرار بالإجراءات الرقابية المطبقة من قبل المصرف لمواجهة هذه التهديدات.

- دراسة (مكتب المحاسبة العام،2003) (GAO)، General Accounting Office:

هدفت دراسة مكتب المحاسبة العام (GAO)، بالولايات المتحدة الأمريكية إلى تحديد مدى قيام الإدارة المالية بتقييم المخاطر الرقابية المرتبطة بالمدفوعات التي تتم عن طريق الإنترنت بالإضافة إلى تحديد مدى قيام تلك الإدارة بتوثيق وتطبيق إجراءات الرقابة الملائمة لحماية تلك المدفوعات وذلك من خلال الفترة من أكتوبر 2002 ، وحتى يونيو 2003 .

ولتحقيق الهدف الأول تم فحص وثائق تقييم المخاطر المعدة من قبل إدارة نظام المدفوعات مع عقد مجموعة من المقابلات وفحص إجراءات تقييم الخطر، بينما لتحقيق الهدف الثاني تم تقييم إجراءات الرقابة وفحص وثائق وسياسات الإجراءات الرقابية واختبار تلك الإجراءات أثناء تشغيل تطبيقات نظام المدفوعات بالإضافة إلى فحص التقارير والوثائق الأخرى المتعلقة بتصميم وتطبيق إجراءات الرقابة .

وقد أشارت الدراسة إلى أن هدف الإدارة في أي مؤسسة هو حماية أنظمة المعلومات والبيانات من الوصول غير المصرح به ويتم تحقيق هذا الهدف من خلال تصميم وتطبيق إجراءات الرقابة والتي تهدف إلى منع واكتشاف ومتابعة الوصول الإلكتروني لموارد الحاسب الآلي (البيانات، البرامج، المعدات، التسهيلات)، وبالتالي حماية تلك الموارد من الإفصاح أو

التعديل أو الاستخدام غير المصرح به، وضمان الفصل الجيد للواجبات حتى لا ينفرد شخص واحد بعملية ما من أولها إلى أخرها، وبالتالي تتاح له فرصة ارتكاب تصرفات غير مصرح بها، ومنع استخدام برامج تطبيقية غير مصرح بها أو إجراء تعديلات غير مصرح بها على البرامج المطبقة، وتقليل مخاطر الانقطاع المفاجئ للأعمال ووضع إجراءات استعادة العمليات الهامة بصورة سريعة في حالة حدوث الانقطاع المفاجئ.

وقد أوضحت الدراسة أن تقييم المخاطر المرتبطة بأنظمة المعلومات تمثل العنصر الأساسي في تطوير الرقابة، لما توفره من معلومات تساعد في تحديد إجراءات الرقابة الملائمة ومستوى الرقابة الذي يجب تطبيقه، كما أوضحت الدراسة أن التقييم لإجراءات الرقابة يضمن سرية وإتاحة وسلامة البيانات وأنظمة الحاسب الآلي.

وتوصلت الدراسة إلى أنه على الرغم من تطبيق الإدارة المالية للعديد من إجراءات الرقابة إلا أنه يتم تقييم المخاطر المرتبطة بنظام المدفوعات عن طريق الإنترنت بصورة شاملة وظهرت العديد من نقاط الضعف في الإجراءات التي تم تطبيقها، حيث لم يتم اتخاذ الخطوات اللازمة لتحديد وتناول التهديدات المحتملة للنظام، ويرجع ذلك لعدم اعتقاد المسئولين في تلك الإدارة بأهمية ذلك التقييم، بالإضافة إلى ذلك فإن الإجراءات والسياسات التي تم اتخاذها من قبل الإدارة للحد من المخاطر الرقابية لم تطبق بفعالية مما أدى إلى وجود العديد من نقاط الضعف في تلك الإجراءات.

- دراسة Cerullo (2005):

هدفت الدراسة إلى توفير قواعد إرشادية للمحاسبين وأخصائي نظم المعلومات لتحديد المخاطر الرقابية وتطبيق إجراءات رقابية لإدارة المخاطر في المؤسسات التي تمتاز بتعقد نظم معلوماتها في المملكة المتحدة.

وقد أشارت الدراسة إلى وجود أربعة أنواع من التهديدات هي احتيال الموارد البشرية، والاحتيال غير المتعمد من الموارد البشرية، والتهديدات الناتجة من الحوادث المتعمدة، والتهديدات الناتجة عن الكوارث الطبيعية .

وقد أوضحت الدراسة وجود مدخلين لاختيار إجراءات الرقابة الملائمة هما المدخل الكمي والمدخل النوعي، حيث يركز المدخل الأول على تحديد تكلفة كل إجراء رقابي والمنافع

المترتبة على هذا الإجراء للوصول إلى مزيج مثالي من الإجراءات الرقابية، بينما المدخل النوعي يهتم بتطبيق مدى مقبول من آليات الرقابة.

وتوصلت الدراسة إلى أن الخطوات التي يجب أتباعها لتحديد إجراءات الرقابة هي تحديد المخاطر المحتملة العاملة التي قد تتعرض لها المؤسسة، والمخاطر ذات الأهداف لبيئة المؤسسة، وإجراءات الرقابة التي تحد من تلك المخاطر، اختيار الإجراءات التي تحد من المخاطر ذات الأهمية لبيئة المؤسسة.

- **دراسة (الفرطاس، 2006):**

هدفت الدراسة إلي التعرف علي مدى توفر إجراءات الرقابة الداخلية المحاسبية في الأنظمة الإلية المستخدمة في فروع المصارف التجارية الليبية العامة بمدينة بنغازي، والعوامل التي تعيق توفر إجراءات الرقابة الداخلية المحاسبية، وانحصرت عينة الدراسة في موظفي أقسام المحاسبة، والمراجعة، والحسابات الجارية، والخزينة، والائتمان، والحوالات والصرف الأجنبي، وأقسام الاعتمادات المستندية في فروع المصارف التجارية الليبية بمدينة بنغازي والبالغ عددهم (234) موظفاً.

توصلت الدراسة إلي عدم توفير إجراءات الرقابة الداخلية المحاسبية في الآلية المستخدمة في فروع المصارف التجارية العامة بمدينة بنغازي.

وأظهرت الدراسة إن العوامل التي تعيق توفر إجراءات الرقابة الداخلية المحاسبية بالمصارف قيد الدراسة حسب نسبة الموافقة مرتبة ترتيباً تنازلياً هي علي النحو الأتي:

الترتيب	العوامل التي تعيق توفر إجراءات الرقابة الداخلية المحاسبية	نسبة الموافقة
الأول	انعدام المعرفة بكيفية استخدام هذه الإجراءات الرقابة.	% 81.8
الثاني	عدم الوعي بأهمية هذه الإجراءات، وفائدتها في تحقيق الرقابة.	% 74.9
الثالث	غياب التفكير المنطقي للحاسبات الآلية.	% 67.9
الرابع	تخزين البيانات في صورة غير ورقية.	% 59.9
الخامس	اختصار مسار المراجعة.	% 58.8
السادس	زيادة تعقيد الحاسبات الآلية.	% 57.7
السابع	عدم متابعة إدارة المراجع الداخلية لأنظمة الرقابة الإلكترونية،	% 19.7

	والعمل علي تطويرها.	
الثامن	عدم اهتمام الإدارة العليا باستخدام الحاسوب، والعمل علي تطبيق الإجراءات الرقابية المتعلقة به.	% 18.1

- **دراسة (الشريف، 2006):**

هدفت الدراسة إلي التعرف علي طبيعة المخاطر التي تهدد أمن نظم المعلومات المحاسبية الإلكترونية في المصارف العاملة في قطاع غزة، وأسباب حدوث تلك المخاطر، والتعرف علي إجراءات الحماية للحد من المخاطر التي تهدد نظم معلومات المحاسبية الإلكترونية، والتمييز بين مخاطر أمن المعلومات وعدم كفاية الضوابط الرقابية لأمن تلك النظم، مع التركيز علي مخاطر مخرجات الحاسب الآلي وعدم إهمالها.

وتوصلت الدراسة إلي مجموعة من النتائج والتي تعتبر في مجملها خلاصة التحليلات والمناقشات وهي قلة عدد موظفي تكنولوجيا المعلومات في المصارف حيث يعتمد الفرع علي موظف واحد مهمته تشغيل أنظمة الحاسوب بينما الموظفين المختصين يكون مكانهم في الإدارة العليا، وعدم اتصال شبكة المصارف بشبكة الانترنت وبالتالي عدم تمكن العملاء من إجراء بعض الخدمات المصرفية من خلال الانترنت، والأنظمة المرتبطة مع شبكة الانترنت أكثر عرضه للفيروسات من الأنظمة غير المرتبطة مع شبكة الانترنت، ومخاطر الإدخال غير المتعمد واشتراك الموظفين في كلمة السر وتوجيه البيانات والمعلومات إلي أشخاص غير مصرح لهم بذلك، قد تحدث من مرة شهرياً إلي مرة أسبوعياً، وتطبيق إجراءات أمن النظم المعلوماتية يقلل من إمكانية حدوث مخاطر نظم المعلومات المحاسبية، وأخيراً الإدارة الجيدة تستطيع أن تقلل أو تحد من حدوث المخاطر التي تواجه نظم المعلومات المحاسبية لدى المصارف.

- **دراسة (الدرسي، 2009):**

هدفت الدراسة إلي التعرف علي مستوى إدراك مديري المصارف التجارية الليبية لمخاطر التشغيل المصرفية الإلكترونية، وذلك ضمن فروع المصارف التجارية العاملة في مدينتي طرابلس وبنغازي كعينة مختارة لمديري فروع المصارف التجارية.

وتوصلت الدراسة إلي أن التركيز علي وضع سياسة ثابتة، يتضمن تعيين مديرين مؤهلين علمياً وعملياً بالمجال المصرفي والإلكتروني، علي أن يتم هذا التعيين بعيداً عن المحاباة

والمجاملة، والاهتمام بإقامة دورات تدريبية في مجال مخاطر التشغيل الإلكتروني لمديري الفروع بشكل خاص وموظفي المصرف بشكل عام تعد من قبل خبراء متخصصين من داخل المصارف التجارية وخارجها، وقيام مصرف ليبيا المركزي بترسيخ منهجية ثابتة لجميع المصارف التجارية العاملة تتضمن إلزام هذه المصارف بجعل عملية قياس وتقييم ومراقبة المخاطر التشغيلية سياسة عمل مطبقة وثقافة ثابتة لدى جميع العاملين بالمصرف، وضرورة قيام مصرف ليبيا المركزي بإلزام إدارات المصارف التجارية بتقديم تقارير دورية ومنتظمة تتعلق بإدارتها لمخاطر التشغيل، وتقديم الملاحظات للمصارف التجارية بناءً علي هذه التقارير، وضرورة قيام مصرف ليبيا المركزي بمواكبة ما يستحدث في نطاق إدارة المخاطر المصرفية، ويتطلب ذلك التنسيق وتبادل الآراء مع المصارف المركزية العربية ولجنة بازل للرقابة المصرفية، كذلك ضرورة قيام جميع المصارف التجارية الليبية باستحداث وحدة لإدارة مخاطر التشغيل علي أن تقوم هذه الوحدة برفع تقاريرها إلي الإدارة العليا للمصرف ومنها إلي مصرف ليبيا المركزي، وقيام الجامعات الليبية برفع مستوى التأهيل لمنتسبيها بمواكبة التطورات العالمية في المجالات المختلفة والتطوير في مناهجها تبعاً لذلك حتى يمكن تقليل الفجوة الحادثة بين التعليم والوظيفة، وأخيراً القيام بدراسات لاحقة تعالج مسالة إدارة المخاطر من زوايا أخرى مثل دراسة وسائل الحد من المخاطر التشغيلية، ودراسة إدراك مديري الفروع للأنواع الأخرى من مخاطر التشغيل والتي لم تتناولها هذه الدراسة.

- **دراسة (جل، 2010):**

هدفت الدراسة إلي محاولة التعرف علي مدى فعالية نظم المعلومات المحاسبية في المصارف التجارية العراقية، وبيان تلبيتها لمتطلبات الإدارة للقيام بوظائفها من التخطيط ورقابة واتخاذ القرارات.

وتوصلت الدراسة إلي أن مستوى فاعلية نظم المعلومات المحاسبية تلبي متطلبات عملية الرقابة بدرجة مرتفعة وهذا يسهم بإعطاء انطباع بفاعلية الرقابة ودقة المعلومات المحاسبية، وهو ما تبين من خلال التقارير المالية، وأن عنصري التخطيط والرقابة حصلا علي درجة أهمية أعلي مما حصل عليه عنصر اتخاذ القرارات، وأن عملية الرقابة في نظم المعلومات المحاسبية توفر تقارير رقابية عن أداء المستويات الإدارية المختلفة لتمكين الإدارة من اتخاذ الإجراءات والقرارات التصحيحية.

- **دراسة (حمادة، 2010):**

هدفت الدراسة إلي التعرف علي أثر الضوابط الرقابية العامة لنظم المعلومات المحاسبية الإلكترونية في زيادة موثوقية المعلومات المحاسبية وذلك من خلال التعرف مفهوم موثوقية المعلومات المحاسبية وخصائصها، ومن ثم التعرف علي مفهوم الضوابط الرقابية العامة لنظم المعلومات المحاسبية الإلكترونية ومكوناتها من ضوابط تنظيمية، وضوابط الرقابة علي الوصول، وضوابط الرقابة علي أمن وحماية الملفات، وضوابط توثيق وتطوير النظام.

كما هدفت إلي التعرف علي رأي مراجعي الحسابات الخارجيين بمدينة دمشق حول أثر الضوابط الرقابية العامة لنظم المعلومات المحاسبية الإلكترونية في زيادة موثوقية المعلومات المحاسبية.

وتوصلت الدراسة إلي أن للضوابط الرقابية وتوثيق النظام وتطويره أثر كبير في زيادة موثوقية المعلومات المحاسبية وكذلك لها أثر كبير علي أمن الملفات وحمايتها، ولها أثر متوسط في الوصول إلي نظم المعلومات الإلكترونية.

- **دراسة (الحكيم، 2010):**

هدفت الدراسة إلي إمكانية القيام بتقييم بنية الرقابة الداخلية من قبل مفتشي جهاز المركزي للرقابة المالية في سوريا عند قيامهم بعملية مراجعة المؤسسات الاقتصادية التي تستخدم نظم المعلومات المحاسبية وفق معايير الرقابة علي نظم المعلومات، بما يتناسب والتطور الحاصل في مجال استخدام تقنية المعلومات في النظم المحاسبية.

وتوصلت الدراسة إلي أن تضمين قوانين الرقابة علي المؤسسات العامة قوانين تلزم مفتش الحسابات بإجراء رقابة علي نظم المعلومات المحاسبية وذلك ليتناسب مع التطور الحاصل في المؤسسات العامة في مجال إدخال تقنية المعلومات، ونشر الوعي بين مفتشي الحسابات بضرورة إجراء الرقابة علي نظم المعلومات المحاسبية وبضرورة العمل علي استخدام احدث الأساليب الرقابية لتحقيق ذلك، وتدريب وتأهيل مفتشي الحسابات علي التقنيات والمهارات التي تمكنهم من إجراء الرقابة علي نظم المعلومات المحاسبية فضلاً عن الرقابة علي البيانات وإجراء دورات تدريبية دائمة وندوات لتطوير مهاراتهم الرقابية، وتشكيل لجنة رقابية مهمتها تطوير الإجراءات الرقابية علي نظم المعلومات المالية والمحاسبية باستمرار، وقيام المفتش بالطلب من الإدارة بتزويده بنسخ عن مصفوفة العبور أي المصفوفة التي تبين صلاحيات المستخدمين في الوصول

إلي البيانات موضوعة ومرخصة من قبل مجلس الإدارة في المؤسسة ومراجعة مدى الالتزام بهذه المصفوفة، ورقابة الوسائل اللازمة لحفظ البيانات وتخزينها من نسخ احتياطية وصيانة وقائية، وقيام مراجع الحسابات بمراجعة عمل ومعالجة وتطوير النظام من خلال مراجعة وثائق التوثيق الخاصة بنظام المعلومات، والتأكد من أن قسم المراجعة الداخلية يقوم بالعناية المهنية المطلوبة للرقابة علي نظم المعلومات في المنظمة ومدى تحقيقه لعوامل الأمان والالتزام بالقوانين وانسجامه مع خطط الطويلة وقصيرة الأمد وإستراتجيتها العامة، والتأكد من حذف اسم وكلمة مرور الموظف الذي ترك العمل أو الذي نقل إلي قسم أخر فوراً في وقت وقوع الحدث، وحصر إمكانية تعديل البيانات وحذفها في مجموعة محددة ومرخص لها من المستخدمين مع تحديد البرنامج لتاريخ التعديل ومن قام به.

يوضح الجدول رقم (2-3) ملخص الدراسات السابقة المرتبطة برقابة نظم المعلومات الالكترونية كما يلي:

جدول رقـم (2-3)

ملخص الدراسات السابقة المرتبطة برقابة نظم المعلومات الالكترونية

م	الدراسة	هدف الدراسة	نتائج الدراسة
1	دراســـــــة Jacobs and Weiner (1997)	توضيح دور مراقبي الحسابات في تصميم وتقييم خطط التغلب علي آثار الكارثة في ظل الموارد المادية المنخفضة للمؤسسات صغيرة ومتوسطة الحجم.	توصلت الدراسة إلي إحدى عشر عنصرا يجب تحديدهن لتصميم خطة فعالة للتغلب علي آثار الكارثة وهي: تحديد الوظائف، وتحديد الإفراد اللازمين، تحديد المعدات، تحديد الموقع، تحديد قائمة المهام، طرق استعادة الملفات الالكترونية، تحديد المستندات المطبوعة الهامة، تحديد المهام الحيوية، تشكيل لجنة طوارئ، تحديد قنوات الاتصال، تحديد جدول دوري لتحديث الخطة.
2	دراســـــــة Wakefield (2000)	تطوير سياسات رقابية تواكب التغيرات المستمرة في تكنولوجيا المعلومات وتحديد التهديدات والإجراءات التي يجب تطبيقها لتحقق أمن الشبكات.	توصلت الدراسة آلي أن السياسة الرقابية لابد أن تتناول ستة مجالات هي الوصول إلي المعلومات، واستدعاء المعلومات، ونقل المستندات، وكلمات المرور، والتقرير عن الحوادث الرقابية، وخيرا المراجعة والفحص الدوري.
3	دراســـــــة Luehlfing (2000)	التعرف علي التهديدات الرقابية لأمن الحاسب الآلي، وتحديد الإجراءات التي يمكن من خلالها تحديد المنافع الرقابية.	تهديدات امن الحاسب خمسة هي: الكوارث الطبيعية، العاملين غير الشرفاء، العاملين الساخطين، اختراق الأنظمة من الخارج، الأخطاء والحذف غير المتعمدة.
4	دراســـــــة Fredrik (2001)	تحديد عوامل النجاح لتطبيق أنظمة رقابة نظم المعلومات المحاسبية.	عوامل النجاح اللازمة لتطبيق أنظمة رقابة من وجهة المراجعين هي التزام الإدارة، إعداد هيكل جيد للرقابة، توعية العاملين، فهم احتياجات الرقابة، الاستعانة بخبراء تكنولوجيا المعلومات، تحفيز العاملين. إما من وجهة نظر أخصائي الحاسب الآلي هي قدرة المؤسسة الإدارية، تفويض السلطات، القدرة المالية، القدرة التحليلية، الاتصال بالعاملين

			والإطراف الخارجية، تنفيذ السياسات المخطط لها.
5	تقرير (2002) Wayna	توضيح سياسة رقابة نظم المعلومات لأحد المصارف الأمريكية بالإضافة إلي التهديدات الرقابية والحد منها.	السياسة الرقابية تسعى لتحقيق ثلاثة أهداف هي حماية وسرية وإتاحة البيانات، توثيق التهديدات المتوقعة، المتابعة المستمرة للتهديدات الجديدة.
6	دراسة (2003) GAO	تحديد مدى قيام الإدارة المالية بقياس المخاطر الرقابية المرتبطة بالانترنت والإجراءات الرقابية لحمايتها.	أظهرت الإدارة المالية العديد من نقاط الضعف في الإجراءات الرقابية المطبقة ويرجع ذلك لعدم اعتقاد المسئولين بأهمية ذلك.
7	دراسة (2005) Cerullo	توفير قواعد إرشادية للمحاسبين وأخصائي نظم المعلومات لتطبيق إجراءات رقابية في المؤسسات التي تمتاز بتعقد نظم معلوماتها.	وجود مدخلين لاختيار الإجراءات الرقابية الملائمة هما المدخل الكمي الذي يركز علي تكلفة الإجراء الرقابي ومنافعه، والمدخل النوعي الذي يركز بتطبيق مدى مقبول من الإجراءات الرقابية.
8	دراسة (الفرطاس، 2006)	التعرف علي مدى توفر إجراءات الرقابة الداخلية المحاسبية في الأنظمة الإلية المستخدمة في المصارف التجارية الليبية بمدينة بنغازي، والعوامل التي تعيق توفر هذه الإجراءات.	عدم توفر إجراءات الرقابة الداخلية المحاسبية في الأنظمة الإلية، والعوامل التي تعيق توفر هذه الإجراءات هي: انعدام المعرفة، عدم الوعي، غياب التفكير المنطقي للحاسبات، تخزين البيانات في صورة غير ورقية، اختصار مسار المراجعة، زيادة تعقيد الحاسبات، عدم المتابعة من إدارة المراجعة الداخلية، عدم اهتمام الدارة العليا.
9	دراسة (الشريف، 2006)	التعرف علي المخاطر التي تهدد أمن نظم المعلومات في المصارف، والإجراءات الرقابية للحد من هذه المخاطر.	قلة موظفي تكنولوجيا المعلومات في المصارف مما يزيد من هذه المخاطر، وان تطبيق الإجراءات الرقابية يقلل من حدوثها.
10	دراسة (الدرسي، 2009)	التعرف علي مستوى إدراك مديري المصارف لمخاطر التشغيل المصرفية الالكترونية.	ضرورة وضع سياسة ثابتة في تعيين مديرين مؤهلين علميا وعمليا، وإقامة دورات تدريبية في مجال مخاطر التشغيل وعملية قياسها وتقييمها ومراقبتها.
11	دراسة (جل، 2010)	التعرف علي مدى فعالية نظم المعلومات في تلبية متطلبات الإدارة للقيام بوظائفه التخطيطية والرقابية في اتخاذ القرارات.	تلبي متطلبات عملية الرقابة والتخطيط بدرجة مرتفعة، وتوفر تقارير رقابية عن أداء المستويات الإدارية المختلفة.
		التعرف علي اثر الضوابط	لها كبير في زيادة موثوقية

12	دراســـــــــة (حمادة، 2010)	الرقابية العامة لنظم المعلومات في زيادة موثوقية المعلومات المحاسبية.	المعلومات المحاسبية وامن الملفات وحمايتها، واثر متوسط في الوصول إلي نظم المعلومات المحاسبية.
13	دراســـــــــة (الحكيم، 2010)	تقييم بنية الرقابة للمؤسسات الاقتصادية التي تستخدم نظم المعلومات المحاسبية من قبل مفتشي جهاز المركزي للرقابة المالية.	تشكيل لجنة رقابية لتطوير الإجراءات الرقابية، عدم وعي المؤسسات بضرورة باستخدام احدث الأساليب الرقابية وضعف تأهيلهم وتدريبهم علي التقنيات والمهارات الرقابية.

يوضح هذا الجدول ملخص الدراسات السابقة المرتبطة بالرقابة في نظم المعلومات الالكترونية

3.4 الخلاصــة:

إن الالتزام بمعايير رقابة البيانات والمعلومات التي ظهرت علي المستوى الدولي خاصة المعيار (ISO-IEUC 27000-2005)، والحصول علي شهادات تثبت ذلك الالتزام يعد من الاتجاهات الرئيسية الحديثة التي تميز العصر الحالي، لما يحققه من مزايا تنافسية للمؤسسات عن طريق تشجيع مختلف الإطراف علي التعامل مع المؤسسة لثقتهم في أمن أنظمة معلوماتها وبالتالي الحفاظ علي سرية المعلومات الخاصة بهم، لذا تناول هذا الفصل أهم الإصدارات والإرشادات واستقراء الدراسات المرتبطة برقابة نظم المعلومات الالكترونية.

ويخلص هذا الفصل إن عملية وضع إجراءات الرقابة تتطلب التحضير والاستعداد سواء من جانب المنظمة أو من جانب الفريق القائم بهذه العملية، يلي ذلك تطوير خطة تقييم إجراءات الرقابة ثم تنفيذ التقييم لإجراءات الرقابة والتحليل والتوثيق وإعداد التقرير وأخيراً تحليل التقرير للقيام بالخطوات التصحيحية اللازمة للتحسين، كما يمكن الحكم علي مدى ملائمة إجراءات الرقابة من خلال تحديد تأثير تلك الإجراءات علي التكاليف المرتبطة بارتكاب الاختراقات والمخاطر الرقابية بالإضافة إلي التأثير علي المنافع التي يمكن أن يحصل عليها الفرد من ارتكاب هذه الاختراقات.

ويستعرض الفصل التالي الدراسة العملية وتوضيح مجتمع وعينة الدراسة، وتحليل البيانات التي تم تجميعها، بهدف اختبار فرضيات الدراسة باستخدام الأساليب الإحصائية المناسبة.

الفصل الرابـــــــــــع:

تجميــع وتحليـل البيانــات

4.1 المقدمــة:

في الفصل السابق تم التعرف علي أهم الإصدارات المهنية، والدراسات السابقة المرتبطة بالرقابة في نظم المعلومات الالكترونية، وسيتناول هذا الفصل تحليل البيانات الدراسة المجمعة باستمارة الاستبيان واختبار الفرضيات، ومن ثم قبولها أو رفضها بناءً علي نتائج التحليل الإحصائي، وكذلك تحليل بيانات الدراسة المجمعة بالملاحظة، فقد تناول الجزء الثاني منهجية الدراسة، وتناول الجزء الثالث مجتمع وعينة الدراسة، أما الجزء الرابع فقد تناول كيفية تجيع بيانات الدراسة، وخصص الجزء الخامس لاختبار الصدق والثبات، وكان الجزء السادس حول اختبار التوزيع الطبيعي، والتحليل الوصفي لعينة الدراسة فخصص له الجزء السابع، أما الجزء الثامن فقد خصص لعرض الكيفية التي تحليل بيانات الدراسة، في حين اهتم الجزء الأخير بعرض خلاص الفصل.

4.2 منهجيــة الدراســة:

تهدف الدراسة إلي معرفة واقع الرقابة في المنظومة المصرفية الموحدة في المصارف الليبية وبذلك تصنف الدراسة بأنها دراسة استكشافية بناءً علي هدفها، وذلك من خلال قيامها باستكشاف الظاهرة محل الدراسة، بالاعتماد علي البيانات التي تم تجميعها للدراسة بواسطة أداتي جمع البيانات المتمثلة في الاستبيان والملاحظة، حيث تم استخدام استمارة الاستبيان وجهاً لوجه بشكل يعطي فهم حقيقي لمشكلة الدراسة، وتجميع بيانات أكثر دقة وبالتالي تقليل الأخطاء، وتم تدوين الإجابات ومراجعتها مباشرة حتى يتم التأكد من عدم فقد أي معلومة، ثم تجميع بيانات الملاحظة من واقع العمل المصرفي، ومن ثم تحليل هذه البيانات باستخدام الأساليب الإحصائية المناسبة، للحصول علي نتائج الدراسة.

وأما من حيث الإجراءات المتبعة فتصنف الدراسة بأنها دراسة كمية، والحقائق التي تم تجميعها للدراسة تتسم بالوجود المادي الظاهر وذلك من خلال التطبيقات الرقابية الظاهرة بالمنظومة المصرفية الموحدة بالمصارف الليبية، وبناءً علي ذلك تم تبني النموذج الوظيفي (Functionalist Paradigm)[9]، الذي يهتم بالاستقصاءات (التحقيقات)، للعالــم الاجتماعــي

[9]- يهتم هذا النموذج بالممارسة العلمية القائمة علي افتراضات الناس عن العالم وطبيعة المعرفة وهو يقدم إطار عام يشمل مجموعة من النظريات والأساليب والطرق لتحديد البيانات (Hussey and Hussy, 1997).

باستخدام علم الوجود الواقعي[10]، ونظرية المعرفة الايجابية[11]، وحتمية وجهة النظر للطبيعة البشرية[12]، ووجهة نظر منهجية البحث الطبيعية[13]، ويرجع اختيار النموذج الوظيفي إلي الأسباب التالية (الفيتورى، 2007):

1- البيانات التي تم جمعها لإغراض هذه الدراسة تتصف بالوجود المادي الظاهر ويمكن التحقق من وجودها بشكل موضوعي وملموس.
2- المعرفة المتعلقة بهذه البيانات هي معرفة مستقلة عن الإفراد.
3- سلوك أفراد العينة وإجاباتهم نابعة من بيئة أعمالهم وليس مجرد وجهات نظر فقط.

4.3 مجتمع وعينــة الدراســة:

تمثل مجتمع الدراسة في المصارف التي تطبق المنظومة المصرفية الموحدة في بيئة العمل الليبية، لعدة فروع من مصارف شمال أفريقيا، والوحدة، والجمهورية، بمختلف مدن ليبيا.

وتم استبعاد المصارف التي رفضت إجراء هذه الدراسة لاعتقادهم أن هذه الدراسة تمثل تهديداً لأنظمة الرقابة الخاصة بها مثل بعض فروع مصرف الجمهورية والوحدة، وكذلك المصارف التي أوقفت العمل بالمنظومة المصرفية الموحدة مثل مصرف التجاري الوطني، أو لم تعمل أساساً بها مثل مصرف الصحاري، ومصرف التجارة والتنمية، ومصرف الأمان، ومصرف الإجماع العربي.

ولاختبار فرضيات الدراسة تم استخدام عينة[14]من الإطراف التي تهتم بمشكلة الدراسة وهم المراجعين الداخليين، ومشرفين المنظومة، ويرجع سبب اختيارهما لإلمامهما بظروف القطاع

---

[10]- علم الوجود الواقعي: علم أو دراسة الوجود أي أنه يهتم بدراسة طبيعة الواقعية، وعما إذا كانت الواقعية ظاهرية للفرد لا بديلاً عن الشعور الفردي (Crott, 1998).

[11]- نظرية المعرفة الايجابية: تهتم بطبيعة المعرفة، وأشكالها التي تتخذها، وكيف يتم تجميعها، وتعتبر الطريق لفهم وشرح المعرفة البشرية، وتوجد بصورة مستقلة عن الأفراد وهي مبنية علي طرق وأساليب تقليدية تسيطر علي البحث العلمي (Crott, 1998).

[12]- طبيعة البشر: يقصد بها العلاقة بين الجنس البشري وبيئته، أي أن الإفراد وتصرفاتهم نابعة من البيئة المحيطة بهم أو العكس هم الذين يصنعون بيئتهم (Burrell and Morgan, 1979).

[13]- المنهجية الطبيعية: أسلوب فطري يؤسس لفهم العالم الاجتماعي باستخدام مؤشرات، علم الوجود الواقعي، ونظرية المعرفة الايجابية، وطبيعة البشر (Hopper and Powell,1985: Burrell and Morgan, 1979).

[14]- عينة الدراسة: تم الاعتماد علي دراسة (Fredrik, 2001) في تحديد عينة الدراسة وهم المراجعين الداخليين ومشرفي المنظومة، لإلمامهما بعوامل النجاح اللازمة لتطبيق أنظمة رقابة المعلومات في بيئة العمل السويدية.

المصرفي الليبي والتهديدات الرقابية التي يتعرض لها هذا القطاع، وأيضاً علاقتهما المباشرة بموضوع الدراسة، وقد بلغ إجمالي عدد العينة (45) مفردة موزعة علي عدد (15) فرع مصرفي.

4.4 تجميع بيانــات الدراســة:

تعتبر عملية جمع البيانات مرحلة أساسية ومتقدمة من مراحل العملية البحثية ويقوم الباحث بجمع البيانات التي يحتاجها في إطار دراسته، أما ميدانياً من خلال الاستبيان والملاحظة، أو من خلال الوسائل غير الميدانية كالإحصائيات والوثائق وغيرها من الوسائل المكتبية المختلفة (خشيم، 2002).

وبما أن استمارة الاستبيان تمثل وسيلة تجميع بيانات يمكن استخدامها في كل من البحوث الكمية والنوعية علي حد سواء، فقد تم استخدام استمارة الاستبيان (وجهاً لوجه)[15] كأداة لجمع البيانات والمعلومات اللازمة لهذه الدراسة، وذلك لكونه أسلوب علمي يطبق ويلتزم فيه بقواعد البحث العلمي، وخصوصاً فيما يتعلق بالصلة التي تربط أسئلة الاستبيان بفرضيات الدراسة، لقبول أو رفض هذه الفرضيات، بالإضافة إلي ما تتميز به استمارة الاستبيان وجهاً لوجه من توفير الإيضاحات الكافية وشرح طبيعة الأسئلة وإعطاء معلومات إضافية لتقديم فهم حقيقي لمشكلة الدراسة وبالتالي تقليل الأخطاء مع التأكيد على سرية المعلومات التي سيتم الحصول عليها واستخدامها لإغراض البحث العلمي.

وفيما يتعلق بالتقسيمات الأساسية لاستمارة الاستبيان، فتكونت من جزئين كالتالي:

الجزء الأول:

يتناول هذا الجزء معلومات شخصية عن عينة الدراسة كالمركز الوظيفي، والمؤهل العلمي، وعدد سنوات الخبرة، وعدد الدورات التدريبية في مجال العمل المصرفي، وأسم المصرف والفرع والمدينة.

[15]- الاستبيان وجهاً لوجه: تم تقديم استمارة الاستبيان للمبحوثين المشاركين في الدراسة للإجابة علي أسئلة الاستبيان بشكل مباشر، دون استخدام وسائل الاتصال الأخرى (مثل: البريد أو الفاكس)، مع تقديم الباحث فهم لمشكلة الدراسة وتوفير الإيضاحات الكافية وشرح طبيعة الأسئلة، شرط أن يتم ذلك دون تحيز أو تضليل.

الجزء الثاني:

وقد خصص هذا الجزء لجمع البيانات والمعلومات المتعلقة باختبار فرضيات الدراسة، وتكون هذا الجزء من تسعة مجموعات وهي كما يلي:

المجموعة الأولى: آليات رقابة خفض الخطأ والغش، مكونة من (5) أسئلة.

المجموعة الثانية: آليات رقابة الوصول المادي، مكونة من (5) أسئلة.

المجموعة الثالثة: آليات الوصول المنطقي، مكونة من (17) سؤال.

المجموعة الرابعة: آليات رقابة أمن البيانات، مكونة من (11) سؤال.

المجموعة الخامسة: آليات رقابة معايير التوثيق، مكونة من (3) أسئلة.

المجموعة السادسة: آليات رقابة التغلب علي آثار الكارثة، مكونة من (9) أسئلة.

المجموعة السابعة: آليات رقابة الاختراقات الأمنية في عمليات التجارة الالكترونية والاتصالات والانترنت، مكونة من (9) أسئلة.

المجموعة الثامنة: آليات رقابة أمن النتائج، مكونة من (5) أسئلة.

المجموعة التاسعة: آليات رقابة أمن خدمات التعهيد، (5) أسئلة.

وبذلك يكون المجموع الكلي للأسئلة (69) سؤال.

بالإضافة إلي استخدام استمارة الاستبيان وجهاً لوجه كأداة لجمع البيانات، اعتمدت الدراسة أيضاً في جمع بياناتها علي الملاحظة[16] كأداة أساسية ثانية، وذلك لكونها أكثر وسائل جمع البيانات فائدة للتعرف علي الظاهرة، وعدم الاعتماد علي إجابات أفراد العينة المشاركين في الدراسة، وهذا ما يمكن من الإلمام بمشكلة الدراسة، وبذلك تكون ألأداتين أكثر واقعية للحصول علي بيانات الدراسة.

[16]- الملاحظة: تم تجميع بيانات الملاحظة وذلك وفقاً للمجموعات التسعة في استمارة الاستبيان، بمعني تم تجميع بيانات الملاحظة للتأكد من تطبيق آليات الرقابة الواردة في الاستبيان وبالتالي مقارنة نتائج الاستبيان مع نتائج الملاحظة وذلك لمعرفة أوجه الاختلاف بين نتائج الأداتين.

بعد تحديد مجتمع وعينة الدراسة تم التعامل مع مجموعتان من المفردات، بالنسبة للمجموعة الأولي استمارة الاستبيان وهي تمثل المراجعين الداخليين ومشرفي المنظومة المصرفية الموحدة في القطاع المصرفي من ذوي الخبرة، رغم صعوبة الحصول علي أكبر قدر من البيانات نتيجة رفض أغلب المصارف الليبية للمشاركة بالدراسة لاعتقادهم بأن موضوع ومشكلة الدراسة من الموضوعات الحساسة والسرية، حيث تم تجميع البيانات باستخدام استمارة الاستبيان أولاً وذلك خلال الفترة من (05- 01- 2013) إلي (27- 02- 2013)، وتم تجميع عدد (30) استمارة استبيان موزعة بالتساوي علي المراجعين الداخليين ومشرفي المنظومة، أي عدد (15) استمارة استبيان للمراجعين الداخليين، وعدد (15) استمارة استبيان لمشرفي المنظومة، وقد استغرق ملء كل استمارة في المتوسط (40) دقيقة، مع تقديم شرح مختصر لبعض المفاهيم التي قد تبدو غامضة لإفراد العينة بسبب حداثة موضوع الدراسة في بيئة الممارسة المهنية في المصارف الليبية مع مراعاة تفادي إعطاء أي انطباعات سواء كانت ايجابية أو سلبية لإفراد العينة.

أما المجموعة الثانية تتمثل في أداة جمع بيانات الدراسة بالملاحظة، بعد الانتهاء من تجميع بيانات استمارة الاستبيان (وجهاً لوجه) في عدد (15) فرع مصرفي تم الرجوع إلي هذه الفروع لتجميع بيانات الدراسة بالأداة الثانية وهي الملاحظة، حيث تم الاعتماد علي الأسئلة الواردة في الاستبيان كأساس لتجميع الملاحظة وذلك من خلال المشاهدة الشخصية لآليات الرقابة المطبقة من واقع العمل المصرفي، وذلك لمقارنة نتائج الاستبيان مع نتائج الملاحظة، بهدف التوصل إلي نتائج أكثر واقعية وموضوعية، وقد بلغت مفردات الملاحظة (15) مفردة لعدد (15) فرع مصرفي، وبالتالي بلغ إجمالي عدد العينة (45) مفردة .

4.5 صدق وثبـات البيانـــات Reliability Analysis:

يعتبر اختبار "ألفا كرونباخ" Alpha Cronbach أحد الاختبارات الإحصائية الهامة لتحليل بيانات الدراسة للمجموعة الأولي المتمثلة في استمارة الاستبيان الموجهة للمراجعين الداخليين ومشرفي المنظومة، حيث إن الصدق مظهر الثبات، بمعنى أن المقياس الصادق يكون ثابتاً وليس العكس، فقد يكون الاختبار ثابتاً ولكنه لا يتمتع بالصدق، ويعرف الثبات بأنه مؤشر علي درجة الدقة أو الضبط في عملية القياس إذا ما طبق أكثر من مرة تحت ظروف مماثلة، وتم استخدام هذه الاختبار للتأكد من مدى ترابط الأسئلة التي احتوتها استمارة الاستبيان، وموثوقية الإجابات المتحصل عليها وذلك لكل فرضية فرعية على حدا، ولكل مجموعة علي حدا (الطيب،

1999; اللافي، 2006)، وكانت نتائـج الاختبار كما يوضحها الجدول رقـم (1-4)، والجدول رقـم (2-4):

جدول رقـم (1-4)

اختبـار الصـدق والثبـات للفرضيـات الفرعيـة للدراسـة

ت	الفرضيات الفرعية للدراسة	الدرجة الكلية لمعامل الثبات	الدرجة الكلية لمعامل الصدق	التعليق
1	آليات رقابة خفض الخطأ والغش.	0.709	0.842	مقبول إحصائياً
2	آليات رقابة الوصول المادي.	0.696	0.834	مقبول إحصائياً
3	آليات رقابة الوصول المنطقي.	0.888	0.942	مقبول إحصائياً
4	آليات رقابة أمن البيانات.	0.861	0.928	مقبول إحصائياً
5	آليات رقابة معايير التوثيق.	0.729	0.854	مقبول إحصائياً
6	آليات خطة التغلب على آثار الكارثة.	0.840	0.917	مقبول إحصائياً
7	آليات الرقابة الخاصة بالإنترنت والاتصالات والمصارف الالكترونية.	0.796	0.892	مقبول إحصائياً
8	آليات رقابة أمن النتائج.	0.749	0.865	مقبول إحصائياً
9	آليات أمن خدمات التعهيد.	0.712	0.844	مقبول إحصائياً

يوضح هذا الجدول نتائج اختبار الصدق والثبات عند مستوى (0.6).

جدول رقـم (2-4)

اختبار الصدق والثبات حسب المجموعات المشاركة في الدراسة

ت	المستهدفين بالدراسة	معامل الثبات	معامل الصدق	التـعليـق
1	المراجعين الداخليين	0.971	0.985	مقبول إحصائياً
2	مشرفي المنظومة	0.965	0.982	مقبول إحصائياً

يوضح هذا الجدول نتائج اختبار الصدق والثبات عند مستوى (0.6).

من خلال الجدولين السابقين يلاحظ أن جميع معاملات الثبات التي تم الحصول عليها كانت مقبولة إحصائياً، ويدل ذلك علي وجود ترابط بين الأسئلة المتعلقة بكل فرضية فرعية علي

حدا، وكل مجموعة من المجموعات المشاركين في الدراسة علي حدا، وأن الإجابات المتحصل عليها قد حققت نسب مقبولة إحصائياً، حيث تعتبر أصغر قيمة مقبولة لـ ألفا هي (0.6)، وأفضل قيمة مقبولة تقع بين (0.7)، و (0.8)، وكلما زادت عن ذلك يدل علي أن بيانات الدراسة ذات ثبات وموثوقية عالية (البياتي، 2005:ص 50).

4.6 اختبار التوزيع الطبيعي Normality Distribution Test:

تم استخدام اختبار كولمجوروف سمرنوف "Kolmogorov- Smirnov Test" لاختبار ما إذا كانت بيانات الدراسة تتبع التوزيع الطبيعي من عدمه وذلك بالنسبة لاستمارة الاستبيان حيث بلغت القيمة الاحتمالية المحسوبة لمتوسطات إجابات المراجعين الداخليين ومشرفي المنظومة (0.280)، (0.312)، وهي أعلى من مستوى المعنوية (0.05) وهذا يعني أن البيانات المتحصل عليها تتبع التوزيع الطبيعي[17]، لذلك تم استخدام أدوات الإحصاء المعلمي لاختبار بيانات الدراسة.

4.7 التحليـل الوصفـي Descriptive Analysis:

تم استخـدام هذا الأسلوب للتعرف علي خصـائص ومعـالم عينة الدراســة ووصفها، من خــلال استخـلاص بعض المؤشـرات الإحصـائية، وبنــاءً علي ذلك قُسـم هذا الجزء من التحليل إلي ثلاث أقسام كالتالي:

القسم الأول: خصص هذا القسم لتحليل بيانات الجزء الأول من استمارة الاستبيان للمراجعين الداخليين، والذي يتضمن معلومات عامة عن العينة محل الدراسة.

القسم الثاني: تناول هذا القسم تحليل بيانات الجزء الأول من استمارة الاستبيان لمشرفي المنظومة، والذي يتضمن معلومات عامة عن العينة محل الدراسة.

القسم الثالث: أما هذا القسم فقد خصص لتحليل بيانات المصارف المشاركة في الدراسة، والذي يتضمن معلومات عامة عن فروع المصارف المشاركة والتوزيع الجغرافي لها.

---

[17]- بيانات الدراسة تخضع للتوزيع الطبيعي عند مستوى الدلالة ألفا (0.05) ولمزيد من الإيضاح حول اختبار التوزيع الطبيعي لبيانات الدراسة انظر ملحق رقم (3).

4.7.1 تحليل الجزء الأول من استمارة الاستبيان للمراجعين الداخليين:

تضمن تحليل الجزء الأول من استمارة الاستبيان تحليل البيانات المتعلقة بالمراجعين الداخليين المشاركين في الدراسة، من حيث المركز الوظيفي، المؤهل العلمي والتخصص، عدد سنوات العمل في مجال المصارف، بالإضافة إلي مدى مشاركتهم في الدورات التدريبية في مجال العمل المصرفي، وذلك وفقاً للتسلسل التالي:

أولاً: المركز الوظيفي للمراجعين الداخليين المشاركين في الدراسة:

يتضح من الجدول رقم (3-4) أن نسبة رؤساء أقسام المراجعة الداخلية الذين قاموا بالإجابة علي استمارات الاستبيان بلغت (13%) من أجمالي المشاركين، في حين بلغت نسبة من يشغلون وظيفة مراجع داخلي أو موظفين بقسم المراجعة الداخلية بلغت (87%)، وهذا يعطي قدراً معقولاً من الثقة في البيانات المتحصل عليها.

جدول رقــم (3-4)

توزيع المراجعين الداخليين المشاركين حسب المركز الوظيفي

المركز الوظيفي	العدد	النسبة %
رئيس قسم المراجعة	2	%13.0
مراجع داخلي	13	%87.0
المجموع	15	%100

يوضح هذا الجدول توزيع المشاركين في الدراسة حسب العدد والنسبة.

ثانياً: المؤهل العلمي للمراجعين الداخليين المشاركين في الدراسة:

يلعب التأهيل العلمي دوراً هاما في الرفع من مستوى الأداء في كافة المجالات وبشكل خاص في مجال المصارف، باعتبار أن طبيعة العمل المصرفي ذات أهمية بالغة وينبغي أن يؤديها أشخاص علي قدر كاف من التأهيل العلمي في مجال المحاسبة والجدول رقم (4-4) يوضح توزيع المراجعين الداخليين المشاركين في الدراسة بحسب التأهيل العلمي:

جـدول رقـــم (4-4)

توزيع المراجعين الداخليين المشاركين حسب المؤهل العلمي

المؤهل العلمي للمراجعين الداخليين	العدد	النسبة%
ماجستير محاسبة	1	%6.5
بكالوريوس محاسبة	13	%87
بكالوريوس تمويل ومصارف	1	%6.5
المجموع	15	100%

يوضح هذا الجدول توزيع المراجعين الداخليين المشاركين في الدراسة حسب العدد والنسبة.

يلاحظ من الجدول أن واحد فقط يحمل ماجستير محاسبة، و(87%) من المراجعين الداخليين المشاركين في الدراسة هم من حملة بكالوريوس محاسبة، وكذلك واحد فقط يحمل بكالوريوس تمويل ومصارف، ويلاحظ أن كل المشاركين في الدراسة يحملون مؤهلات علمية الأمر الذي يسهل من عملية استيعاب وفهم متطلبات الرقابة في نظم المعلومات الالكترونية وإمكانية الحصول علي بيانات مناسبة لدراسة الموضوع.

ثالثاً: عدد الدورات التدريبية للمراجعين الداخليين المشاركين في الدراسة:

يهتم هذا الجزء بمدى قيام المصارف بتدريب موظفيها وكذلك مدى حصول المشاركين في الدراسة على دورات تدريبية في مجال عملهم ويمكن من خلال الجدول رقم (4-5) توضيح نسبة وعدد المراجعين الداخليين المشاركين في الدورات التدريبية في مجال العمل المصرفي

جدول رقــم (5-4)

توزيع المراجعين الداخليين المشاركين بحسب عدد الدورات التدريبية التي شاركوا فيها

المشاركة في دورات تدريبية	العدد	النسبة%
أقل من 4 دورات	3	%20
من 4 دورات إلي أقل من 6 دورات	3	%20
من 6 دورات إلي أقل من 8 دورات	6	%40
من 8 دورات فأكثر	3	%20
المجموع	15	%100

يوضح هذا الجدول توزيع المراجعين الداخليين المشاركين بحسب العدد والنسبة.

يلاحظ من الجدول أن ما نسبته (40%) من المراجعين الداخليين المشاركين في الدراسة تراوحت عدد الدورات التدريبية التي شاركوا فيها ما بين أقل من أربع دورات إلي أقل من ست دورات تدريبية، في حين بلغت نسبة المشاركين في أكثر من ست إلي أقل من ثمانية دورات تدريبية (40%)، وما نسبته (20%) تلقوا دورات تدريبية أكثر من ثمانية، وهي تعتبر نسب معقولة تدل علي اهتمام المصارف المشاركة في الدراسة بتدريب العاملين فيها ورفع كفاءتهم المصرفية.

رابعاً: عدد سنوات العمل في مجال العمل المصرفي للمراجعين الداخليين المشاركين في الدراسة:

يمثل اكتساب الخبرة في مجال العمل المصرفي أمراً هاماً وضرورياً لرفع الأداء، والجدول التالي يوضح توزيع العدد والنسبة لسنوات الخبرة بالنسبة للمراجعين الداخليين المشاركين في الدراسة:

جدول رقـم (6-4)

توزيع المراجعين الداخليين المشاركين حسب سنوات العمل في مجال العمل المصرفي

عدد سنوات العمل	العدد	النسبة%
أقل من 5 سنوات	1	%6.5
من 5 سنوات إلي أقل من 7 سنوات	3	%20
من 7 سنوات إلي أقل من 9 سنوات	3	%20
من 9 سنوات إلي أقل من 11 سنة	6	%40
من 11 سنة فأكثر	2	%13.5
المجموع	15	%100

يوضح هذا الجدول توزيع المراجعين الداخليين المشاركين حسب العدد والنسبة.

من الجدول السابق يمكن ملاحظة أن واحد من المراجعين الداخليين المشاركين في الدراسة تتراوح مدة خبرتهم ما بين أقل من خمس سنوات، في حين أن (20%) منهم كانت مدة خبرتهم من خمس سنوات إلي أقل من سبع سنوات، و(20%) بلغت خبرتهم من سبع سنوات إلي اقل من تسع سنوات، و(40%) منهم تراوحت مدة خبرتهم من تسع سنوات إلي اقل من إحدى عشر سنة، واثنان منهم بلغت مدة خبرتهم من إحدى عشر سنة فأكثر، ويمكن أن نستخلص من هذه المؤشرات أن البيانات المتحصل عليها للدراسة كان مصدرها في الغالب من المشاركين ذوي خبرة طويلة نسبياً مما يعطي للبيانات التي قدموها أهمية.

4.7.2 تحليل الجزء الأول من استمارة الاستبيان لمشرفي المنظومة:

تناول هذا القسم تحليل البيانات المتعلقة بمشرفي المنظومة المشاركين في الدراسة، من حيث المركز الوظيفي، والمؤهل العلمي والتخصص، وعدد سنوات العمل في مجال المصارف، بالإضافة إلي عدد مشاركتهم في الدورات التدريبية في مجال العمال المصرفي، وذلك وفقاً للتالي:

أولاً: المركز الوظيفي لمشرفي المنظومة المشاركين في الدراسة:

يوضح الجدول رقم (7-4) توزيع المركز الوظيفي لمشرفي المنظومة المشاركين في الدراسة بحسب العدد والنسب، ويلاحظ أن (20%) يعملون كرئيس قسم تقنية المعلومات، في حين بلغت ما نسبته (7%) يشغلون وظيفة مشرف منظومة وهي نسبة متدنية مما يدل علي عدم

اهتمام المصارف المشاركة في الدراسة بتعيين كفاءات مهمتهم الإشراف علي نظم المعلومات المحاسبية الالكترونية، وأن (73%) يعملون كموظفين في قسم تقنية المعلومات.

جدول رقــم (7-4)

توزيع مشرفي المنظومة المشاركين حسب المركز الوظيفي

المركز الوظيفي	العدد	النسبة %
رئيس قسم تقنية المعلومات	3	% 20
مشرف المنظومة	1	%7
موظف في قسم تقنية المعلومات	11	%73
المجموع	15	%100

يوضح هذا الجدول توزيع مشرفي المنظومة المشاركين في الدراسة بحسب العدد والنسبة.

ثانياً: المؤهل العلمي لمشرفي المنظومة المشاركين في الدراسة:

يبين الجدول رقم (8-4) توزيع مشرفي المنظومة المشاركين في الدراسة بحسب التأهيل العلمي وذلك وفقاً لعدد ونسبة كل منهم، ويلاحظ أن واحد فقط منهم يحمل بكالوريوس حاسوب، وأيضاً واحد فقط منهم يحمل بكالوريوس محاسبة، ما نسبته (26%) من مشرفي المنظومة المشاركين في الدراسة هم من حملة البكالوريوس في تقنية المعلومات، و(20%) يحملون الدبلوم العالي في أساسيات نظم والحاسوب، وما نسبته (26%) هم من حملة دبلوم عالي حاسوب، وبلغت نسبة من يحملون دبلوم متوسط حاسوب (14%)، وهذا مؤشر جيد يدل علي توافر موارد بشرية مناسبة ومؤهلات علمية داخل المصارف المشاركة بالدراسة.

جدول رقــم (4-8)

توزيع مشرفي المنظومة المشاركين حسب المؤهل العلمي

المؤهل العلمي لمشرفي المنظومة	العدد	النسبة%
بكالوريوس حاسوب	1	%7
بكالوريوس تقنية معلومات	4	%26
بكالوريوس محاسبة	1	%7
دبلوم عالي أساسيات نظم	3	%20
دبلوم عالي حاسوب	4	%26
دبلوم متوسط حاسوب	2	%14
المجموع	15	%100

يوضح هذا الجدول توزيع مشرفي المنظومة المشاركين في الدراسة حسب العدد والنسبة.

ثالثاً: عدد الدورات التدريبية لمشرفي المنظومة المشاركين في الدراسة:

يبين الجدول رقم (4-9) مشرفي المنظومة المشاركين في الدراسة من حيث عدد ونسبة الدورات التدريبية في مجال العمل المصرفي ويلاحظ من الجدول أن اثنان من مشرفي المنظومة لديهم دورات تدريبية أقل من ثلاث، وما نسبته (53%) من مشرفي المنظومة المشاركين في الدراسة تراوحت عدد الدورات التدريبية التي شاركوا فيها ما بين ثلاث دورات إلي أقل من خمس دورات تدريبية، في حين بلغت نسبة المشاركين في خمس دورات تدريبية إلي أقل من سبع (20%)، و(13.5%) تلقوا دورات تدريبية أكثر من سبعة، كما يلاحظ أن جميع المشاركين في الدراسة قد تلقوا دورات تدريبية مما يدل علي اهتمام المصارف بتدريب موظفيها في مجال عملهم لكسب المهارات المختلفة، والرفع من كفاءتهم التقنية.

جدول رقــم (4-9)

توزيع مشرفي المنظومة المشاركين بحسب عدد الدورات التدريبية التي شاركوا فيها

المشاركة في دورات تدريبية	العدد	النسبة%
أقل من 3 دورات	2	%13.5
من 3 دورات إلي أقل من 5 دورات	8	%53
من 5 دورات إلي أقل من 7 دورات	3	%20
من 7 دورات فأكثر	2	%13.5
المجموع	15	%100

يوضح هذا الجدول توزيع مشرفي المنظومة المشاركين بحسب العدد والنسبة.

رابعاً: عدد سنوات العمل في مجال العمل المصرفي لمشرفي المنظومة المشاركين في الدراسة:

يتطلب أداء وظيفة الإشراف علي نظم المعلومات المحاسبية الالكترونية كفاءة عالية مع ضرورة توافر المهارات التقنية لتكنولوجيا المعلومات، والجدول رقم (4-10) يوضح توزيع مشرفي المنظومة المشاركين في الدراسة حسب سنوات الخبرة:

جدول رقــم (4-10)

توزيع مشرفي المنظومة المشاركين حسب سنوات العمل في مجال العمل المصرفي

عدد سنوات العمل	العدد	النسبة%
أقل من 5 سنوات	3	%20
من 5 سنوات إلي أقل من 7 سنوات	7	%47
من 7 سنوات إلي أقل من 9 سنوات	4	%27
من 9 سنوات فأكثر	1	%6
المجموع	15	%100

يوضح هذا الجدول توزيع مشرفي المنظومة المشاركين حسب العدد والنسبة.

من الجدول رقم (4- 10) يلاحظ أن (20%) من مشرفي المنظومة المشاركين في الدراسة تتراوح مدة خبرتهم أقل من خمس سنوات، في حين أن (47%) منهم كانت مدة خبرتهم ما بين خمس سنوات إلي أقل من سبع سنوات، وبلغت نسبة من خبرتهم من سبع سنوات إلي أقل

من تسع سنوات (27%)، وواحد فقط من المشاركين تجاوزت مدة خبرتهم تسع سنوات فأكثر، وهذا يدل علي أن المصارف المشاركة في الدراسة يتوافر لديها موارد بشرية ذات خبرة كافية لتطبيق متطلبات الرقابة محل الدراسة.

4.7.3 تحليل البيانات المتعلقة بالمصارف المشاركة والتوزيع الجغرافي لها:

اختص هذا الجزء بتحليل البيانات المتعلقة بالمصارف المشاركة في الدراسة، من حيث فروع المصارف والتوزيع الجغرافي لها وذلك علي النحو التالي:

أولاً: المصارف المشاركة في الدراسة:

يبين الجدول رقم (11-4) توزيع العدد والنسب للمصارف المشاركة في الدراسة ويلاحظ أن (46%) من المصارف المشاركة في الدراسة تمثل فروع مصرف شمال إفريقيا حيث بلغ عددها سبعة فروع، في حين أن (27%) تمثل مصرف الجمهورية وبلغ عددها أربع فروع، وبلغ عدد فروع مصرف الوحدة أربعه وهو يمثل ما نسبته (27%) أيضاً، وهي مصارف يمتلك مصرف ليبيا المركزي معظم أو كامل رأس مالها الأمر الذي قد يؤثر علي تطبيق آليات الرقابة في المنظومة المصرفية الموحدة.

جدول رقــم (11-4)

توزيع فروع المصارف المشاركة في الدراسة

اسم المصرف المشارك	العدد	النسبة%
مصرف شمال إفريقيا	7	%46
مصرف الجمهورية	4	%27
مصرف الوحدة	4	%27
المجموع	15	%100

يوضح هذا الجدول توزيع فروع المصارف المشاركة حسب العدد والنسبة.

ثانياً: التوزيع الجغرافي للمصارف المشاركة في الدراسة:

يوضح الجدول رقم (12-4) توزيع الجغرافي للمصارف المشاركة في الدراسة وذلك بحسب العدد والنسبة لفروع المدن، ويلاحظ من الجدول أن أكبر نسبة للمدن المشاركة هي مدينة بنغازي حيث بلغ عدد فروع المصارف المشاركة خمس فروع أي ما نسبته (33%) وهي ثاني

أكبر المدن الليبية، ومدينة درنة بأربع فروع ما بنسبة (27%)، ثم مدينة طبرق بنسبة (20%) بثلاث فروع، وتليها مدينة البيضاء بفرعين ما بنسبة (13%)، وأخيراً مدينة طرابلس حيث مثلها فرع واحد من مصرف شمال أفريقيا.

جدول رقـم (12-4)

توزيع الجغرافي لفروع المصارف المشاركة في الدراسة

اسم المدينة المشاركة	العدد الفروع	النسبة%
مدينة بنغازي	5	%33
مدينة درنة	4	%27
مدينة طبرق	3	%20
مدينة البيضاء	2	%13
مدينة طرابلس	1	%7
المجموع	15	%100

يوضح الجدول توزيع الجغرافي لفروع المصارف المشاركة في الدراسة حسب العدد والنسبة.

4.8 تحليـل بيانـــات الدراســـة:

تم تقسيم تحليل بيانات الدراسة إلي جزئيين، يختص الجزء الأول بتحليل بيانات الدراسة المجمعة باستمارة الاستبيان، أما الجزء الثاني فهو يختص بتحليل بيانات الدراسة المجمعة بالأداة الأساسية الثانية وهي الملاحظة كما يلي:

4.8.1 تحليـل بيانـات الدراسة المجمعة باستمارة الاستبيـان:

تم الاعتماد علي التحليل الاستدلال (Inferential Analysis) في تحليل البيانات التي تم تجميعها في الجزء الثاني من استمارة الاستبيان، والذي احتوى علي مجموعة من الأسئلة التي من شأنها الحكم علي فرضيات الدراسة، وذلك من خلال استخدام اختبار (One Sample T-Test)، الذي يستخدم لفحص ما إذا كان متوسط متغير ما لعينة واحدة يساوي قيمة ثابتة[18].

[18]- يشترط لإجراء هذا الاختبار أن يتبع المتغير التوزيع الطبيعي، وفي حالة زيادة حجم العينة عن (100) مفردة يتم الاستعاضة عن شرط التوزيع الطبيعي (الزعبي والطلافحة، 2004).

وفيما يلي عرض للخطوات الأساسية التي تم إتباعها عند اختبار الفرضية الرئيسية والفرضيات الفرعية للدراسة:

1- تم إجراء الاختبار الإحصائي لكل سؤال من الأسئلة الخاصة بكل فرضية فرعية علي اعتبار أنها فرضيات جزئية للفرضية التابعة لها وذلك عند نسبة (70%)، وتم تحديد هذه النسبة بناءً علي رأي احد الخبراء في مجال الإحصاء[19] وموافقة المشرف علي الدراسة، وبالتالي فلن يتم قبول أية أجابه تكون أصغر من أو تساوي (70%)، وفي المقابل سيتم قبول أية أجابه تكون أكبر من (70%) وبناءً علي ذلك تم صياغة الفرضية الصفرية (H_0) والفرضية البديلة (H_1) لهذه المجموعة من الأسئلة علي النحو التالي:

$$H_0: \mu \leq 0.7 \quad * \quad H_1: \mu > 0.7$$

بمعني أخر حسب مقياس ليكرت:

$$H_0: \mu \leq 3.5 \quad * \quad H_1: \mu > 3.5$$

2- تم استخدام قيمة (P-Value)[20] للمقارنة مع مستوى المعنوية (α) الذي تم إجراء الاختبار الإحصائي للفرضيات الفرعية عندها، وهي ($\alpha = 0.05$)، وذلك وفقاً للحالات التالية:

أ- إذا كانت قيمة ($P\text{-value} \leq 0.05$) فأنه يتم رفض الفرضية الصفرية (H_0)، وقبول الفرضية البديلة (H_1) لها.

ب- إما إذا كانت قيمة ($P\text{-value} > 0.05$) فأنه يتم قبول الفرضية الصفرية (H_0)، ورفض الفرضية البديلة (H_1) لها.

3- يتم قبول أو رفض الفرضية بناءً علي نتائج الاختبارات التي أجريت علي الأسئلة المتعلقة بكل فرضية، وذلك وفقاً للحالات التالية:

---

[19]- الدكتور: أحمد مامي، عضو هيئة التدريس بقسم الإحصاء، كلية العلوم: جامعة بنغازي.

[20]- P-Value: هي أصغر مستوى معنوية لـ α التي عندها يمكن أن ترفض فرضية إحصائية (H_0)، (اللافي، 2003: 111).

أ- إذا كان عدد الفرضيات الصفرية التي تم رفضها أكثر من عدد الفرضيات الصفرية التي تم قبولها، وذلك بالنسبة لكل سؤال من أسئلة الفرضيات الفرعية محل الاختبار، فأنه في هذه الحالة يتم رفض الفرضية الصفرية (H_0) للفرضية الفرعية، وقبول الفرضية البديلة (H_1) لها.

ب- إذا كان عدد الفرضيات الصفرية التي تم رفضها أقل من عدد الفرضيات الصفرية التي تم قبولها، وذلك بالنسبة لكل سؤال من أسئلة الفرضيات الفرعية محل الاختبار، فأنه في هذه الحالة يتم قبول الفرضية الصفرية (H_0) للفرضية الفرعية، ورفض الفرضية البديلة (H_1) لها.

4- تم اختبار الفرضية الرئيسية لهذه الدراسة من خلال المقارنة بين عدد الفرضيات الصفرية للفرضيات الفرعية التي تم رفضها، وفقاً للحالات التالية:

أ- إذا كان عدد الفرضيات الصفرية للفرضيات الفرعية التي تم رفضها أكثر من عدد الفرضيات الصفرية للفرضيات الفرعية التي تم قبولها، فأنه يتم رفض الفرضية الصفرية (H_0) للفرضية الرئيسية، وقبول الفرضية البديلة (H_1) لها.

ب- أما إذا كان عدد الفرضيات الصفرية للفرضيات الفرعية التي تم رفضها أقل من عدد الفرضيات الصفرية للفرضيات الفرعية التي تم قبولها، فأنه في هذه الحالة يتم قبول الفرضية الصفرية (H_0) للفرضية الرئيسية، ورفض الفرضية البديلة (H_1) لها.

5- عند الانتهاء من الخطوات الأساسية التي تم إتباعها لاختبار الفرضيات الفرعية والفرضية الرئيسية للدراسة، سيتم استخلاص نتائج الدراسة حول فعالية الرقابة للمنظومة المصرفية الموحدة في المصارف الليبية المشاركة بالدراسة.

4.8.1.1 اختبـــار الفرضيـــات الفرعيـــة:

وللإجابة علي سؤال الدراسة من البيانات المجمعة باستمارة الاستبيان، وتحقيق الهدف الذي قامت من أجله، تـم صياغة الفرضية الرئيسية لها علي النحو التالي:

"عدم فعالية الرقابة للمنظومة المصرفية الموحدة في ليبيا".

ولاختبار هذه الفرضية تم التعبير عنها إحصائياً علي النحو التالي:

الفرضية الصفرية (H_0):

عدم فعالية الرقابة للمنظومة المصرفية الموحدة في ليبيا.

الفرضية البديلة (H_1):

الرقابة في المنظومة المصرفية الموحدة في ليبيا فعالة.

ولكي يمكن اختبار الفرضية الرئيسية للدراسة ومن ثم قبولها أو رفضها، تم صياغة عدد (9) فرضيات فرعية، وفيما يلي تحليل النتائج التي توصلت إليها استمارة الاستبيان والقرار المتخذ حيال كل فرضية من هذه الفرضيات.

4.8.1.1.1 اختبـــار الفرضية الفرعية الأولـــي:

هدفت هذه الفرضية إلي التعرف علي مدى فعالية آليات الرقابة في خفض الخطأ والغش في المصارف الليبية التي تعمل وفقاً للمنظومة الموحدة، وكان نص هذه الفرضية كما يلي:

"لا تخفض آليات الرقابة من الخطأ والغش".

ولاختبار هذه الفرضية تم التعبير عنها إحصائياً علي النحو التالي:

الفرضية الصفرية (H_0): لا تخفض آليات الرقابة من الخطأ والغش.

الفرضية البديلة (H_1): تخفض آليات الرقابة من الخطأ والغش.

وتم تخصيص المجموعة الأولي من الجزء الثاني لاستمارة الاستبيان لاختبار الفرضية الفرعية الأولي، واحتوت هذا المجموعة علي (5) أسئلة تم اعتبار كل سؤال منها بمثابة فرضية جزئية للفرضية الفرعية الأولي، والجدول رقم (13-4) يوضح نتائج الاختبار الإحصائي:

جدول رقـم (13-4)
نتائج اختبار الفرضية الفرعية الأولي

م	الأسئلة المتعلقة بالفرضية	المراجعين الداخليين			مشرفي المنظومة		
		المتوسط الحسابي	الدلالة الإحصائية	القرار الإحصائي	المتوسط الحسابي	الدلالة الإحصائية	القرار الإحصائي
1	التأكد من الصحيفة الجنائية للعاملين المصرح لهم الوصول للبيانات الهامة.	4.67	0.000	رفض H_0	4.53	0.000	رفض H_0
2	الفصل الجيد بين وظائف تطوير نظم المعلومات، والوظائف المحاسبية.	4.33	0.000	رفض H_0	4.53	0.000	رفض H_0
3	وجود إشراف علي الوظائف الرقابية.	3.67	0.036	رفض H_0	3.73	0.022	رفض H_0
4	تناوب الواجبات لتقليل فرص حدوث الغش وزيادة فرص اكتشاف الخطأ.	3.40	0.189	قبول H_0	3.80	0.001	رفض H_0
5	إعطاء إجازات إجبارية للعاملين لتخفيض احتمال الغش.	2.00	0.003	رفض H_0	1.93	0.003	رفض H_0

يوضح هذا الجدول نتائج اختبار الفرضية الفرعية الأولي عند مستوى معنوية (0.05).

يوضح الجدول نتائج اختبار الفرضية الفرعية الأولي حول آليات رقابة خفض الخطأ والغش وفيما يلي تحليل لكل فئة علي حدا:

أولاً: فيما يتعلق بالمراجعين الداخليين:

أظهرت نتائج المراجعين الداخليين الجدول رقم (13- 4) بأنه تم رفض عدد (4) فرضيات صفرية (H_0) من أصل (5) فرضيات صفرية وذلك بالنسبة للفرضيات الجزئية، حيث كانت المتوسطات الحسابية للأسئلة أرقام (1)،(2)،(3) أكبر من المتوسط النظري (3.5)، بالإضافة إلي قيمة P-value كانت ذات دلالة إحصائية معنوية وهي أصغر من مستوى المعنوية (0.05) لكل سؤال، وهذا يعني يتم التأكد من الصحيفة الجنائية للعاملين المصرح لهم الوصول للبيانات الهامة، وجود فصل جيد بين وظائف تطوير نظم المعلومات والوظائف الإدارية والمحاسبية، بالإضافة إلي وجود إشراف علي الوظائف الرقابية في المصارف المشاركة بالدراسة، أما السؤال رقم (5) حول إعطاء إجازات إجبارية للعاملين لتخفيض احتمال الغش كان المتوسط الحسابي أصغر من المتوسط النظري (3.5)، إلا أن قيمة P-value كانت ذات دلالة إحصائية معنوية أصغر من مستوى المعنوية (0.05)، وبالتالي تم رفض الفرضية الصفرية وقبول الفرضية البديلة له أيضاً.

أما السؤال رقم (4) حول تناوب الواجبات لتقليل فرص حدوث الخطأ والغش وزيادة اكتشافها، كانت قيمة المتوسط الحسابي أصغر من المتوسط النظري (3.5)، بالإضافة إلي أن قيمة

P-value كانت ذات دلالة إحصائية غير معنوية أكبر من مستوى المعنوية (0.05)، وبالتالي تم قبول الفرضية الصفرية لهذا السؤال ورفض الفرضية البديلة له.

وبناءً علي ما تم التوصل إليه من نتائج الاختبار تم رفض عدد أربع فرضيات صفرية للفرضيات الجزئية، وقبول فرضية صفرية واحدة فقط، مما يعني رفض الفرضية الصفرية (H_0) للفرضية الفرعية الأولي، وقبول الفرضية البديلة (H_1) لها، أي أن من وجهت نظر المراجعين الداخليين تخفض آليات الرقابة من الخطأ والغش في المصارف المشاركة بالدراسة

ثانياً: فيما يتعلق بمشرفى المنظومة:

أظهرت نتائج مشرفي المنظومة الجدول رقم (13- 4) أنه تم رفض كل الفرضيات الصفرية (H_0) وذلك بالنسبة للفرضيات الجزئية، وقبول الفرضيات البديلة لها (H_1)، حيث كان المتوسطات الحسابية للأسئلة أرقام (1)،(2)،(3)،(4) أكبر من المتوسط النظري (3.5)، وكانت قيمة P-value ذات دلالة إحصائية معنوية أصغر من مستوى المعنوية (0.05)، مما يدل علي التأكد من الصحيفة الجنائية للعاملين المصرح لهم الوصول للبيانات الهامة، ووجود فصل جيد بين الوظائف تطوير نظم المعلومات والوظائف الإدارية والمحاسبية، بالإضافة إلي وجود إشراف علي الوظائف الرقابية، وتناوب الواجبات لتقليل فرص حدوث الغش وزيادة فرص اكتشاف الخطأ، أما السؤال رقم (5) حول إعطاء إجازات إجبارية للعاملين لتخفيض احتمال الغش، كان المتوسط الحسابي لهذا السؤال أصغر من المتوسط النظري (3.5)، إلا أن قيمة P-value كانت ذات دلالة إحصائية معنوية أصغر من مستوى المعنوية (0.05)، وبالتالي تم رفض الفرضية الصفرية لهذا السؤال وقبول الفرضية البديلة له أيضاً.

مما سبق وبناءً علي نتائج مشرفي المنظومة تم رفض كل الفرضيات الصفرية للفرضيات الجزئية، مما يعني رفض الفرضية الصفرية (H_0) للفرضية الفرعية الأولي، وقبول الفرضية البديلة (H_1) لها، أي أن من وجهت نظر مشرفي المنظومة تخفض آليات الرقابة من الخطأ والغش في المصارف المشاركة في الدراسة.

- **خلاصة نتائج اختبار الفرضية الفرعية الأولى:**

يتضح من نتائج اختبار الفرضية الفرعية الأولي، أن المراجعين الداخليين ومشرفي المنظومة متفقون علي أن المصارف المشاركة في الدراسة بها نظام رقابة يمكن من خلاله تخفيض الخطأ والغش وزيادة فرص اكتشافها مما يدل علي فعالية آليات رقابة خفض الخطأ والغش.

4.8.1.1.2 اختبار الفرضية الفرعية الثانية:

تهدف هذه الفرضية إلي التعرف علي مدى فعالية آليات الرقابة في خفض الوصول المادي في المصارف الليبية، وكان نص الفرضية كالتالي:

"لا تخفض آليات الرقابة من الوصول المادي".

ولاختبار هذه الفرضية تم التعبير عنها إحصائياً علي النحو التالي:

الفرضية الصفرية (H_0): لا تخفض آليات الرقابة من الوصول المادي.

الفرضية البديلة (H_1): تخفض آليات الرقابة من الوصول المادي.

ولقبول أو رفض هذه الفرضية خصص لها المجموعة الثانية من الجزء الثاني لاستمارة الاستبيان لاختبار الفرضية الفرعية الثانية، حيث احتوت هذا المجموعة علي (5) أسئلة تم اعتبار كل سؤال منها كفرضية جزئية للفرضية الفرعية الثانية، وكانت نتائج الاختبار كما يوضحها الجدول رقم (14-4):

جدول رقـــم (14-4)
نتائج اختبار الفرضية الفرعية الثانية

م	الأسئلة المتعلقة بالفرضية	المراجعين الداخليين			مشرفي المنظومة		
		المتوسط الحسابي	الدلالة الإحصائية	القرار الإحصائي	المتوسط الحسابي	الدلالة الإحصائية	القرار الإحصائي
1	وضع جهاز الخادم (Server) والمعدات الهامة في حجرات مغلقة بإحكام.	4.40	0.000	رفض H_0	4.60	0.000	رفض H_0
2	تركيب أجهزة إنذار علي معدات الحاسب الآلي.	2.13	0.032	رفض H_0	1.93	0.008	رفض H_0
3	وضع سجلات دخول وخروج حجرات الحاسب الآلي والمتابعة من الموظف المختص.	2.07	0.017	رفض H_0	2.27	0.060	قبول H_0
4	وجود سجلات للزائرين يحتوي علي البيانات الكافية وأسباب الزيارة.	2.07	0.004	رفض H_0	2.20	0.017	رفض H_0
5	وجود تأمين ضد السرقة والمخاطر الأخرى تغطي أجهزة الحاسب الآلي.	1.53	0.000	رفض H_0	2.00	0.010	رفض H_0

يوضح هذا الجدول نتائج اختبار الفرضية الفرعية الثانية عند مستوى معنوية (0.05).

يوضح الجدول نتائج اختبار الفرضية الفرعية الثانية حول فعالية آليات رقابة الوصول المادي لكل فئة علي حدا:

أولاً: فيما يتعلق بالمراجعين الداخليين:

أظهرت نتائج المراجعين الداخليين الجدول رقم (14- 4) أنه تم رفض كل الفرضيات الصفرية وذلك بالنسبة للفرضيات الجزئية للفرضية الفرعية الثانية، بالنسبة للسؤال رقم (1) تم رفض الفرضية الصفرية لهذا السؤال وقبول الفرضية البديلة له، حيث أن قيمة المتوسط الحسابي لهذا السؤال كانت أكبر من المتوسط النظري (3.5)، بالإضافة إلي إن قيمة P-value كانت ذات دلالة إحصائية معنوية أكبر من مستوى المعنوية (0.05)، مما يدل على أن المصارف المشاركة في الدراسة حريصة علي وضع جهاز الخادم والمعدات الهامة الخاصة بالمنظومة الموحدة في حجرات مغلقة بإحكام.

وكانت الأسئلة أرقام (2)،(3)،(4)،(5)، حول تركيب أجهزة إنذار علي معدات وأجهزة الحاسب الآلي، ووضع سجلات دخول وخروج حجرات الحاسب الآلي والمتابعة من الموظف المختص، ووجود سجلات للزائرين يحتوي علي البيانات الكافية وأسباب الزيارة، ووجود تأمين ضد السرقة والمخاطر الأخرى تغطي أجهزة الحاسب الآلي، وتركيب أجهزة إنذار علي معدات وأجهزة الحاسب الآلي، ظهرت قيمة المتوسطات الحسابية لهذه الأسئلة أصغر من المتوسط النظري (3.5)، إلا أن قيمة P-value كانت ذات دلالة إحصائية معنوية أصغر من مستوى المعنوية (0.05)، وبالتالي تم رفض الفرضيات الصفرية الجزئية لهذه الأسئلة وقبول الفرضيات البديلة لها.

مما سبق وبناءً علي نتائج الاختبار تم رفض كل الفرضيات الصفرية للفرضيات الجزئية، وقبول الفرضيات البديلة لها، مما يعني رفض الفرضية الصفرية (H_0) للفرضية الفرعية الثانية، وقبول الفرضية البديلة (H_1) لها، أي أنه من وجهت نظر المراجعين الداخليين فأن آليات رقابة الوصول المادي ذات فعالية في المصارف المشاركة في الدراسة.

ثانياً: فيما يتعلق بمشرفي المنظومة:

أظهرت نتائج مشرفي المنظومة الجدول رقم (14- 4) بأنه تم رفض عدد (4) فرضيات صفرية من أصل (5) فرضيات صفرية وذلك بالنسبة للفرضيات الجزئية، وقبول الفرضيات البديلة لها، حيث تم رفض الفرضية الصفرية للسؤال رقم (1) وقبول الفرضية البديلة له، حيث كانت قيمة المتوسط الحسابي أكبر من المتوسط النظري (3.5)، بالإضافة إلي أن قيمة P-value كانت ذات دلالة إحصائية معنوية أصغر من مستوى المعنوية (0.05)، مما يدل علي حرص المصارف المشاركة في الدراسة علي وضع جهاز الخادم والمعدات الهامة في حجرات مغلقة بإحكام، أما الأسئلة أرقام (2)،(4)،(5)، حول تركيب أجهزة إنذار علي معدات الحاسب الآلي، ووجود سجلات للزائرين يحتوي علي البيانات الكافية وأسباب الزيارة، ووجود تأمين ضد

السرقة والمخاطر الأخرى تغطي أجهزة الحاسب الآلي، كانت قيمة المتوسطات الحسابية لهذه الأسئلة أصغر من المتوسط النظري (3.5)، إلا أن قيمة P-value لهذه الأسئلة كانت ذات دلالة إحصائية معنوية أصغر من مستوى المعنوية (0.05)، وبالتالي تم رفض الفرضيات الصفرية لهذا الأسئلة وقبول الفرضيات البديلة له.

وكان السؤال رقم (3) حول وضع سجلات دخول وخروج حجرات الحاسب الآلي والمتابعة من الموظف المختص، أن قيمة المتوسط الحسابي كانت أصغر من المتوسط النظري (3.5)، وقيمة P-value كانت ذات دلالة إحصائية غير معنوية أصغر من مستوي المعنوية (0.05)، وبالتالي تم قبول الفرضية الصفرية لهذا السؤال ورفض الفرضية البديلة له.

مما سبق وبناءً علي نتائج الفرضيات الجزئية للفرضية الفرعية الثانية يتضح بأنه تم رفض عدد (4) فرضيات صفرية للفرضيات الجزئية، مما يعني رفض الفرضية الصفرية (H_0) للفرضية الفرعية الثانية، وقبول الفرضية البديلة (H_1) لها، أي أنه من وجهت نظر مشرفي المنظومة أن آليات رقابة الوصول المادي فعالة في المصارف المشاركة في الدراسة.

- **<u>خلاصة نتائج اختبار الفرضية الفرعية الثانية:</u>**

يتضح من نتائج اختبار الفرضية الفرعية الثانية، أن المراجعين الداخليين ومشرفي المنظومة متفقون علي أن المصارف في الدراسة يوجد بها نظام رقابة يمكن من خلاله تخفيض الوصول المادي ومنع الوصول غير المصرح به لحجرات ومعدات المنظومة الموحدة مما يدل علي فعالية آليات الرقابة في تخفيض الوصول المادي.

4.8.1.1.3 اختبــار الفرضية الفرعية الثالثة:

اهتمت الفرضية الفرعية الثالثة بالتعرف علي مدى فعالية آليات رقابة الوصول المنطقي في المصارف الليبية، وكان نصها كالتالي:

"لا تخفض آليات الرقابة من الوصول المنطقي".

ولاختبار هذه الفرضية تم التعبير عنها إحصائياً علي النحو التالي:

الفرضية الصفرية (H_0): لا تخفض آليات الرقابة من الوصول المنطقي.

الفرضية البديلة (H_1): تخفض آليات الرقابة من الوصول المنطقي.

وتم تخصيص المجموعة الثالثة من الجزء الثاني لاستمارة الاستبيان لاختبار الفرضية الفرعية الثالثة، حيث احتوت هذا المجموعة علي (17) سؤال تم اعتبار كل سؤال منها بمثابة فرضية جزئية للفرضية الفرعية الثالثة، والجدول رقم (15-4) يوضح نتائج الاختبار الإحصائي:

جدول رقم (15-4)
نتائج اختبار الفرضية الفرعية الثالثة

م	الأسئلة المتعلقة بالفرضية	المراجعين الداخليين			مشرفي المنظومة		
		المتوسط الحسابي	الدلالة الإحصائية	القرار الإحصائي	المتوسط الحسابي	الدلالة الإحصائية	القرار الإحصائي
1	تغيير كلمات المرور بصورة دورية علي الأقل 90 يوم.	4.80	0.000	رفض H_0	4.80	0.000	رفض H_0
2	وضع شاشات توقف بكلمات مرور (Screen Saver).	4.80	0.000	رفض H_0	4.67	0.000	رفض H_0
3	في حالة الحاجة إلي تجاوز الإجراءات الرقابية لابد من توافر التصريح الملائم لذلك التجاوز.	4.73	0.000	رفض H_0	4.60	0.000	رفض H_0
4	كل مستخدم له هوية (ID) وكلمة المرور الخاصة به التي يصعب تخمينها.	4.67	0.000	رفض H_0	4.67	0.000	رفض H_0
5	توفير إجراءات رقابية لحماية أشرطة الأمن المخزنة في النظام التي تستخدم للتحقق من الصحة.	4.67	0.000	رفض H_0	4.33	0.000	رفض H_0
6	منع النسخ غير المصرح به لرخص البرامج.	4.53	0.000	رفض H_0	4.67	0.000	رفض H_0
7	منع استخدام نسخ غير أصلية من البرامج.	4.53	0.000	رفض H_0	4.53	0.000	رفض H_0
8	تحديد الأشخاص المصرح لهم منح تغيير هويات التعريف وكلمات المرور للمستخدمين.	4.40	0.000	رفض H_0	4.60	0.000	رفض H_0
9	تحديد الأشخاص المفوض لهم الوصول إلي معلومات المصرف وتوفير الهويات اللازمة لذلك.	3.93	0.008	رفض H_0	3.93	0.001	رفض H_0
10	توعية العاملين بضرورة عدم كتابة كلمة المرور أو إظهارها علي الشاشة أو تداولها فيما بينهم.	3.60	0.045	رفض H_0	3.53	0.041	رفض H_0
11	استخدام برنامج ربط الشبكات الافتراضي لمنع الوصول غير المصرح به.	3.33	0.238	قبول H_0	3.27	0.301	قبول H_0
12	التحديد الالكتروني لكل الشبكات الطرفية.	3.00	1.000	قبول H_0	3.53	0.120	قبول H_0
13	احتواء كلمة المرور علي الأقل (6) أحرف واحدها علي الأقل رقمي.	2.87	0.670	قبول H_0	3.13	0.610	قبول H_0
14	استخدام إجراءات التحقق من المسلك لضمان عدم إرسال رسائل الالكترونية إلي عناوين خاطئة.	2.73	0.413	قبول H_0	2.67	0.313	قبول H_0
15	إجراء فحوصات رقابية للمخاطر المحتملة بصورة دورية والتقرير عن النتائج الفحص للإدارة العليا.	2.67	0.403	قبول H_0	2.13	0.022	رفض H_0
16	استخدام تقنيات التقرير عن الرسائل لإعلام الراسل إن الرسائل المرسلة تم استلامها.	2.53	0.235	قبول H_0	2.87	0.728	قبول H_0

17	استخدام أنظمة تعقب المتطفلين لاكتشاف المبكر للاختراقات الرقابية المحتملة.	2.13	0.007	رفض H_0	2.00	0.006	رفض H_0

يوضح هذا الجدول نتائج اختبار الفرضية الفرعية الثالثة عند مستوى معنوية (0.05).

يوضح الجدول السابق نتائج اختبار الفرضية الفرعية الثالثة حول فعالية رقابة الوصول المنطقي وفيما يلي تحليل لكل فئة علي حدا:

أولاً: فيما يتعلق بالمراجعين الداخليين:

أظهرت نتائج المراجعين الداخليين الجدول رقم (15- 4) بأنه تم رفض عدد (11) فرضيات صفرية من أصل (17) فرضية صفرية وذلك بالنسبة للفرضيات الجزئية، بالنسبة للأسئلة أرقام (1)،(2)،(3)،(4)،(5)،(6)،(7)،(8)،(9)،(10)، تم رفض الفرضيات الصفرية لهذه الأسئلة وقبول الفرضيات البديلة لها، ذلك أن قيمة المتوسطات الحسابية لهذه الأسئلة كانت أكبر من المتوسط النظري (3.5)، بالإضافة إلي أن قيمة P-value كانت ذات دلالة إحصائية معنوية أصغر من مستوى المعنوية (0.05)، أما السؤال رقم (17) حول استخدام أنظمة تعقب المتطفلين لاكتشاف المبكر للاختراقات الرقابية المحتملة، كانت قيمة المتوسط الحسابي أصغر من المتوسط النظري (3.5)، إلا أن قيمة P-value كانت ذات دلالة إحصائية معنوية أصغر من مستوى المعنوية (0.05)، وبالتالي تم رفض الفرضية الصفرية لهذا السؤال وقبول الفرضية البديلة له.

أما الأسئلة أرقام (11)،(12)،(13)،(14)،(15)،(16)، كانت قيمة المتوسطات الحسابية لهذه الأسئلة أصغر من المتوسط النظري (3.5)، بالإضافة إلي قيمة P-value كانت ذات دلالة إحصائية غير معنوية أكبر من مستوى المعنوية (0.05)، وبالتالي تم قبول الفرضيات الصفرية لهذه الأسئلة ورفض الفرضيات البديلة لها.

مما سبق وبناءً علي نتائج الاختبار تم رفض عدد (11) فرضيات صفرية للفرضيات الجزئية من أصل (17) فرضية صفرية، مما يعني رفض الفرضية الصفرية (H_0) للفرضية الفرعية الثالثة، وقبول الفرضية البديلة (H_1) لها، أي أنه من وجهت نظر المراجعين الداخليين أنه تخفض آليات الرقابة من الوصول المنطقي في المصارف المشاركة في الدراسة.

ثانياً: فيما يتعلق بمشرفي المنظومة:

أظهرت نتائج مشرفي المنظومة الجدول رقم (15- 4) أنه تم رفض عدد (12) فرضية صفرية، من أصل (17) فرضية صفرية وذلك بالنسبة للفرضيات الجزئية، حيث تم رفض الفرضيات الصفرية للأسئلة أرقام (1)،(2)،(3)،(4)،(5)،(6)،(7)،(8)،(9)،(10)، وقبول الفرضيات البديلة لها، كانت قيمة المتوسطات الحسابية لهذه الأسئلة أكبر من المتوسط النظري

(3.5)، بالإضافة إلي أن قيمة P-value كانت ذات دلالة إحصائية معنوية أصغر من مستوى المعنوية (0.05)، أما السؤالين أرقام (15)،(17)، حول إجراء فحوصات رقابية للمخاطر المحتملة بصورة دورية والتقرير عن النتائج الفحص للإدارة العليا، واستخدام أنظمة تعقب المتطفلين لاكتشاف المبكر للاختراقات الرقابية المحتملة، كانت قيمة المتوسط الحسابي لها أصغر من المتوسط النظري (3.5)، إلا أن قيمة P-value كانت ذات دلالة إحصائية معنوية أصغر من مستوى المعنوية (0.05)، بالتالي تم رفض الفرضيتين الصفريتين لهذين السؤالين وقبول الفرضيتين البديلتين لهما.

أما الأسئلة أرقام (11)،(12)،(13)،(14)،(16)، كانت قيمة المتوسط الحسابي أصغر من المتوسط النظري (3.5)، بالإضافة إلي أن قيمة P-value كانت ذات دلالة إحصائية غير معنوية أكبر مستوى المعنوية (0.05)، وبالتالي تم قبول الفرضيات الصفرية لهذه الأسئلة ورفض الفرضيات البديلة لها.

مما سبق وبناءً علي نتائج الاختبار تم رفض عدد (12) فرضية صفرية للفرضيات الجزئية من أصل عدد (17) فرضية صفرية، مما يعني رفض الفرضية الصفرية (H_0) للفرضية الفرعية الثالثة وقبول الفرضية البديلة (H_1) لها، أي أنه من وجهت نظر مشرفي المنظومة فأنه تخفض آليات الرقابة من الوصول المنطقي في المصارف الليبية المشاركة في الدراسة.

- **<u>خلاصة نتائج اختبار الفرضية الفرعية الثالثة:</u>**

يتضح من نتائج اختبار الفرضية الفرعية الثالثة، أن المراجعين الداخليين ومشرفي المنظومة توصلوا إلي أن المصارف المشاركة في الدراسة يوجد بها نظام رقابة يمكن من خلاله تخفيض الوصول المنطقي وحماية أجهزة الحاسب من الاستخدام غير المصرح به، وهذا يدل علي فعالية آليات الرقابة في تخفيض الوصول المنطقي في المصارف المشاركة في الدراسة.

4.8.1.1.4 اختبـار الفرضية الفرعية الرابعة:

تهدف هذه الفرضية إلي التعرف علي مدى فعالية آليات الرقابة في تحسين أمن البيانات في المصارف المشاركة في الدراسة، وكان نصها كالتالي:

"لا تحسن آليات الرقابة من أمن البيانات".

ولاختبار هذه الفرضية تم التعبير عنها إحصائياً علي النحو التالي:

الفرضية الصفرية (H_0): لا تحسن آليات الرقابة من أمن البيانات.

الفرضية البديلة (H_1): تحسن آليات الرقابة من أمن البيانات.

وخصصت المجموعة الرابعة من الجزء الثاني لاستمارة الاستبيان لاختبار الفرضية الفرعية الرابعة، حيث احتوت هذا المجموعة علي (11) سؤال تم اعتبار كل سؤال منها كفرضية جزئية للفرضية الفرعية الرابعة، وكانت نتائج الاختبار كما يوضحها الجدول رقم (16-4):

جدول رقـم(16-4)

نتائج اختبار الفرضية الفرعية الرابعة

م	الأسئلة المتعلقة بالفرضية	المراجعين الداخليين			مشرفي المنظومة		
		المتوسط الحسابي	الدلالة الإحصائية	القرار الإحصائي	المتوسط الحسابي	الدلالة الإحصائية	القرار الإحصائي
1	توفير إجراءات الحماية من الكتابة لضمان عدم إعادة الكتابة علي البيانات المخزنة أو حذفها.	4.80	0.000	رفض H_0	4.67	0.000	رفض H_0
2	حماية الأقراص المغناطيسية للنسخ الاحتياطية وذلك لحفظها في خزائن آمنة.	4.80	0.000	رفض H_0	4.67	0.000	رفض H_0
3	تخزين الملفات في أماكن محمية من الحريق والأتربة وأي ظروف ضارة.	4.67	0.000	رفض H_0	4.33	0.001	رفض H_0
4	منع استخدام لغات البرمجة المتقدمة التي قد تغير من البيانات.	4.40	0.000	رفض H_0	4.80	0.000	رفض H_0
5	متابعة البيانات الهامة بصورة دورية.	4.40	0.000	رفض H_0	4.47	0.000	رفض H_0
6	تشفير البيانات الهامة.	4.00	0.001	رفض H_0	3.53	0.015	رفض H_0
7	تحديد المستخدم المصرح به الحصول علي كل نوع من المعلومات وتحديد التوقيت الملائم ومكان تواجدها.	3.93	0.004	رفض H_0	3.60	0.120	قبول H_0
8	تطبيق الإجراءات الرقابية الملائمة عند المناولة اليدوية للبيانات بين الأقسام المختلفة والمركز الرئيسي والفروع.	3.80	0.028	رفض H_0	3.67	0.055	قبول H_0
9	توفير جداول زمنية لإعداد نسخ احتياطية من البيانات وحفها بصورة جيدة.	3.20	0.550	قبول H_0	3.60	0.108	قبول H_0
10	تقسيم البيانات حسب أهميتها وتحديد مستوى الحماية لكل نوع.	2.93	0.869	قبول H_0	2.53	0.131	قبول H_0
11	إعداد واستخدام دليل جيد للبيانات.	2.60	0.288	قبول H_0	2.60	0.288	قبول H_0

يوضح هذا الجدول نتائج اختبار الفرضية الفرعية الرابعة عند مستوى معنوية (0.05).

يوضح الجدول نتائج اختبار الفرضية الفرعية الرابعة حول فعالية آليات رقابة أمن البيانات وفيما يلي تحليل لكل فئة علي حدا:

أولاً: فيما يتعلق بالمراجعين الداخليين:

أظهرت نتائج المراجعين الداخليين الجدول رقم (16- 4) بأنه تم رفض عدد (8) فرضيات صفرية من أصل (11) فرضية صفرية وذلك بالنسبة للفرضيات الجزئية، حيث تم رفض الفرضيات الصفرية للأسئلة أرقام (1)،(2)،(3)،(4)،(5)،(6)،(7)،(8)، وقبول الفرضيات البديلة لها، وكانت قيمة المتوسطات الحسابية لهذه الأسئلة أكبر من المتوسط النظري (3.5)، بالإضافة إلي أن قيمة P-value كانت ذات دلالة إحصائية معنوية أكبر من مستوى المعنوية (0.05)، مما يدل علي توفير إجراءات الحماية من الكتابة لضمان عدم إعادة الكتابة علي البيانات المخزنة أو حذفها، وحماية الأقراص المغناطيسية للنسخ الاحتياطية وذلك لحفظها في خزائن آمنة، وتخزين الملفات في أماكن محمية من الحريق والأتربة وأي ظروف ضارة، ومنع استخدام لغات البرمجة المتقدمة التي قد تغير من البيانات، ومتابعة البيانات الهامة بصورة دورية، وتشفير البيانات الهامة، وتحديد المستخدم المصرح به الحصول علي كل نوع من المعلومات وتحديد التوقيت الملائم ومكان تواجدها، وكذلك تطبيق الإجراءات الرقابية الملائمة عند المناولة اليدوية للبيانات بين الأقسام المختلفة والمركز الرئيسي والفروع في المصارف المشاركة في الدراسة.

وكانت الأسئلة أرقام (9)،(10)،(11)، حول توفير جداول زمنية لإعداد نسخ احتياطية من البيانات وحفظها بصورة جيدة، وتقسيم البيانات علي حسب أهميتها وتحديد مستوى الحماية لكل نوع، وإعداد واستخدام دليل جيد للبيانات، كانت قيمة المتوسطات الحسابية لهذه الأسئلة أصغر من المتوسط النظري (3.5)، بالإضافة إلي قيمة P-value كانت ذات دلالة إحصائية غير معنوية أكبر من مستوى المعنوية (0.05)، بالتالي تم قبول الفرضيات الصفرية لهذه الأسئلة ورفض الفرضيات البديلة لها.

مما سبق وبناءً علي نتائج اختبار الفرضية الفرعية الرابعة تم رفض عدد (8) فرضيات صفرية للفرضيات الجزئية من أصل (11) فرضية صفرية، مما يعني رفض الفرضية الصفرية (H_0) للفرضية الفرعية الرابعة، وقبول الفرضية البديلة (H_1) لها، أي أنه من وجهت نظر المراجعين الداخليين فأن تحسن آليات الرقابة من أمن البيانات في المصارف المشاركة في الدراسة.

ثانياً: فيما يتعلق بمشرفي المنظومة:

أظهرت نتائج مشرفي المنظومة الجدول رقم (16- 4) أنه تم رفض عدد (6) فرضيات صفرية، من أصل (11) فرضية صفرية وذلك بالنسبة للفرضيات الجزئية، بالنسبة للأسئلة أرقام

(1)،(2)،(3)،(4)،(5)،(6)، تم رفض الفرضيات الصفرية لهذه الأسئلة وقبول الفرضيات البديلة لها، حيث كانت قيمة المتوسطات الحسابية لهذه الأسئلة أكبر من المتوسط النظري (3.5)، بالإضافة إلي أن قيمة P-value كانت ذات دلالة إحصائية معنوية أصغر من مستوى المعنوية (0.05)، مما يدل علي توفير إجراءات الحماية من الكتابة لضمان عدم إعادة الكتابة علي البيانات المخزنة أو حذفها، وحماية الأقراص المغناطيسية للنسخ الاحتياطية وذلك لحفظها في خزائن آمنة، وتخزين الملفات في أماكن محمية من الحريق والأتربة وأي ظروف ضارة، ومنع استخدام لغات البرمجة المتقدمة التي قد تغير من البيانات، ومتابعة البيانات الهامة بصورة دورية، وتشفير البيانات الهامة في المصارف المشاركة في الدراسة.

أما الأسئلة أرقام (7)،(8)،(9)،(10)،(11)، كانت قيمة المتوسطات الحسابية لها تقارب المتوسط النظري (3.5)، إلا أن قيمة P-value كانت ذات دلالة إحصائية غير معنوية أكبر من مستوى المعنوية (0.05)، وبالتالي تم قبول الفرضيات الصفرية لهذه الأسئلة ورفض الفرضيات البديلة لها.

مما سبق وبناءً علي نتائج الاختبار تم رفض عدد (6) فرضيات صفرية الجزئية من أصل عدد (11) فرضية صفرية، مما يعني رفض الفرضية الصفرية (H_0) للفرضية الفرعية الرابعة، وقبول الفرضية البديلة (H_1) لها، أي أنه من وجهت نظر مشرفي المنظومة فأنه تحسن آليات الرقابة من أمن البيانات في المصارف المشاركة في الدراسة.

- **<u>خلاصة نتائج اختبار الفرضية الفرعية الرابعة:</u>**

يتضح من نتائج اختبار الفرضية الفرعية الرابعة، أن المراجعين الداخليين ومشرفي المنظومة توصلوا إلي أن المصارف المشاركة في الدراسة بها نظام رقابة يمكن من خلاله تحسين أمن البيانات وحمايتها سواء كانت هذه البيانات موجودة علي أجهزة الحاسب الآلي أو محفوظة في صورة رقمية أو ورقية، مما يدل علي فعالية آليات الرقابة في تحسين أمن البيانات.

4.8.1.1.5 اختبــار الفرضية الفرعية الخامسة:

هدفت هذه الفرضية إلي التعرف علي مدى فعالية آليات الرقابة في تحسين معايير التوثيق في المصارف الليبية التي تعمل وفقاً للمنظومة المصرفية الموحدة، وكان نص هذه الفرضية كما يلي:

"لا تحسن آليات الرقابة من تطبيق معايير التوثيق".

ولاختبار هذه الفرضية تم التعبير عنها إحصائياً علي النحو التالي:

الفرضية الصفرية (H_0): لا تحسن آليات الرقابة من تطبيق معايير التوثيق.

الفرضية البديلة (H_1): تحسن آليات الرقابة من تطبيق معايير التوثيق.

ولاختبار هذه الفرضية خصصت لها المجموعة الخامسة من الجزء الثاني لاستمارة الاستبيان لاختبار الفرضية الفرعية الرابعة، حيث احتوت هذا المجموعة علي (3) أسئلة تم اعتبار كل سؤال منها كفرضية جزئية للفرضية الفرعية الخامسة، وكانت نتائج الاختبار كما يوضحها الجدول رقم (17-4):

جدول رقم (17-4)
نتائج اختبار الفرضية الفرعية الخامسة

م	الأسئلة المتعلقة بالفرضية	المراجعين الداخليين			مشرفي المنظومة		
		المتوسط الحسابي	الدلالة الإحصائية	القرار الإحصائي	المتوسط الحسابي	الدلالة الإحصائية	القرار الإحصائي
1	التحديد الجيد للإجراءات المتبعة في حالة عدم الالتزام بالسياسات الرقابية.	4.20	0.002	رفض H_0	4.40	0.000	رفض H_0
2	التحديد الجيد للمعايير والإجراءات الخاصة بعمليات التخزين والمناولة للبيانات.	3.53	0.056	قبول H_0	3.27	0.413	قبول H_0
3	تزويد المستخدم بالتوجيهات اللازمة للتبليغ عن أي اختراقات أمنية للنظام.	3.33	0.173	قبول H_0	3.27	0.364	قبول H_0

يوضح هذا الجدول نتائج اختبار الفرضية الفرعية الخامسة عند مستوى معنوية (0.05).

يوضح الجدول نتائج اختبار الفرضية الفرعية الرابعة حول فعالية آليات رقابة معايير التوثيق وفيما يلي تحليل لكل فئة علي حدا:

أولاً: فيما يتعلق بالمراجعين الداخليين:

أظهرت نتائج المراجعين الداخليين الجدول رقم (17- 4) أنه تم رفض عدد (2) فرضية صفرية من أصل (3) فرضيات صفرية وذلك بالنسبة للفرضيات الجزئية، حيث كان السؤال رقم (1) حول إتباع إجراءات جيدة في حالات عدم الالتزام بالسياسات الرقابية، قيمة المتوسط الحسابي لهذا السؤال أكبر من المتوسط النظري (3.5)، بالإضافة إلي قيمة P-value كانت ذات دلالة إحصائية معنوية أصغر من مستوى المعنوية (0.05)، وبالتالي تم رفض الفرضية الصفرية لهذا السؤال ورفض الفرضية البديلة لها.

وبالنسبة للسؤالين أرقام (2)،(3)، تم قبول الفرضيتين الصفريتين لهذين السؤالين وقبول الفرضيتين البديلتين لهما، حيث كانت قيمة المتوسط الحسابي لكل سؤال تقارب المتوسط النظري (3.5)، إلا أن قيمة P-value كانت ذات دلالة إحصائية غير معنوية أكبر من مستوى المعنوية

(0.05)، وهذا يعني أنه لا توجد إجراءات محدده ومتبعة في حالة عدم الالتزام بالسياسات الرقابية، وعدم تزويد المستخدمين بالتوجيهات اللازمة للتبليغ عن أي اختراقات أمنية للنظام بالمصارف المشاركة في الدراسة.

مما سبق وبناءً علي نتائج الاختبار تم رفض عدد (2) من الفرضيات الصفرية الجزئية من أصل عدد (3) فرضيات صفرية، مما يعني قبول الفرضية الصفرية (H_0) للفرضية الفرعية الرابعة ورفض الفرضية البديلة (H_1) لها، أي أنه من وجهت نظر المراجعين الداخليين فأنه لا تحسن آليات الرقابة من تطبيق معايير التوثيق في المصارف المشاركة في الدراسة.

ثانياً: فيما يتعلق بمشرفي المنظومة:

أظهرت نتائج مشرفي المنظومة الجدول رقم (17- 4) أنه تم رفض عدد (2) فرضية صفرية من أصل (3) فرضيات صفرية وذلك بالنسبة للفرضيات الجزئية، بالنسبة للسؤال رقم (1) تم رفض الفرضية الصفرية وقبول الفرضية البديلة لها، حيث كانت قيمة المتوسط الحسابي أكبر من المتوسط النظري (3.5)، بالإضافة إلي أن قيمة P-value كانت ذات دلالة إحصائية معنوية أصغر من مستوى المعنوية (0.05)، وهذا يدل علي تحديد إجراءات جيدة في حالات عدم الالتزام بالسياسات الرقابية في المصارف المشاركة بالدراسة.

وكان السؤالين (2)،(3)، حول التحديد الجيد للمعايير والإجراءات الخاصة بعمليات التخزين والمناولة للبيانات، وتزويد المستخدمين بالتوجيهات اللازمة للتبليغ عن أي اختراقات أمنية للنظام، كانت قيمة المتوسطات الحسابية لهذين السؤالين أصغر من المتوسط النظري (3.5)، بالإضافة إلي قيمة P-value كانت غير ذات دلالة إحصائية غير معنوية أكبر من مستوى المعنوية (0.05)، وبالتالي تم قبول الفرضيتين الصفريتين لهذين السؤالين ورفض الفرضيتين البديلة لهما.

مما سبق وبناءً علي نتائج الاختبار تم رفض عدد (2) من الفرضيات الصفرية الجزئية من أصل عدد (3) فرضيات صفرية، مما يعني قبول الفرضية الصفرية (H_0) للفرضية الفرعية الرابعة ورفض الفرضية البديلة (H_1) لها، أي أنه من وجهت نظر مشرفي المنظومة فأنه لا تحسن آليات الرقابة من تطبيق معايير التوثيق في المصارف المشاركة في الدراسة.

- **خلاصة نتائج اختبار الفرضية الفرعية الخامسة:**

يتضح من نتائج اختبار الفرضية الفرعية الخامسة، أن المراجعين الداخليين ومشرفي المنظومة، توصلوا إلي أن المصارف المشاركة في الدراسة بها نظام رقابة لا يمكن من خلاله تحقيق نظام رقابي فعال يتضمن الإجراءات الرقابية الملائمة لبيئة النظام وتطبيقاته، ولا يعمل

وفقاً لمواصفات التشغيل المعيارية، مما يدل علي عدم فعالية آليات الرقابة في تحسين تطبيق معايير التوثيق.

4.8.1.1.6 اختبــار الفرضية الفرعية السادسة:

تهدف هذه الفرضية إلي التعرف علي مدى فعالية آليات الرقابة في التغلب علي آثار الكارثة في المصارف الليبية التي تعمل وفقاً للمنظومة المصرفية الموحدة، فنصت علي ما يلي:

"لا تمكن آليات الرقابة من التغلب علي آثار الكارثة".

ولاختبار هذه الفرضية تم التعبير عنها إحصائياً علي النحو التالي:

الفرضية الصفرية (H_0): لا تمكن آليات الرقابة من التغلب علي آثار الكارثة.

الفرضية البديلة (H_1): تمكن آليات الرقابة من التغلب علي آثار الكارثة.

ولاختبار هذه الفرضية والوصول إلي القرار الملائم حولها، تم تخصيص المجموعة السادسة من الجزء الثاني لاستمارة الاستبيان لاختبار الفرضية الفرعية السادسة، حيث احتوت هذا المجموعة علي (9) أسئلة تم اعتبار كل سؤال منها كفرضية جزئية للفرضية الفرعية السادسة، وكانت نتائج الاختبار كما يوضحها الجدول رقم (18-4):

جدول رقـم (18-4)
نتائج اختبار الفرضية الفرعية السادسة

م	الأسئلة المتعلقة بالفرضية	المراجعين الداخليين			مشرفي المنظومة		
		المتوسط الحسابي	الدلالة الإحصائية	القرار الإحصائي	المتوسط الحسابي	الدلالة الإحصائية	القرار الإحصائي
1	توفير نسخ احتياطية من كل الملفات والبرامج مخزنة خارج المصرف لتمكين المصرف من استعادة الملفات والبرامج المدمرة أو التي تم فقدها عند حدوث الكارثة.	4.20	0.003	رفض H_0	4.33	0.001	رفض H_0
2	الاحتفاظ بالبرامج الأصلية في أماكن آمنة خارج المصرف حتى يمكن الاستفادة من تلك البرامج عند حدوث الكارثة.	3.67	0.106	قبول H_0	4.20	0.001	رفض H_0
3	توفير إجراءات رقابية ملائمة تطبق على خروج وعودة ملفات البيانات والبرامج من أماكن تخزينها إلي أماكن استخدامها.	3.40	0.288	قبول H_0	3.20	0.663	قبول H_0
4	وجود التطبيقات والأجهزة والبرامج الضرورية للحفاظ على استمرار المصرف في حالة حدوث أي حالات طارئة.	2.00	0.019	رفض H_0	2.07	0.014	رفض H_0
5	إجراء فحص واختبار دوري لخطة التغلب على آثار الكارثة للتأكد من إمكانية تنفيذها في الواقع العملي.	1.73	0.001	رفض H_0	1.27	0.000	رفض H_0
6	توافر بوليصة تامين شاملة تغطي تكاليف أجهزة ومعدات الحاسب الآلي بالإضافة إلي تكاليف انقطاع الإعمال الذي قد ينتج من حدوث كوارث بالحاسب الآلي.	1.67	0.001	رفض H_0	1.47	0.000	رفض H_0
7	التحديد الواضح للأشخاص المسئولين عند تنفيذ خطة التغلب علي آثار الكارثة مع تحديد مسؤولية كل فرد من هؤلاء الأشخاص.	1.60	0.000	رفض H_0	1.40	0.000	رفض H_0
8	التحديد الجيد لكل الأنشطة اللازمة لاستعادة الإعمال وتتابع تنفيذ تلك الأنشطة والوقت اللازم لتنفيذ كل نشاط.	1.53	0.000	رفض H_0	1.67	0.001	رفض H_0
9	الأماكن التي يمكن من خلالها متابعة مزاولة نشاط المصرف في حالة ما إذا كان الضرر يلحق بمباني المصرف.	1.47	0.000	رفض H_0	1.47	0.000	رفض H_0

يوضح هذا الجدول نتائج اختبار الفرضية الفرعية السادسة عند مستوى معنوية (0.05).

يوضح الجدول السابق نتائج اختبار الفرضية الفرعية السادسة، وفيما يلي تحليل لكل فئة علي حدا:

أولاً: فيما يتعلق بالمراجعين الداخليين:

أظهرت نتائج المراجعين الداخليين الجدول رقم (18- 4) أنه تم رفض عدد (7) فرضيات صفرية من أصل (9) فرضية صفرية وذلك بالنسبة للفرضيات الجزئية، كان السؤال رقم (1) حول توفير نسخ احتياطية من كل الملفات والبرامج مخزنه خارج المصرف لتمكين المصرف من

استعادة الملفات والبرامج المدمرة أو التي تم فقدها عند حدوث الكارثة، أن قيمة المتوسط الحسابي لهذا السؤال أكبر من المتوسط النظري (3.5)، بالإضافة إلي قيمة P-value كانت ذات دلالة إحصائية معنوية أصغر من مستوى المعنوية (0.05)، وبالتالي تم رفض الفرضية الصفرية لهذا السؤال وقبول الفرضية البديلة له، بالإضافة إلي الأسئلة أرقام (4)،(5)،(6)،(7)،(8)،(9)، تم رفض الفرضيات الصفرية لهذه الأسئلة وقبول الفرضيات البديلة لها، علي رغم من أن قيمة المتوسطات الحسابية كانت أصغر من المتوسط النظري(3.5)، إلا أن قيمة P-value كانت ذات دلالة إحصائية معنوية أصغر من مستوى المعنوية (0.05)، مما يدل علي توافر التطبيقات والأجهزة والبرامج الضرورية للحفاظ علي استمرار المصرف في حالة حدوث أي حالات طارئة، وإجراء فحص واختبار دوري لخطة التغلب علي آثار الكارثة للتأكد من إمكانية تنفيذها في الواقع العملي، وتوفير بوليصة تأمين شاملة تغطي تكاليف أجهزة ومعدات الحاسب الآلي بالإضافة إلي تكاليف انقطاع الإعمال الذي قد ينتج من حدوث كوارث بالنظام، وتحديد واضح للأشخاص المسئولين عن تنفيذ خطة التغلب علي آثار الكارثة مع تحديد مسؤولية كل فرد من هؤلاء الأشخاص، وجود تحديد جيد لكل الأنظمة اللازمة لاستعادة الإعمال وتنفيذ الأنشطة في الوقت اللازم، وتحديد أماكن جيدة يمكن من خلالها متابعة مزاولة نشاط المصرف في حالة ما إذا كان الضرر يلحق بمباني المصرف في المصارف المشاركة بالدراسة.

أما بالنسبة للسؤالين أرقام (2)،(3) حول الاحتفاظ بالبرامج الأصلية في أماكن آمنة خارج المصرف حتى يمكن الاستفادة من تلك البرامج عند حدوث الكارثة، وتوفير إجراءات رقابية ملائمة تطبق علي خروج وعودة ملفات البيانات والبرامج من أماكن تخزينها إلي أماكن استخدامها، كانت قيمة المتوسطات الحسابية أصغر من المتوسط النظري (3.5)، بالإضافة إلي قيمة P-value كانت ذات دلالة إحصائية غير معنوية أكبر من مستوى المعنوية (0.05)، وبالتالي تم قبول الفرضيتين الصفريتين لهذين السؤالين ورفض الفرضيتين البديلتين لهما.

مما سبق وبناءً علي نتائج الاختبار تم رفض عدد (7) فرضيات صفرية للفرضيات الجزئية من أصل (9) فرضيات صفرية، مما يعني رفض الفرضية الصفرية (H_0) للفرضية الفرعية السادسة، وقبول الفرضية البديلة (H_1) لها، أي أنه من وجهت نظر المراجعين الداخليين فأنه تمكن آليات الرقابة من التغلب علي آثار الكارثة في المصارف المشاركة في الدراسة.

ثانياً: فيما يتعلق بمشرفي المنظومة:

أظهرت نتائج مشرفي المنظومة الجدول (18- 4) أنه تم رفض عدد (8) فرضيات صفرية من أصل (9) فرضيات صفرية وذلك بالنسبة للفرضيات الجزئية، كان السؤالين أرقام (1)،(2)، حول توفير نسخ احتياطية من كل الملفات والبرامج مخزنة خارج المصرف لتمكين

المصرف من استعادة الملفات والبرامج المدمرة أو التي تم فقدها عند حدوث الكارثة، والاحتفاظ بالبرامج الأصلية في أماكن آمنة خارج المصرف حتى يمكن الاستفادة من تلك البرامج عند حدوث الكارثة، أن المتوسطات الحسابية لهذين السؤالين أكبر من المتوسط النظري (3.5)، بالإضافة إلي قيمة P-value كانت ذات دلالة إحصائية معنوية أصغر من مستوى المعنوية (0.05)، وبالتالي تم رفض الفرضيتين الصفريتين لهذين السؤالين وقبول الفرضيتين البديلتين لهما، أما الأسئلة (4)،(5)،(6)،(7)،(8)،(9)، فأنة تم رفض الفرضيات الصفرية لهذه الأسئلة وقبول الفرضيات البديلة لها، علي الرغم من أن قيمة المتوسطات الحسابية لهذه الأسئلة كانت أصغر من المتوسط النظري (3.5)، إلا أن قيمة P-value كانت ذات دلالة إحصائية معنوية أصغر من مستوى المعنوية (0.05)، مما يدل علي وجود هذه الآليات في المصارف المشاركة في الدراسة.

وكان السؤال رقم (3)، حول توفير إجراءات رقابية ملائمة تطبق علي خروج وعودة ملفات البيانات والبرامج من أماكن تخزينها إلي أماكن استخدامها، كانت قيمة المتوسط الحسابي لهذا السؤال أصغر من المتوسط النظري (3.5)، بالإضافة إلي قيمة P-value كانت ذات دلالة إحصائية غير معنوية أكبر من مستوى المعنوية (0.05)، وبالتالي تم رفض الفرضية الصفرية لهذا السؤال وقبول الفرضية البديلة له.

مما سبق وبناءً علي نتائج الاختبار فأنه تم رفض عدد (8) فرضيات صفرية من أصل (9) فرضيات صفرية للفرضيات الجزئية، مما يعني رفض الفرضية الصفرية (H_0) للفرضية الفرعية السادسة، وقبول الفرضية البديلة (H_1) لها، أي أنه من وجهت نظر مشرفي المنظومة فأنه تمكن آليات الرقابة من التغلب علي آثار الكارثة في المصارف المشاركة في الدراسة.

- **<u>خلاصة نتائج اختبار الفرضية الفرعية السادسة:</u>**

يتضح من نتائج اختبار الفرضية الفرعية السادسة، أن المراجعين الداخليين ومشرفي المنظومة متفقون علي أن المصارف المشاركة في الدراسة بها نظام رقابة يمكن من خلاله التغلب علي آثار الكارثة لتحقيق نظام فعال وضمان توافر التطبيقات والبرامج والأجهزة الضرورية للحفاظ علي تشغيل المصرف في الحالات الطارئة وتحديد مسؤولية كل فرد بالإضافة إلي تحديد الوقت اللازم لاستعادة الإعمال عند المستوى الطبيعي لها مما يدل علي فعالية آليات الرقابة في التغلب علي آثار الكارثة.

4.8.1.1.7 اختبــار الفرضية الفرعية السابعة:

الهدف من الفرضية الفرعية السابعة التعرف علي مدى فعالية آليات الرقابة في الحد من الاختراقات الأمنية في عمليات التجارة الالكترونية والاتصالات والإنترنت في المصارف الليبية التي تعمل وفقاً للمنظومة المصرفية الموحدة، فكان نص هذه الفرضية كما التالي:

"لا تخفض آليات الرقابة من الاختراقات الأمنية في عمليات التجارة الالكترونية والاتصالات والانترنت".

ولاختبار هذه الفرضية تم التعبير عنها إحصائياً علي النحو التالي:

الفرضية الصفرية (H_0): لا تخفض آليات الرقابة من الاختراقات الأمنية في عمليات التجارة الالكترونية والاتصالات والانترنت.

الفرضية البديلة (H_1): تخفض آليات الرقابة من الاختراقات الأمنية في عمليات التجارة الالكترونية والاتصالات والانترنت.

وتم تخصيص المجموعة السابعة من الجزء الثاني لاستمارة الاستبيان لاختبار الفرضية الفرعية السابعة، حيث احتوت هذا المجموعة علي (9) أسئلة تم اعتبار كل سؤال منها كفرضية جزئية للفرضية الفرعية السابعة، و الجدول رقم (19-4) يوضح نتائج التحليل الإحصائي:

جدول رقـــم (19-4)
نتائج اختبار الفرضية الفرعية السابعة

م	الأسئلة المتعلقة بالفرضية	المراجعين الداخليين			مشرفي المنظومة		
		المتوسط الحسابي	الدلالة الإحصائية	القرار الإحصائي	المتوسط الحسابي	الدلالة الإحصائية	القرار الإحصائي
1	يتم وقف التعامل علي أي حساب غير مستخدم لمدة (6) شهور.	4.93	0.000	رفض H_0	4.93	0.000	رفض H_0
2	وضع برامج الحماية ضد الفيروسات بما فيها البرامج الخاصة بفحص رسائل البريد الالكتروني الواردة، بالإضافة إلي التحديث المستمر لتلك البرامج.	4.80	0.000	رفض H_0	4.93	0.000	رفض H_0
3	تنشيط الحسابات الالكترونية يتم بعد التسجيل علي الموقع ويستطيع المستخدم الخروج بالخاصية الملائمة (Sign out) أو بعد مرور وقت قصير جداً من التوقف عن الاستخدام.	4.67	0.000	رفض H_0	4.80	0.000	رفض H_0
4	منع الدخول علي حساب بعد ثلاث محاولات غير ناجحة لإدخال الهوية مع تسجيل تلك المحاولات حتى يتم متابعتها.	4.40	0.000	رفض H_0	4.87	0.000	رفض H_0
5	توفير بطاقتي هوية (ID) لكل مستخدم لعمليات المصرف الالكترونية الأولي تستخدم في الاستعلامات العامة والثانية تستخدم في إجراء التحويلات والصفقات النقدية.	3.93	0.001	رفض H_0	3.73	0.010	رفض H_0
6	استخدام التشفير لتشفير المعلومات السرية والخاصة وهويات المستخدمين وكلمات المرور.	3.73	0.016	رفض H_0	4.20	0.000	رفض H_0
7	حصر التحويلات النقدية علي الحسابات في نفس المصرف (المرسل والمرسل إليه في نفس المصرف).	3.47	0.131	قبول H_0	3.60	0.023	رفض H_0
8	وضع حد للصفقات النقدية الالكترونية التي تتم في اليوم الواحد علي نفس الحساب.	3.13	0.670	قبول H_0	3.20	0.384	قبول H_0
9	استخدام حوائط النار (أجهزة - برامج) لرقابة وحماية الاتصالات بين الشبكة الداخلية والشبكات الخارجية مثل الانترنت.	2.93	0.843	قبول H_0	3.07	0.827	قبول H_0

يوضح هذا الجدول نتائج اختبار الفرضية الفرعية السابعة عند مستوى معنوية (0.05).

يوضح الجدول نتائج اختبار الفرضية الفرعية السابعة، وفيما يلي تحليل لكل فئة علي حدا:

أولاً: فيما يتعلق بالمراجعين الداخليين:

أظهرت نتائج المراجعين الداخليين الجدول رقم (19- 4) أنه تم رفض عدد (6) فرضيات صفرية من أصل (9) فرضية صفرية وذلك بالنسبة للفرضيات الجزئية، بالنسبة للأسئلة أرقام (1)،(2)،(3)،(4)،(5)،(6)، تم رفض الفرضيات الصفرية لهذه الأسئلة وقبول الفرضيات البديلة لها، حيث كانت قيمة المتوسطات الحسابية لهذه الأسئلة أكبر من المتوسط النظري (3.5)، و قيمة P-value كانت ذات دلالة إحصائية معنوية أصغر من مستوى المعنوية (0.05)، مما يدل علي

وقف التعامل مع أي حساب غير مستخدم (خامل) لمدة ستة أشهر، ووضع برامج الحماية ضد الفيروسات بما فيها البرامج الخاصة بفحص رسائل البريد الالكتروني الواردة بالإضافة إلي التحديث المستمر لتلك البرامج، وكذلك تنشيط الحسابات الالكترونية بعد التسجيل علي الموقع مع تفعيل خاصية الملائمة (Sign out)، للخروج بعد مرور مدة قصيرة جداً من التوقف عن الاستخدام، ويتم منع الدخول علي الحساب بعد ثلاثة محاولات غير ناجحة لإدخال الهوية مع تسجيل تلك المحاولات حتى يتم متابعتها، وتوفير بطاقتي هوية (ID) لكل مستخدم لعمليات المصرف الالكتروني الأولى تستخدم في الاستعلامات العامة والثانية تستخدم في إجراء التحويلات والصفقات النقدية، واستخدام التشفير لتشفير المعلومات السرية والخاصة وهويات المستخدمين وكلمات المرور في المصارف المشاركة في الدراسة.

أما الأسئلة أرقام (7)،(8)،(9)، حول حصر التحويلات النقدية علي الحسابات في نفس المصرف (المرسل والمرسل إليه في نفس المصرف)، ووضع حد للصفقات النقدية الالكترونية التي تتم في اليوم الواحد علي نفس الحساب، واستخدام حوائط النار وحماية الاتصالات بين الشبكة الداخلية والشبكات الخارجية مثل الانترنت، كانت قيمة المتوسطات الحسابية أصغر من المتوسط النظري (3.5)، بالإضافة إلي قيمة P-value غير ذات دلالة إحصائية غير معنوية أكبر من مستوى المعنوية (0.05)، وبالتالي تم قبول الفرضيات الصفرية لهذه الأسئلة ورفض الفرضيات البديلة لها.

مما سبق وبناءً علي نتائج الاختبار تم رفض عدد (6) فرضيات صفرية للفرضيات الجزئية من أصل (9) فرضيات صفرية، مما يعني رفض الفرضية الصفرية (H_0) للفرضية الفرعية السابعة، وقبول الفرضية البديلة (H_1) لها، أي أنه من وجهت نظر المراجعين الداخليين فأنه تخفض آليات الرقابة من الاختراقات الأمنية في عمليات التجارة الالكترونية والاتصالات الانترنت في المصارف المشاركة في الدراسة.

ثانياً: فيما يتعلق بمشرفى المنظومة:

أظهرت نتائج مشرفي المنظومة الجدول رقم (19- 4) أنه تم رفض عدد (7) فرضيات صفرية من أصل (9) فرضيات صفرية وذلك بالنسبة للفرضيات الجزئية، حيث كانت الأسئلة أرقام (1)،(2)،(3)،(4)،(5)،(6)،(7)، قيمة المتوسطات الحسابية لها أكبر من المتوسط النظري (3.5)، وكانت قيمة P-value ذات دلالة إحصائية معنوية أصغر من مستوى المعنوية (0.05)، مما يعني رفض الفرضيات الصفرية لهذه الأسئلة وقبول الفرضيات البديلة لها.

وكان السؤالين أرقام (8)،(9)، حول وضع حد للصفقات النقدية الالكترونية التي تتم في اليوم الواحد علي نفس الحساب، واستخدام حوائط النار وحماية الاتصالات بين الشبكة الداخلية

والشبكات الخارجية مثل الانترنت، كانت قيمة المتوسطات الحسابية أصغر من المتوسط النظري (3.5)، وكانت قيمة P-value ذات دلالة إحصائية غير معنوية أكبر من مستوى المعنوية (0.05)، وبالتالي تم قبول الفرضيتين الصفريتين لهذين السؤالين ورفض الفرضيتين البديلة لهما.

مما سبق وبناءً علي نتائج الاختبار تم رفض عدد (7) فرضيات صفرية من أصل (9) فرضيات صفرية للفرضيات الجزئية، مما يعني رفض الفرضية الصفرية (H_0) للفرضية الفرعية السابعة، وقبول الفرضية البديلة (H_1) لها، أي أنه من وجهت نظر مشرفي المنظومة تخفض آليات الرقابة من الاختراقات الأمنية في عمليات التجارة الالكترونية والاتصالات والانترنت في المصارف المشاركة في الدراسة.

- **<u>خلاصة نتائج اختبار الفرضية الفرعية السابعة:</u>**

يتضح من نتائج اختبار الفرضية الفرعية السابعة أن المراجعين الداخليين ومشرفي المنظومة، توصلوا إلي أن المصارف المشاركة في الدراسة بها نظام رقابة يمكن من خلاله التقليل من الاختراقات الأمنية في عمليات الاتصالات والانترنت والمصارف الالكترونية، مما يدعم فعالية آليات الرقابة للمنظومة المصرفية الموحدة.

4.8.1.1.8 اختبــار الفرضية الفرعية الثامنة:

تهدف الفرضية الفرعية الثامن إلي التعرف علي مدى فعالية آليات الرقابة في تحسين أمن النتائج في المصارف الليبية التي تعمل وفقاً للمنظومة المصرفية الموحدة، وكان نص هذه الفرضية كالتالي:

"لا تحسن آليات الرقابة من أمن النتائج".

ولاختبار هذه الفرضية تم التعبير عنها إحصائياً علي النحو التالي:

الفرضية الصفرية (H_0): لا تحسن آليات الرقابة من أمن النتائج.

الفرضية البديلة (H_1): تحسن آليات الرقابة من أمن النتائج.

ولاختبار هذه الفرضية تم تخصيص المجموعة الثامنة من الجزء الثاني لاستمارة الاستبيان لاختبار الفرضية الفرعية الثامنة، حيث احتوت هذا المجموعة علي (5) أسئلة تم اعتبار كل سؤال منها كفرضية جزئية للفرضية الفرعية الثامنة، وكانت نتائج الاختبار كما يوضحها الجدول رقم (4-20):

جدول رقـم (20-4)
نتائج اختبار الفرضية الفرعية الثامنة

م	الأسئلة المتعلقة بالفرضية	المراجعين الداخليين			مشرفي المنظومة		
		المتوسط الحسابي	الدلالة الإحصائية	القرار الإحصائي	المتوسط الحسابي	الدلالة الإحصائية	القرار الإحصائي
1	كل مخرجات أنظمة المعلومات الهامة يتم الاحتفاظ بها في حجرات مقفلة.	4.60	0.000	رفض H_0	4.47	0.000	رفض H_0
2	الدخول المصرح به للمعلومات الهامة يجب أن يتم مراقبته وتحديده للمستخدمين المصرح لهم خلال فترة التصريح.	4.47	0.000	رفض H_0	4.40	0.000	رفض H_0
3	استخدام الآلات المخصصة للتخلص من الورق للتخلص من الأوراق التي تم الانتهاء منها.	3.93	0.017	رفض H_0	4.40	0.000	رفض H_0
4	طباعة وتوزيع النسخ الورقية لمخرجات المنظومة يتم ختمها بالوقت والتاريخ في ظل إشراف ملائم.	3.80	0.041	رفض H_0	4.13	0.002	رفض H_0
5	إجراء مراجعة عشوائية للمدخلات والمخرجات للتحقق من التشغيل الصحيح.	2.33	0.086	قبول H_0	2.20	0.028	رفض H_0

يوضح هذا الجدول نتائج اختبار الفرضية الفرعية الثامنة عند مستوى معنوية (0.05).

يوضح الجدول السابق نتائج اختبار الفرضية الفرعية الثامنة، وفيما يلي تحليل لكل فئة علي حدا:

أولاً: فيما يتعلق بالمراجعين الداخليين:

أظهرت نتائج المراجعين الداخليين الجدول رقم (20- 4) أنه تم رفض عدد (4) فرضيات صفرية من أصل (5) فرضيات صفرية وذلك بالنسبة للفرضيات الجزئية، حيث تم رفض الفرضيات الصفرية للأسئلة أرقام (1)،(2)،(3)،(4)، وقبول الفرضيات البديلة لها، حيث كانت قيمة المتوسطات الحسابية لها أكبر من المتوسط النظري (3.5)، و قيمة P-value كانت ذات دلالة إحصائية معنوية أصغر من مستوى المعنوية (0.05)، مما يدل علي أن مخرجات المنظومة المصرفية الموحدة يتم الاحتفاظ بها في حجرات مقفلة، ويتم مراقبة وتحديد المستخدمين المصرح لهم الدخول للمعلومات الهامة خلال فترة التصريح، واستخدام الآلات المخصصة للتخلص من الأوراق التي تم الانتهاء منها، وطباعة وختم النسخ الورقية لمخرجات المنظومة بالوقت والتاريخ بالمصارف المشاركة في الدراسة.

أما السؤال رقم (5) حول إجراء مراجعة عشوائية للمدخلات والمخرجات للتحقق من التشغيل الصحيح كانت قيمة المتوسط الحسابي أصغر من المتوسط النظري (3.5)، وكانت قيمة

P-value ذات دلالة إحصائية غير معنوية أكبر من مستوى المعنوية (0.05)، وبالتالي تم قبول الفرضية الصفرية لهذا السؤال ورفض الفرضية البديلة له.

مما سبق وبناءً علي نتائج الاختبار تم رفض عدد (4) فرضيات صفرية للفرضيات الجزئية من أصل (5) فرضيات صفرية، مما يعني رفض الفرضية الصفرية (H_0) للفرضية الفرعية الثامنة، وقبول الفرضية البديلة (H_1) لها، أي أنه من وجهت نظر المراجعين الداخليين فأنه تحسن آليات الرقابة من أمن النتائج في المصارف المشاركة في الدراسة.

ثانياً: فيما يتعلق بمشرفى المنظومة:

أظهرت نتائج مشرفي المنظومة الجدول رقم (20- 4) بأنه تم رفض كل الفرضيات صفرية وذلك بالنسبة للفرضيات الجزئية للفرضية الفرعية السابعة، حيث كانت الأسئلة أرقام (1)،(2)،(3)،(4)، قيمة المتوسطات الحسابية لها أكبر من المتوسط النظري (3.5)، بالإضافة إلي قيمة P-value كانت ذات دلالة إحصائية معنوية أصغر من مستوى المعنوية (0.05)، مما يعني رفض الفرضيات الصفرية لهذه الأسئلة وقبول الفرضيات البديلة لها، أما السؤال رقم (5) حول إجراء مراجعة عشوائية للمدخلات والمخرجات للتحقق من التشغيل الصحيح، كانت قيمة المتوسط الحسابي أصغر من المتوسط النظري (3.5)، إلا أن قيمة P-value كانت ذات دلالة إحصائية معنوية أصغر من مستوى المعنوية (0.05)، وبالتالي تم رفض الفرضية الصفرية لهذا السؤال وقبول الفرضية البديلة له أيضاً.

مما سبق وبناءً علي نتائج الاختبار تم رفض كل الفرضيات الصفرية للفرضيات الجزئية، مما يعني رفض الفرضية الصفرية (H_0) للفرضية الفرعية الثامنة، وقبول الفرضية البديلة (H_1) لها، أي أنه من وجهت نظر مشرفي المنظومة تحسن آليات الرقابة من أمن النتائج في المشاركة في الدراسة.

- **خلاصة نتائج اختبار الفرضية الفرعية الثامنة:**

يتضح من نتائج اختبار الفرضية الفرعية الثامنة أن المراجعين الداخليين ومشرفي المنظومة متفقون علي أن المصارف المشاركة في الدراسة بها نظام رقابة يمكن خلاله تحسين أمن النتائج لحماية كافة مخرجات المنظومة الموحدة من الوصول غير المصرح به وهذا يدل علي فعالية آليات الرقابة في تحسين أمن النتائج.

4.8.1.1.9 اختبـار الفرضية الفرعية التـاسعة:

تهدف هذه الفرضية إلي التعرف علي مدى فعالية آليات الرقابة في تحسين أمن خدمات التعهيد في المصارف الليبية التي تعمل وفقاً للمنظومة المصرفية الموحدة، وكان نصها كما يلي:

"لا تحسن آليات الرقابة من أمن خدمات التعهيد".

ولاختبار هذه الفرضية تم التعبير عنها إحصائياً علي النحو التالي:

الفرضية الصفرية (H_0): لا تحسن آليات الرقابة من أمن خدمات التعهيد.

الفرضية البديلة (H_1): تحسن آليات الرقابة من أمن خدمات التعهيد.

ولاختبار هذه الفرضية تم تخصيص المجموعة التاسعة من الجزء الثاني لاستمارة الاستبيان لاختبار الفرضية الفرعية التاسعة، حيث احتوت هذا المجموعة علي (5) أسئلة تم اعتبار كل سؤال منها كفرضية جزئية للفرضية الفرعية التاسعة، والجدول رقم (21- 4) يوضح نتائج الاختبار الإحصائي:

جدول رقم (21-4)
نتائج اختبار الفرضية الفرعية التاسعة

م	الأسئلة المتعلقة بالفرضية	المراجعين الداخليين			مشرفي المنظومة		
		المتوسط الحسابي	الدلالة الإحصائية	القرار الإحصائي	المتوسط الحسابي	الدلالة الإحصائية	القرار الإحصائي
1	وجود تحديد واضح لمسؤوليات والتزامات كلا الطرفين في تعاقدات خدمات التعهيد،	2.80	0.531	قبول H_0	2.67	0.265	قبول H_0
2	توثيق متطلبات الرقابة المستهدفة من قبل المصرف والتي يجب أن يلتزم بها موفر خدمات التعهيد.	2.73	0.452	قبول H_0	2.47	0.135	قبول H_0
3	توفير التصريحات اللازمة لمقدم خدمات التعهيد حتى يتمكن من أداء الإعمال المكلف بها.	2.73	0.469	قبول H_0	2.47	0.120	قبول H_0
4	تحديد مستوى الأداء الرقابي.	2.07	0.029	رفض H_0	1.53	0.000	رفض H_0
5	تقييم الأداء الرقابي لموفر خدمات التعهيد من قبل المصرف.	2.00	0.015	رفض H_0	1.83	0.024	رفض H_0

يوضح هذا الجدول نتائج اختبار الفرضية الفرعية التاسعة عند مستوى معنوية (0.05).

يوضح الجدول نتائج اختبار الفرضية الفرعية التاسعة، وفيما يلي تحليل لكل فئة علي حدا:

أولاً: فيما يتعلق بالمراجعين الداخليين:

أظهرت نتائج المراجعين الداخليين الجدول رقم (21- 4) أنه تم قبول عدد (3) فرضيات صفرية من أصل (5) فرضيات صفرية وذلك بالنسبة للفرضيات الجزئية، حيث كانت الأسئلة أرقام (1)،(2)،(3)، حول وجود تحديد واضح لمسؤوليات والالتزامات كلا الطرفين في تعاقدات خدمات التعهيد، وتوثيق متطلبات الرقابة المستهدفة من قبل المصرف والتي يجب أن يلتزم بها

موفر خدمات التعهيد، وتوفير التصريحات اللازمة لمقدم خدمات التعهيد حتى يتمكن من أداء الإعمال المكلف بها، قيمة المتوسطات الحسابية لها أصغر من المتوسط النظري (3.5)، بالإضافة إلي قيمة P-value ذات دلالة إحصائية غير معنوية أكبر من مستوى المعنوية (0.05)، وبالتالي تم قبول الفرضيات الصفرية لهذه الأسئلة ورفض الفرضيات البديلة لها.

أما السؤالين أرقام (4)،(5)، فأنه تم رفض الفرضيتين الصفريتين لهذين السؤالين وقبول الفرضيتين البديلتين لهما، حيث كانت قيمة المتوسطات الحسابية لهما أصغر من المتوسط النظري (3.5)، إلا أن قيمة P-value كانت ذات دلالة إحصائية معنوية أصغر من مستوى المعنوية (0.05)، مما يدل علي أن موفر خدمات التعهيد يحدد مستوى الأداء الرقابي وتقييمه من قبل المصرف في المصارف المشاركة في الدراسة.

مما سبق وبناءً علي نتائج الاختبار تم قبول عدد (3) فرضيات صفرية للفرضيات الجزئية من أصل (5) فرضيات صفرية، مما يعني قبول الفرضية الصفرية (H_0) للفرضية الفرعية التاسعة، ورفض الفرضية البديلة (H_1) لها، أي أنه من وجهت نظر المراجعين الداخليين فأنه لا تحسن آليات الرقابة من أمن خدمات التعهيد في المصارف المشاركة في الدراسة.

ثانياً: فيما يتعلق بمشرفي المنظومة:

أظهرت نتائج مشرفي المنظومة الجدول رقم (21- 4) بأنه تم قبول عدد (3) فرضيات صفرية من أصل (5) فرضيات صفرية وذلك بالنسبة للفرضيات الجزئية حيث كانت الأسئلة أرقام (1)،(2)،(3)، حول وجود تحديد واضح لمسؤوليات والالتزامات كلا الطرفين في تعاقدات خدمات التعهيد، وتوثيق متطلبات الرقابة المستهدفة من قبل المصرف والتي يجب أن يلتزم بها موفر خدمات التعهيد، وتوفير التصريحات اللازمة لمقدم خدمات التعهيد حتى يتمكن من أداء الإعمال المكلف بها، كانت قيمة المتوسطات الحسابية أصغر من المتوسط النظري (3.5)، إلا أن قيمة P-value كانت ذات دلالة إحصائية غير معنوية أكبر من مستوى المعنوية (0.05)، وبالتالي تم قبول الفرضيات الصفرية لهذه الأسئلة وقبول الفرضيات البديلة لها.

أما السؤالين أرقام (4)،(5)، حول إتاحة موفر خدمات التعهيد تحديد مستوى الأداء الرقابي، وتقييم ذلك المستوى من قبل المصرف، كانت قيمة المتوسطات الحسابية لهذين السؤالين أصغر من المتوسط النظري (3.5)، إلا أن قيمة P-value كانت ذات دلالة إحصائية معنوية أصغر من مستوى المعنوية (0.05)، وبالتالي تم رفض الفرضيتين الصفريتين لهذين السؤالين وقبول الفرضيتين البديلتين لهما.

مما سبق وبناءً علي نتائج الاختبار تم قبول عدد (3) فرضيات صفرية للفرضيات الجزئية من أصل عدد (5) فرضيات صفرية، مما يعني قبول الفرضية الصفرية (H_0) للفرضية

الفرعية التاسعة، ورفض الفرضية البديلة (H_1) لها، أي أنه من وجهت نظر مشرفي المنظومة لا تحسن آليات الرقابة من أمن خدمات التعهيد في المصارف المشاركة في الدراسة.

- **<u>خلاصة نتائج اختبار الفرضية الفرعية التاسعة:</u>**

يتضح من نتائج اختبار الفرضية الفرعية التاسعة أن نتائج المراجعين الداخليين ونتائج مشرفي المنظومة توصلوا إلي أن المصارف المشاركة في الدراسة بها نظام رقابة لا يمكن من خلاله تحسين أمن خدمات التعهيد ورقابة أنشطتها لضمان سرية وسلامة المنظومة الموحدة، وهذا يدل علي عدم فعالية آليات الرقابة في تحسين أمن خدمات التعهيد في المصارف المشاركة في الدراسة.

4.8.1.2 اختبــار الفرضيــة الرئيسيــة:

اعتمدت هذه الدراسة علي فرضية رئيسية واحدة، تم صياغتها علي النحو التالي:

"عدم فعالية الرقابة للمنظومة المصرفية الموحدة في ليبيا".

ولاختبار هذه الفرضية تم التعبير عنها إحصائياً علي النحو التالي:

الفرضية الصفرية (H_0): عدم فعالية الرقابة للمنظومة المصرفية الموحدة في ليبيا.

الفرضية البديلة (H_1): الرقابة في المنظومة المصرفية الموحدة في ليبيا فعالة.

ولقبول أو رفض الفرضية الرئيسية للدراسة، تم صياغة تسع فرضيات فرعية، واختبارها إحصائياً باستخدام اختبار (T) عند مستوى معنوية (0.05)، والجدول رقم (22-4) يوضح ملخص نتائج اختبار الفرضيات الفرعية لبيانات المجمعة باستمارة الاستبيان:

جدول رقـم (4-22)

ملخص نتائج اختبار الفرضيات الفرعية

م	الفرضيات الفرعية للدراسة	المراجعين الداخليين	مشرفي المنظومة
1	لا تخفض آليات الرقابة من الخطأ والغش.	رفض H_0	رفض H_0
2	لا تخفض آليات الرقابة من الوصول المادي.	رفض H_0	رفض H_0
3	لا تخفض آليات الرقابة من الوصول المنطقي.	رفض H_0	رفض H_0
4	لا تحسن آليات الرقابة من أمن البيانات.	رفض H_0	رفض H_0
5	لا تحسن آليات الرقابة من تطبيق معايير التوثيق.	قبول H_0	قبول H_0
6	لا تمكن آليات الرقابة من التغلب علي آثار الكارثة	رفض H_0	رفض H_0
7	لا تخفض آليات الرقابة من الاختراقات الأمنية في عمليات التجارة الالكترونية والاتصالات والانترنت.	رفض H_0	رفض H_0
8	لا تحسن آليات الرقابة من أمن النتائج.	رفض H_0	رفض H_0
9	لا تحسن آليات الرقابة من أمن خدمات التعهيد.	قبول H_0	قبول H_0

يوضح هذا الجدول ملخص نتائج اختبار الفرضيات الفرعية عند مستوى معنوية (0.05).

يوضح الجدول ملخص نتائج الفرضيات الفرعية للدراسة، وفيما يلي تحليل لكل فئة علي حدا:

أولاً: فيما يتعلق بالمراجعين الداخليين:

أظهرت نتائج اختبار الفرضيات الفرعية للمراجعين الداخليين أنه تم رفض عدد (7) فرضيات صفرية (H_0) من أصل (9) فرضيات صفرية وذلك بالنسبة للفرضيات الفرعية للدراسة، الأمر الذي ترتب عليه منطقياً رفض الفرضية الصفرية (H_0) للفرضية الرئيسية لهذه الدراسة وقبول الفرضية البديلة (H_1) لها، أي أنه حسب نتائج اختبار المراجعين الداخليين أن:

" الرقابة في المنظومة المصرفية الموحدة في المصارف الليبية فعالة "

ثانياً: فيما يتعلق بمشرفي المنظومة:

أظهرت نتائج اختبار الفرضيات الفرعية لمشرفي المنظومة أنه تم رفض عدد (7) فرضيات صفرية من أصل (9) فرضيات صفرية وذلك بالنسبة للفرضيات الفرعية للدراسة، الأمر الذي

ترتب عليه منطقياً رفض الفرضية الصفرية (H_0) للفرضية الرئيسية لهذه الدراسة وقبول الفرضية البديلة (H_1) لها، أي أنه حسب نتائج اختبار مشرفي المنظومة أن:

" الرقابة في المنظومة المصرفية الموحدة في المصارف الليبية فعالة "

- **<u>خلاصة نتائج اختبار الفرضية الرئيسية للدراسة:</u>**

يتضح من نتائج اختبار الفرضية الرئيسية للدراسة أن المراجعين الداخليين ومشرفي المنظومة توصلوا إلي أن الرقابة في المنظومة المصرفية الموحدة فعالة في المصارف الليبية المشاركة في الدراسة.

4.8.2 تحليـــل بيانـات الدراســة المجمعة بالملاحظـــة:

تم تحليل البيانات التي تم تجميعها بالملاحظة وذلك بالاعتماد علي الأسئلة الواردة في الاستبيان كأساس لتجميع الملاحظة وذلك من خلال المشاهدة الشخصية لآليات الرقابة المطبقة من واقع العمل المصرفي، حيث احتوت علي عدد (9) آليات رقابة التي من شأنها الحكم علي فعالية الرقابة في المنظومة المصرفية الموحدة وقد بلغت مفردات الملاحظة (15) مفردة لعدد (15) فرع مصرفي.

وفيما يلي عرض للخطوات الأساسية التي تم إتباعها عند تحليل بيانات الملاحظة:

1- تم اخذ نتائج الملاحظة التي ظهرت خلاف نتائج استمارة الاستبيان دون إعادة ذكر نتائج الملاحظة التي ظهرت مطابقة لنتائج استمارة الاستبيان وذلك للتعرف علي أوجوه الاختلاف بين نتائج الأداتين.
2- تم إجراء تحليل لكل سؤال (إجراء رقابي) من الأسئلة الخاصة بكل آلية من آليات الرقابة التسعة وذلك عند نسبة (70%) من إجمالي الملاحظات لكل سؤال (أجراء رقابي)، وتم تحديد هذه النسبة بنـاءً علي رأي احد الخبراء في مجـال الإحصـــاء[21] وموافقـــة المشرف علـي الدراســـة، وبالتالي يمكـن الحكم علـى آليات الرقابة ليست فعالة عندما يكون مجموع الملاحظات للإجراءات الرقابية الغير فعالة في المصارف عينة الدراسة أصغر من أو تساوي (70%) من أجمالي الملاحظات، وفي المقابل سيتم اعتبـــار آليات

[21]- الدكتور: أحمد مامي، عضو هيئة التدريس بقسم الإحصاء، كلية العلوم: جامعة بنغازي.

الرقابة فعالة عندما تكــون مجمــوع الملاحظات للإجراءات الرقابية الفعالة أكبر من (70%) من أجمالي الملاحظات.

3- يتم الحكم علي آليات الرقابة بناءً علي نتائج الملاحظة التي أجريت علي الإجراءات الرقابية المتعلقة بكل آلية من آليات الرقابة، وذلك وفقاً للحالات التالية:

أ- إذا كان عدد الإجراءات الرقابية الفعالة أكثر من عدد الإجراءات الرقابية الغير فعالة، وذلك بالنسبة لكل مجموعة من آليات الرقابة التسعة محل الاختبار، فأنه في هذه الحالة يتم الحكم عليها بأنها فعالة في المصارف المشاركة في الدراسة.

ب- إذا كان عدد الإجراءات الرقابية الغير فعالة أكثر من عدد الإجراءات الرقابية الفعالة، وذلك بالنسبة لكل مجموعة من آليات الرقابة التسعة محل الاختبار، فأنه في هذه الحالة يتم الحكم عليها بأنها ليست فعالة في المصارف المشاركة في الدراسة.

4- يتم الحكم علي فعالية الرقابة في المنظومة المصرفية الموحدة في المصارف المشاركة بالدراسة بناءً علي نتائج الملاحظة التي أجريت علي آليات الرقابة التسعة، من خلال المقارنة بين عدد آليات الرقابة الفعالة وعدد آليات الرقابة الغير فعالة وفقاً للحالات التالية:

أ- إذا كان عدد آليات الرقابة الفعالة أكثر من عدد آليات الرقابة الغير فعالة، فأنه في هذه الحالة يتم الحكم عليها بأنها فعالة في المصارف المشاركة بالدراسة.

ب- إذا كان عدد آليات الرقابة الغير فعالة أكثر من عدد آليات الرقابة الفعالة، فأنه في هذه الحالة يتم الحكم عليها بأنها ليست فعالة في المصارف المشاركة بالدراسة.

5- عند الانتهاء من الخطوات الأساسية التي تم إتباعها لتحليل بيانات الدراسة المجمعة بالملاحظة، سيتم استخلاص نتائج الدراسة حول فعالية الرقابة للمنظومة المصرفية الموحدة في المصارف الليبية المشاركة بالدراسة.

وللإجابة علي سؤال الدراسة من البيانات المجمعة بالملاحظة تم تقسيم هذا الجزء إلي قسمين، يختص القسم الأول بتحليل بيانات الملاحظة حول كل آلية من آليات الرقابة التسعة علي حدا، أما القسم الثاني فقد خصص لتحليل بيانات الملاحظة حول فعالية الرقابة في المنظومة المصرفية الموحدة في المصارف المشاركة بالدراسة كما يلي:

4.8.2.1 الملاحظات حول آليات الرقابة في المنظومة المصرفية الموحدة:

لكي يمكن الحكم علي فعالية كل إلية من آليات الرقابة تم تجميع الملاحظة وفقاً للمجموعات التسعة لآليات الرقابة، وفيما يلي توضيح لهذه الآليات والقرار المتخذ حيال كل مجموعة من آليات الرقابة للمنظومة المصرفية الموحدة في المصارف المشاركة بالدراسة.

4.8.2.1.1 الملاحظة حول آليات خفض الخطأ والغش:

تهدف هذه الآليات إلي تخفيض فرص ارتكاب الخطأ والغش وزيادة فرص اكتشافها، وهي تحتوى علي عدد (5) أسئلة (إجراءات رقابية)، حيث أظهرت نتائج الملاحظة وجود بعض الاختلاف مع نتائج المراجعين الداخليين ونتائج مشرفي المنظومة أيضاً، وذلك بالنسبة للسؤالين أرقام (3)،(5)، حول وجود إشراف علي الوظائف الرقابية، وإعطاء إجازات إجبارية للعاملين لتخفيض احتمال الغش، تبين من الملاحظة إهمال معظم المصارف المشاركة في الدراسة لهذه الإجراءات الرقابية، وهذا خلاف ما توصلت إلية نتائج المراجعين الداخليين ونتائج مشرفي المنظومة أيضاً.

أما بالنسبة للسؤال رقم (4) حول تناوب الواجبات لتقليل فرص حدوث الغش وزيادة فرص اكتشاف الخطأ، تبين من الملاحظة أن هذا الإجراء الرقابي لا يتم التركيز عليه بشكل كبير في معظم المصارف المشاركة في الدراسة، وهذا ما أكدته نتائج المراجعين الداخليين، وعكس ما توصلت إليه نتائج مشرفي المنظومة.

بناءً علي نتائج الملاحظة يمكن القول أن المصارف المشاركة في الدراسة بها نظام رقابة لا يمكن من خلاله تخفيض الخطأ والغش وزيادة فرص اكتشافها مما يدل علي عدم فعالية آليات رقابة خفض الخطأ والغش، وهذا خلاف ما توصلت إلية نتائج المراجعين الداخليين ونتائج مشرفي المنظومة أيضاً وذلك فيما يتعلق بالأسئلة أرقام (3)،(4)،(5)، كما سبق ذكره.

4.8.2.1.2 الملاحظة حول آليات رقابة الوصول المادي:

تهدف هذه الآليات إلي حماية حجرات وأجهزة وتجهيزات الحاسب الآلي من الوصول غير المصرح وهي تحتوى علي عدد (5) أسئلة (إجراءات رقابية)، حيث أظهرت نتائج الملاحظة أن هناك اختلاف كبير مع نتائج المراجعين الداخليين ونتائج مشرفي المنظومة، وذلك بالنسبة الأسئلة أرقام (2)،(4)،(5)، حول تركيب أجهزة إنذار علي معدات الحاسب الآلي، ووجود سجلات للزائرين يحتوي علي البيانات الكافية وأسباب الزيارة، وكذلك وجود تأمين ضد السرقة والمخاطر الأخرى تغطي أجهزة الحاسب الآلي، تبين من الملاحظة أن هذه الإجراءات الرقابية لا يتم التركيز

عليها وأنها ليست ذات فعالية في معظم المصارف المشاركة في الدراسة، وهذا خلاف ما توصلت إليه نتائج المراجعين الداخليين ونتائج مشرفي المنظومة أيضاً.

وأما السؤال رقم (3)، حول وضع سجلات دخول وخروج حجرات الحاسب الآلي والمتابعة من الموظف المختص، تبين من الملاحظة عدم أدراك موظفي المصارف لأهمية هذه السجلات وقلت استخدامها في معظم المصارف المشاركة في الدراسة، وهذا بعكس ما توصلت إلية نتائج المراجعين الداخليين، وما أكدته نتائج مشرفي المنظومة.

بناءً علي نتائج الملاحظة يمكن القول أن المصارف المشاركة في الدراسة يوجد بها نظام رقابة لا يمكن من خلاله تخفيض الوصول المادي ومنع الوصول غير المصرح به لحجرات ومعدات المنظومة الموحدة مما يدل علي عدم فعالية آليات الرقابة في تخفيض الوصول المادي، في حين أظهرت نتائج المراجعين الداخليين ونتائج مشرفي المنظومة خلاف ذلك فيما يتعلق بالأسئلة الأربعة سابقة الذكر.

4.8.2.1.3 الملاحظة حول آليات رقابة الوصول المنطقي:

تهدف هذه الآليات إلي حماية أجهزة الحاسب الآلي من الاستخدام غير المصرح به وهي تحتوى علي عدد (17) سؤال (أجراء رقابي)، حيث أظهرت نتائج الملاحظة بأن هناك اختلاف بسيط نسبياً مع نتائج المراجعين الداخليين ونتائج مشرفي المنظومة وهذا الاختلاف لا يؤثر علي القرار المتخذ للحكم علي فعالية آليات رقابة الوصول المنطقي، وذلك بالنسبة للسؤالين أرقام (10)،(17)، حول توعية العاملين بضرورة عدم كتابة كلمة المرور أو إظهارها علي الشاشة أو تداولها فيما بينهم، واستخدام أنظمة تعقب المتطفلين لاكتشاف المبكر للاختراقات الرقابية المحتملة، تبين من الملاحظة أن هذه الآليات ليست ذات فعالية في معظم المصارف المشاركة في الدراسة، وهذا خلاف ما توصلت إليه نتائج المراجعين الداخليين ونتائج مشرفي المنظومة أيضاً،

أما السؤال رقم (15) حول إجراء فحوصات رقابية للمخاطر المحتملة بصورة دورية والتقرير عن نتائج الفحص للإدارة العليا، تبين من الملاحظة إهمال معظم المصارف المشاركة في الدراسة إجراء مثل هذه الفحوصات الرقابية سواءً بصورة دورية أو عشوائية، وهذا ما أكدته نتائج المراجعين الداخليين، وخلاف ما توصلت إلية نتائج مشرفي المنظومة.

بناءً علي نتائج الملاحظة يمكن القول أن المصارف المشاركة في الدراسة يوجد بها نظام رقابة يمكن من خلاله تخفيض الوصول المنطقي وحماية أجهزة الحاسب من الاستخدام غير المصرح به، وهذا يدل علي فعالية آليات الرقابة في تخفيض الوصول المنطقي في المصارف المشاركة في الدراسة، وهذا ما أكدته نتائج المراجعين الداخليين ونتائج مشرفي المنظومة أيضاً.

4.8.2.1.4 الملاحظة حول آليات رقابة أمن البيانات:

تهدف هذه الآليات إلي حماية البيانات والمعلومات سواء كانت هذه البيانات موجودة علي أجهزة الحاسب الآلي أو محفوظة في صورة رقمية أو صورة ورقية وهي تحتوي علي عدد (11) سؤال (أجراء رقابي)، حيث أظهرت نتائج الملاحظة إن آليات رقابة أمن البيانات في المصارف المشاركة في الدراسة ذات فعالية وهذا ما توصلت إلية نتائج المراجعين الداخليين ومشرفي المنظومة مع وجود اختلاف بسيط نسبياً لا يؤثر في الحكم حول فعالية آليات رقابة أمن البيانات وهما السؤالين أرقام (7)،(8)، حول تحديد المستخدم المصرح به الحصول علي كل نوع من المعلومات وتحديد التوقيت الملائم ومكان تواجدها، وتطبيق الإجراءات الرقابية الملائمة عند المناولة اليدوية للبيانات بين الأقسام المختلفة والمركز الرئيسي والفروع، تبين من الملاحظة إهمال معظم المصارف المشاركة في الدراسة هذه الآليات وأنها ليست ذات فعالية، وهذا خلاف ما توصلت إليه نتائج المراجعين الداخليين، وما أكدته نتائج مشرفي المنظومة.

بناءً نتائج الملاحظة يمكن القول أن المصارف المشاركة في الدراسة بها نظام رقابة يمكن من خلاله تحسين أمن البيانات وحمايتها سواء كانت هذه البيانات موجودة علي أجهزة الحاسب الآلي أو محفوظة في صورة رقمية أو ورقية، مما يدل علي فعالية آليات الرقابة في تحسين أمن البيانات وهذا ما أكدته نتائج المراجعين الداخليين ومشرفي المنظومة أيضاً.

4.8.2.1.5 الملاحظة حول آليات رقابة تطبيق معايير التوثيق:

تهتم هذه الآليات بتحسين معايير التوثيق في المصارف الليبية التي تعمل وفقاً للمنظومة المصرفية الموحدة وهي تحتوى علي (3) أسئلة (إجراءات رقابية)، حيث أظهرت نتائج الملاحظة إهمال معظم المصارف المشاركة في الدراسة تطبيق آليات رقابة معايير التوثيق، المتمثلة في الأسئلة أرقام (1)،(2)،(3)، حول التحديد الجيد للمعايير والإجراءات الخاصة بعمليات التخزين والمناولة للبيانات، وتزويد المستخدم بالتوجيهات اللازمة للتبليغ عن أي اختراقات أمنية للنظام، والتحديد الجيد للإجراءات المتبعة في حالة عدم الالتزام بالسياسات الرقابية، مما يدل علي عدم فعاليتها وهذا ما أكدته نتائج المراجعين الداخليين ونتائج مشرفي المنظومة أيضاً.

بناءً علي نتائج الملاحظة يمكن القول أن المصارف المشاركة في الدراسة بها نظام رقابة لا يمكن من خلاله تحقيق نظام رقابي فعال يتضمن الإجراءات الرقابية الملائمة لبيئة النظام وتطبيقاته، ولا يعمل وفقاً لمواصفات التشغيل المعيارية، مما يدل علي عدم فعالية آليات الرقابة في تحسين تطبيق معايير التوثيق، وهذا ما أكدته نتائج المراجعين الداخليين ونتائج مشرفي المنظومة أيضاً.

4.8.2.1.6 الملاحظة حول آليات خطة التغلب علي آثار الكارثة:

تهدف هذه الآليات إلي التحقق من مدى وجود خطة شاملة للتغلب علي آثار أي الكارثة محتملة الحدوث وتتضمن تلك الخطة كل التطبيقات والبرامج والأجهزة الضرورية للحفاظ علي تشغيل المصرف في الحالات الطارئة، وهي تحتوي علي عدد (9) أسئلة (إجراءات رقابية)، حيث أظهرت نتائج الملاحظة بأن هناك اختلاف مع نتائج المراجعين الداخليين ونتائج مشرفي المنظومة، بالنسبة للسؤال رقم (1) تبين من الملاحظة أن معظم المصارف المشاركة في الدراسة تحرص علي توفير نسخ احتياطية من كل الملفات والبرامج مخزنة خارج المصرف لتمكين المصرف من استعادة الملفات والبرامج المدمرة أو التي تم فقدها عند حدوث الكارثة، وهذا خلاف ما توصلت إلية نتائج المراجعين الداخليين وما توصلت إليه نتائج مشرفي المنظومة أيضاً، أما السؤال رقم (2) حول الاحتفاظ بالبرامج الأصلية في أماكن آمنة خارج المصرف حتى يمكن الاستفادة من تلك البرامج عند حدوث الكارثة، تبين من الملاحظة أن معظم المصارف المشاركة في الدراسة التي تعمل وفقاً للمنظومة الموحدة تحتفظ بالبرامج الأصلية في أماكن آمنة خارج المصرف وهذا ما أكدته نتائج مشرفي المنظومة وعكس ما توصلت إليه نتائج المراجعين الداخليين المشاركين في الدراسة.

وكانت الأسئلة أرقام (4)،(5)،(6)،(7)،(8)،(9)، حول الاحتفاظ بالتطبيقات والأجهزة والبرامج الضرورية للحفاظ علي استمرار المصرف في حالة حدوث أي حالات طارئة، إجراء فحص واختبار دوري لخطة التغلب علي آثار الكارثة للتأكد من إمكانية تنفيذها في الواقع العملي، وتوافر بوليصة تأمين شاملة تغطي تكاليف أجهزة ومعدات الحاسب الآلي بالإضافة إلي تكاليف انقطاع الإعمال الذي ينتج من حدوث كوارث بالحاسب الآلي، والتحديد الواضح للأشخاص المسئولين عند تنفيذ خطة التغلب علي آثار الكارثة مع تحديد مسؤولية كل فرد من هؤلاء الأشخاص، بالإضافة إلي التحديد الجيد لكل الأنشطة اللازمة لاستعادة الإعمال وتتابع تنفيذ تلك الأنشطة والوقت اللازم لتنفيذ كل نشاط، والأماكن التي يمكن من خلالها متابعة مزاولة نشاط المصرف في حالة ما إذا كان الضرر يلحق بمباني المصرف، تبين من الملاحظة أن معظم المصارف المشاركة في الدراسة لا تهتم بتطبيق هذه الآليات وأنها ليست ذات فعالية، وهذا خلاف ما توصلت إليه نتائج المراجعين الداخليين ونتائج مشرفي المنظومة أيضاً.

بناءً علي نتائج الملاحظة يمكن القول أن المصارف المشاركة في الدراسة بها نظام رقابة لا يمكن من خلاله التغلب علي آثار الكارثة لتحقيق نظام فعال وضمان توافر التطبيقات والبرامج والأجهزة الضرورية للحفاظ علي تشغيل المصرف في الحالات الطارئة وتحديد

مسؤولية كل فرد بالإضافة إلي تحديد الوقت اللازم لاستعادة الإعمال عند المستوى الطبيعي لها مما يدل علي عدم فعالية آليات الرقابة في التغلب علي آثار الكارثة، وهذا بعكس ما توصلت إلية نتائج المراجعين الداخليين ونتائج مشرفي المنظومة كما سبق ذكره في الفقرة السابقة.

4.8.2.1.7 الملاحظة حول آليات الرقابة الخاصة بالانترنت والاتصالات والمصارف الالكترونية:

تهدف هذه الآليات في الحد من الاختراقات الأمنية في عمليات الاتصالات والإنترنت في المصارف الليبية التي تعمل وفقاً للمنظومة المصرفية الموحدة وهي تحتوى علي عدد (9) أسئلة (إجراءات رقابية)،حيث أظهرت نتائج الملاحظة بأن هناك خلاف مع نتائج المراجعين الداخليين ونتائج مشرفي المنظومة بالنسبة للسؤالين أرقام (5)،(6)، حيث تبين من نتائج الملاحظة إهمال معظم المصارف المشاركة في الدراسة في توفير بطاقتي هوية (ID) لكل مستخدم لعمليات المصرف الأولي تستخدم في الاستعلامات العامة والثانية تستخدم في التحويلات النقدية والعمليات المصرفية الأخرى، كما لا تهتم بتشفير المعلومات السرية والخاصة وهويات المستخدمين وكلمات المرور، وهذا خلاف ما توصلت إليه نتائج المراجعين الداخليين ونتائج مشرفي المنظومة أيضاً.

أما السؤال رقم (7) تبين من الملاحظة أن معظم المصارف المشاركة في الدراسة لا تركز علي حصر التحويلات النقدية علي الحسابات في نفس المصرف (المراسل والمرسل إليه في نفس المصرف)، وهذا ما أكدته نتائج المراجعين الداخليين وخلاف ما توصلت إلية نتائج مشرفي المنظومة.

بناءً علي نتائج الملاحظة يمكن القول أن المصارف المشاركة في الدراسة بها نظام رقابة لا يمكن من خلاله تقليل الاختراقات الأمنية في عمليات الاتصالات والانترنت والمصارف الالكترونية مما يدل علي عدم فعاليتها، وهذا خلاف ما توصلت إليه نتائج المراجعين الداخليين ونتائج مشرفي المنظومة كما سبق ذكره في الفقرة أعلاه.

4.8.2.1.8 الملاحظة حول آليات رقابة أمن النتائج:

تهدف هذه الآليات إلي حماية مخرجات الحاسب الآلي من الوصول غير المصرح به وهي تحتوى علي عدد (5) أسئلة (إجراءات رقابية)، حيث أظهرت نتائج الملاحظة أن هناك اختلاف كبير مع نتائج المراجعين الداخليين ونتائج مشرفي المنظومة بالنسبة للأسئلة أرقام (2)،(3)،(4)، حيث تبين من الملاحظة أن معظم المصارف المشاركة في الدراسة لا تهتم بمراقبة وتحديد المستخدمين المصرح لهم الدخول للمعلومات الهامة خلال فترة التصريح، كما لا يتم استخدام ألآلات المخصصة للتخلص من الأوراق التي تم الانتهاء منها رغم تواجدها، ولا يتم ختم النسخ

الورقية لمخرجات المنظومة بالوقت والتاريخ، وكذلك قصور في طباعة وتوزيع البيانات في ظل إشراف ملائم من الأشخاص المصرح لهم في المصرف، ، وهذا بعكس ما توصلت إلية نتائج المراجعين الداخليين ونتائج مشرفي المنظومة أيضاً.

إما السؤال رقم (5) تبين من الملاحظة أن معظم المصارف المشاركة في الدراسة لا تستخدم إجراء المراجعة العشوائية للمدخلات والمخرجات للتحقق من التشغيل الصحيح، وهذا ما أكدته نتائج المراجعين الداخليين وخلاف ما توصلت إليه نتائج مشرفي المنظومة.

بناءً علي نتائج الملاحظة يمكن القول أن المصارف المشاركة في الدراسة بها نظام رقابة لا يمكن من خلاله تحسين أمن النتائج لحماية كافة مخرجات المنظومة الموحدة من الوصول غير المصرح به وهذا يدل علي عدم فعالية آليات الرقابة في تحسين أمن النتائج، وهذا بعكس ما توصلت إليه نتائج المراجعين الداخليين ونتائج مشرفي المنظومة كما سبق ذكره.

4.8.2.1.9 الملاحظة حول آليات رقابة أمن خدمات التعهيد:

تهدف هذه الآليات إلي رقابة الخدمات التي يتم تعهيدها ورقابة أنشطة موفر خدمات التعهيد لضمان سرية وسلامة نظم المعلومات وهي تحتوى علي عدد (5) أسئلة (إجراءات رقابية)، حيث أظهرت نتائج الملاحظة بأن هناك خلاف بسيط نسبياً مع ما توصلت إليه نتائج المراجعين الداخليين ونتائج مشرفي المنظومة وهو لا يؤثر في الحكم علي فعالية آليات رقابة خدمات التعهيد، في السؤال رقم (4)، حيث تبين من الملاحظة أن معظم المصارف المشاركة في الدراسة لا يوفر لها مقدم خدمات التعهيد التعرف علي مستوى الأداء الرقابي وتقييم ذلك المستوى من قبل المصرف، وهذا بعكس ما توصلت إلية نتائج المراجعين الداخليين ونتائج مشرفي المنظومة أيضاً.

بناءً علي نتائج الملاحظة يمكن القول أن نتائج الملاحظة قدمت دليل علمي علي أن المصارف المشاركة في الدراسة بها نظام رقابة لا يمكن من خلاله تحسين أمن خدمات التعهيد ورقابة أنشطتها لضمان سرية وسلامة المنظومة الموحدة، وهذا يدل علي عدم فعالية آليات الرقابة في تحسين أمن خدمات التعهيد في المصارف المشاركة في الدراسة وهذا ما أكدته نتائج المراجعين الداخليين ومشرفي المنظومة أيضاً.

4.8.2.2 الملاحظة حول فعالية الرقابة للمنظومة المصرفية الموحدة في ليبيا:

للحكم علي فعالية الرقابة في المنظومة المصرفية الموحدة من خلال نتائج الملاحظة لآليات الرقابة التسعة السابقة الذكر، حيث تبين من نتائج الملاحظة أن هناك خلاف كبير مع ما توصلت إلية نتائج المراجعين الداخليين ونتائج مشرفي المنظومة وذلك بالنسبة للمجموعة الأولي

والثانية والسادسة والسابعة والثامنة حول آليات رقابة خفض الخطأ والغش، وآليات رقابة الوصول المادي، وآليات خطة التغلب علي آثار الكارثة، وآليات رقابة الاختراقات الأمنية في عمليات التجارة الالكترونية والاتصالات والانترنت، وآليات رقابة أمن النتائج، أن هذه الآليات ليست ذات فعالية في معظم المصارف الليبية المشاركة في الدراسة وهذا بعكس ما توصل إلية نتائج المراجعين الداخليين ونتائج مشرفي المنظومة أيضاً، أما المجموعة الخامسة والتاسعة حول آليات رقابة تطبيق معايير التوثيق، وآليات رقابة أمن خدمات التعهيد، تبين من الملاحظة أن هذه الآليات ليست ذات فعالية في المصارف الليبية المشاركة في الدراسة وهذا ما أكدته نتائج المراجعين الداخليين ونتائج مشرفي المنظومة أيضاً، وكانت المجموعة الثالثة والرابعة حول آليات رقابة الوصول المنطقي، وآليات رقابة أمن البيانات، تبين من الملاحظة أن هذه الآليات ذات فعالية في المصارف الليبية المشاركة في الدراسة وهذا ما أكدته أيضاً نتائج المراجعين الداخليين ونتائج مشرفي المنظومة أيضاً، والجدول رقم (23-4) يوضح ملخص نتائج الملاحظة حول آليات الرقابة للمنظومة المصرفية الموحدة المطبقة في المصارف الليبية.

جدول رقـم (23-4)
ملخص نتائج الملاحظة

م	آليات الرقابة للمنظومة المصرفية الموحدة	التعليق
1	آليات رقابة خفض الخطأ والغش.	ليست فعالة
2	آليات رقابة خفض الوصول المادي.	ليست فعالة
3	آليات رقابة خفض الوصول المنطقي.	فعالة
4	آليات الرقابة أمن البيانات.	فعالة
5	آليات رقابة معايير التوثيق.	ليست فعالة
6	آليات خطة التغلب علي آثار الكارثة	ليست فعالة
7	آليات رقابة الاختراقات الأمنية في عمليات التجارة الالكترونية والاتصالات والانترنت.	ليست فعالة
8	آليات رقابة أمن النتائج.	ليست فعالة
9	آليات رقابة أمن خدمات التعهيد.	ليست فعالة

يوضح هذا الجدول ملخص نتائج الملاحظة عند مستوى (0.7)

بناءً علي نتائج الملاحظة يمكن القول أن الرقابة في المنظومة المصرفية الموحدة ليست فعالة في المصارف المشاركة في الدراسة، وهذا خلاف ما توصلت إليه نتائج المراجعين الداخليين ونتائج مشرفي المنظومة أيضاً وذلك بالنسبة للمجموعة الأولي والثانية والسادسة والسابعة والثامنة سابقة الذكر.

4.8.3 مقارنة نتائج الدراسة التي تم التوصل إليها من استمارة الاستبيان مع نتائج الملاحظة:

يمكن مقارنة نتائج الدراسة التي تم التوصل إليها من استمارة الاستبيان مع نتائج الدراسة التي تم التوصل إليها من الأداة الأساسية الثانية في الدراسة وهي الملاحظة وذلك كما يتضح من الجدول رقم (24- 4):

جدول رقـم (24-4)
ملخص نتائج الدراسة

م	آليات الرقابة للمنظومة المصرفية الموحدة	استمارة الاستبيان		الملاحظة
		المراجعين الداخليين	مشرفي المنظومة	
1	آليات رقابة خفض الخطأ والغش.	فعالة	فعالة	ليست فعالة
2	آليات رقابة خفض الوصول المادي.	فعالة	فعالة	ليست فعالة
3	آليات رقابة خفض الوصول المنطقي.	فعالة	فعالة	فعالة
4	آليات الرقابة أمن البيانات.	فعالة	فعالة	فعالة
5	آليات رقابة معايير التوثيق.	ليست فعالة	ليست فعالة	ليست فعالة
6	آليات خطة التغلب علي آثار الكارثة	فعالة	فعالة	ليست فعالة
7	آليات رقابة الاختراقات الأمنية في عمليات التجارة الالكترونية والاتصالات والانترنت.	فعالة	فعالة	ليست فعالة
8	آليات رقابة أمن النتائج.	فعالة	فعالة	ليست فعالة
9	آليات رقابة أمن خدمات التعهيد.	ليست فعالة	ليست فعالة	ليست فعالة

يوضح هذا الجدول ملخص نتائج استمارة الاستبيان عند مستوى معنوية (0.05)
مقارنة مع نتائج الملاحظة عند مستوى (0.7).

أظهرت نتائج الدراسة الجدول رقم (24- 4) أنه يوجد اختلاف بين نتائج الدراسة التي تم التوصل إليها من استمارة الاستبيان ونتائج الملاحظة حيث تبين من نتائج المراجعين الداخليين ومشرفي المنظومة فعالية آليات رقابة خفض الخطأ والغش، وآليات رقابة الوصول المادي، وآليات خطة التغلب علي آثار الكارثة، وآليات رقابة الاختراقات الأمنية والاتصالات والانترنت، وآليات رقابة أمن النتائج، في حين أظهرت نتائج الملاحظة خلاف ذلك.

واتفقت نتائج المراجعين الداخليين ومشرفي المنظومة مع نتائج الملاحظة علي فعالية آليات رقابة الوصول المنطقي، واليات رقابة أمن البيانات، كما اتفقت نتائج المراجعين الداخليين ومشرفي المنظومة مع نتائج الملاحظة علي أن آليات رقابة تطبيق معايير التوثيق، واليات رقابة أمن خدمات التعهيد أنها ليست فعالة في المصارف المشاركة بالدراسة.

يمكن تفسير ما توصلت إلية نتائج المراجعين الداخليين ومشرفي المنظومة إلي اعتقادهم بأن موضوع ومشكلة الدراسة يعتبر من الموضوعات التي تتصف بالحساسية والسرية، وبالتالي يمكن استنتاج أن إجابات أفراد العينة جاءت مضللة في سبيل عدم تقديم معلومات حقيقية للدراسة.

كما يمكن تفسير ما توصلت إلية نتائج الملاحظة بعدم فعالية آليات الرقابة في المنظومة المصرفية الموحدة إلي انعدام المعرفة بكيفية استخدام الإجراءات الرقابية، وأهميتها، وفائدتها في تحقيق نظام رقابة فعال، وعدم متابعة إدارة المراجعة الداخلية لأنظمة الرقابة الالكترونية والعمل علي تطويرها، وعدم اهتمام إدارات المصارف بتطبيق الإجراءات الرقابية المتعلقة بالأنظمة الالكترونية في المصارف الليبية، وهذا يتفق مع ما توصلت إليه نتائج دراسة (الفرطاس، 2006)[21].

[21]_ دراسة (الفرطاس، 2006): هدفت الدراسة الي التعرف علي مدى توافر إجراءات الرقابة الداخلية في الأنظمة الإلية المستخدمة في فروع المصارف التجارية الليبية، أنظر ملخص الدراسة ص (55).

4.9 الخلاصــة:

احتوى هذا الفصل علي تحليل بيانات الدراسة بشقيها الوصفي والاستدلالي، حيث تم استخدام الإحصاء الوصفي لتحليل البيانات التي تم تجميعها عن طريق الجزء الأول من استمارة الاستبيان وذلك بالنسبة للمراجعين الداخليين ومشرفي المنظومة، وذلك بهدف وصف بعض خصائص ومعالم عينة الدراسة، في حين تم استخدام الإحصاء الاستدلالي لتحليل البيانات الدراسة المجمعة من استمارة الاستبيان المتعلقة باختبار فرضيات الدراسة، وهي البيانات التي تم تجميعها عن طريق الجزء الثاني من استمارة الاستبيان فقط، من خلال استخدام اختبار (T)، لقبول أو رفض الفرضيات الفرعية للدراسة عند مستوى معنوية (0.05).

كما أن استخدام وسيلة الملاحظة في تجميع البيانات أظهرت خلافات مع ما تم الحصول عليه من نتائج الاستبيان، وبذلك تم التوصل إلي حقائق أكثر واقعية حيث أظهرت نقاط ضعف وقصور كبير في آليات الرقابة بالمنظومة المصرفية الموحدة المستخدمة في المصارف المشاركة وتم التوصل إلي نتيجة رئيسية تتمثل في أن الرقابة في المنظومة المصرفية الموحدة في المصارف الليبية فعالة وهذا بالنسبة للمراجعين الداخليين ومشرفي المنظومة، وهذا خلاف ما توصلت إلية نتائج الملاحظة فأن الرقابة في المنظومة المصرفية الموحدة ليست فعالة في المصارف الليبية المشاركة في الدراسة.

وبذلك وفرت نتائج هذه الدراسة دليل علمي علي أن الاعتماد علي بيانات وسيلة الاستبيان في بيئة المصارف الليبية لا توفر بيانات حقيقية وموضوعية تعكس الواقع الفعلي، وتبين ذلك جلياً من خلال التوصل إلي نتائج من خلال الملاحظة عكس ما تم التوصل إليه من خلال الاستبيان ويشير ذلك إلي أن المشاركين في الإجابة علي الاستبيان لم يقوموا بتقديم الإجابات الموضوعية والحقيقية التي تعكس الواقع الفعلي كما تم التوصل إليها من خلال الملاحظة والمشاهدة في الواقع العملي وبمقارنة الوسيلتين تعتبر الملاحظة والمشاهدة أكثر واقعية وموضوعية وحيادية من الاستبيان ويمكن الاعتماد عليها وعلي مصادقتيها أكثر من نتائج الاستبيان.

الفصـــل الخامس:

النتائــج والتوصيـــات

5.1 مقدمــة:

استعرض الفصل الرابع منهجية الدراسة، وأسلوب الدراسة والإجراءات التي تم تتبعها، وأدوات تجميع البيانات ومراحل إعدادها، والهدف الرئيسي لهذا البحث هو التعرف علي واقع الرقابة في المنظومة المصرفية الموحدة في القطاع المصرفي الليبي، من خلال التعرف علي أراء أطراف العينة المشاركة في الدراسة وهم المراجعين الداخليين ومشرفي المنظومة، بالإضافة إلي الملاحظة من واقع العمل المصرفي ويرجع ذلك للعلاقة المباشرة للأطراف المشاركة في الدراسة بموضوع الدراسة وإلمامهم بظروف القطاع المصرفي والتهديدات الرقابية التي يتعرض لها هذا القطاع.

وقد احتوت الدراسة علي خمس فصول، اهتم الفصل الأول بإعطاء صورة شاملة عن خطة البحث، من خلال توضيح مشكلة وسؤال وهدف البحث، وفرضياته الرئيسية والفرعية، والتي تم صياغتها علي النحو التالي:

الفرضية الرئيسية: عدم فعالية الرقابة للمنظومة المصرفية الموحدة في ليبيا.

الفرضية الفرعية الأولي: لا تخفض آليات الرقابة من الخطأ والغش.

الفرضية الفرعية الثانية: لا تخفض آليات الرقابة من الوصول المادي.

الفرضية الفرعية الثالثة: لا تخفض آليات الرقابة من الوصول المنطقي.

الفرضية الفرعية الرابعة: لا تحسن آليات الرقابة من أمن البيانات.

الفرضية الفرعية الخامسة: لا تحسن آليات الرقابة من تطبق معايير التوثيق.

الفرضية الفرعية السادسة: لا تمكن آليات الرقابة من التغلب علي آثار الكارثة.

الفرضية الفرعية السابعة: لا تخفض آليات الرقابة من الاختراقات الأمنية في عمليات التجارة الالكترونية والاتصالات والانترنت.

الفرضية الفرعية الثامنة: لا تحسن آليات الرقابة من أمن النتائج.

الفرضية الفرعية التاسعة: لا تحسن آليات الرقابة من أمن خدمات التعهيد.

كما أوضح الفصل الأول أن البحث يستمد أهميته من أهمية دور الرقابة في النظم المصرفية الالكترونية، وكونها أول دراسة من نوعها فيتوقع أن يستفيد من نتائجها ذوي العلاقة من المهتمين سواء في القطاع المصرفي أو الأكاديمي، وتمثل مجتمع الدراسة في المصارف الليبية التي تطبق المنظومة المصرفية الموحدة، وتم اختيار عينة الدراسة من المراجعين الداخليين ومشرفي المنظومة بالإضافة إلي الملاحظة الشخصية حيث بلغ إجمالي مفردات العينة (45) مفردة، وتم تحليل البيانات باستخدام كل من الإحصاء الوصفي والاستدلالي.

أما الفصل الثاني فقدم نبذة حول الرقابة في نظم المعلومات الالكترونية، وذلك من خلال عرض مفهوم وأهداف الرقابة في النظم الالكترونية وأهميتها، والمبادئ الأساسية للرقابة، ومقومات النظام الجيد للرقابة وتصنيفها، والتعرف علي مقاييس الأمان بها ومراحل تطويرها، واستعراض المخاطر الرقابية والمخاطر القانونية المتعلقة بنظم المعلومات الالكترونية، بالإضافة إلي أساليب تقييمها والعوامل المؤثرة علي فعالية هذه النظم.

وفي الفصل الثالث تم مراجعة الدراسات السابقة المتعلقة بالرقابة في النظم المعلومات الالكترونية، وتم تقسيم هذا الفصل إلي مجموعتين الأولي تهتم بعرض الإصدارات المهنية المتعلقة بموضوع الدراسة، أما المجموعة الثانية فاهتمت بعرض الدراسات السابقة ذات الصلة بموضوع الدراسة، وذلك لإعطاء خلفية مناسبة حول هذا الموضوع.

وبناءً علي ذلك فقد شكلت الفصول الأول الثاني والثالث الإطار النظري للدراسة والذي ساهم في بناء قاعدة علمية واضحة لانجاز الجزء العملي لها، والذي خصص له الفصل الرابع والذي تضمن تحليل البيانات الدراسة باستخدام كل من الإحصاء الوصفي، والإحصاء الاستدلالي، وإظهار نتائج هذا التحليل.

وأخيراً يحتوي الفصل الحالي علي عرض خلاصة لأجمالي البحث، وتكوين صورة شاملة تحتوي علي كل خطوات وأجزاء البحث، وسيحتوي الجزء الباقي من هذا الفصل علي عرض نتائج الدراسة، ومحدداتها وتوصياتها.

5.2 نتائـــج الدراســـة:

تم تقسيم النتائج التي تم التوصل إليها في هذه الدراسة إلي قسمين كما يلي:

5.2.1 نتائـــج استمـــارة الاستبيان:

يمكن تلخيص النتائج التي توصلت إليها استمارة الاستبيان علي النحو التالي:

1- أتفق كل من المراجعين الداخليين ومشرفي المنظومة أن معظم المصارف الليبية التي تعمل وفقاً للمنظومة المصرفية الموحدة بها نظام رقابة يمكن من خلاله تخفيض فرص ارتكاب الخطأ الغش وزيادة فرص اكتشافها، وهذا مؤشر جيد وهام يدل علي فعالية آليات الرقابة في تخفيض الخطأ والغش.

2- أتفق كل من المراجعين الداخليين ومشرفي المنظومة أن معظم المصارف الليبية التي تعمل وفقاً للمنظومة المصرفية الموحدة بها نظام رقابة يمكن من خلاله تخفيض الوصول المادي وحماية حجرات وأجهزة وتجهيزات الحاسب الآلي من الوصول غير المصرح به، وهذا يدل علي فعالية آليات الرقابة في تخفيض الوصول المادي.

3- أتفق كل من المراجعين الداخليين ومشرفي المنظومة أن معظم المصارف الليبية التي تعمل وفقاً للمنظومة المصرفية الموحدة بها نظام رقابة يمكن من خلاله تخفيض الوصول المنطقي وحماية أجهزة الحاسب الآلي من الاستخدام غير المصرح به، وهذا يدل علي فعالية آليات الرقابة في تخفيض الوصول المنطقي.

4- أتفق كل من المراجعين الداخليين ومشرفي المنظومة أن معظم المصارف الليبية التي تعمل وفقاً للمنظومة المصرفية الموحدة بها نظام رقابة يمكن من خلاله تحسين أمن البيانات وحمايتها سواء كانت هذه البيانات موجودة علي أجهزة الحاسب الآلي أو محفوظة في صورة رقمية أو في صورة ورقية، وهذا يدل علي فعالية آليات الرقابة في تحسين أمن البيانات.

5- أتفق كل من المراجعين الداخليين ومشرفي المنظومة أن معظم المصارف الليبية التي تعمل وفقاً للمنظومة المصرفية الموحدة بها نظام رقابة لا يمكن من خلاله تطبيق معايير التوثيق في بناء نظام يتضمن الإجراءات الرقابية الملائمة لبيئة النظام وتطبيقاته، وهذا يدل علي عدم فعالية آليات الرقابة في تطبيق معايير التوثيق.

6- أتفق كل من المراجعين الداخليين ومشرفي المنظومة، أن معظم المصارف الليبية التي تعمل وفقاً للمنظومة المصرفية الموحدة بها نظام رقابة يمكن من خلاله التغلب علي آثار أي كارثة محتملة الحدوث وتتضمن تلك الخطة كل التطبيقات والبرامج والأجهزة الضرورية للحفاظ علي تشغيل المصرف في الحالات الطارئة ومسئولية كل، وهذا يدل علي فعالية آليات الرقابة في التغلب علي آثار الكارثة.

7- أتفق كل من المراجعين الداخليين ومشرفي المنظومة أن معظم المصارف الليبية التي تعمل وفقاً للمنظومة المصرفية الموحدة بها نظام رقابة يمكن من خلاله التقليل من الاختراقات الأمنية في عمليات التجارة الالكترونية والاتصالات والانترنت، مما يدعم فعالية آليات الرقابة للمنظومة المصرفية الموحدة.

8- أتفق كل من المراجعين الداخليين ومشرفي المنظومة أن معظم المصارف الليبية التي تعمل وفقاً للمنظومة المصرفية الموحدة بها نظام رقابة يمكن من خلاله تحسين أمن النتائج وحماية مخرجات الحاسب الآلي من الوصول غير المصرح به، وهذا مؤشر جيد وهام يدل علي فعالية آليات الرقابة في تحسين أمن النتائج.

9- أتفق كل من المراجعين الداخليين ومشرفي المنظومة أن معظم المصارف الليبية التي تعمل وفقاً للمنظومة المصرفية الموحدة بها نظام رقابة لا يمكن من خلاله تحسين أمن خدمات التعهيد ومعالجة المشاكل التقنية التي قد تطرأ عليه، ورقابة أنشطة موفر خدمات التعهيد لضمان سرية وسلامة النظام، وهذا مؤشر غير جيد يدل علي عدم فعالية آليات الرقابة في أمن خدمات التعهيد.

5.2.2 نتائـــج الملاحظـــة:

يمكن تلخيص النتائج التي توصلت إليها الملاحظة علي النحو التالي:

1- أظهرت نتائج الملاحظة أن معظم المصارف الليبية التي تعمل وفقاً للمنظومة المصرفية الموحدة بها نظام رقابة لا يمكن من خلاله تخفيض فرص ارتكاب الخطأ الغش وزيادة فرص اكتشافها، مما يدل علي عدم فعالية آليات الرقابة في تخفيض الخطأ والغش، وهذا بعكس ما توصلت إلية نتائج المراجعين الداخليين ونتائج مشرفي المنظومة أيضاً.

2- أظهرت نتائج الملاحظة أن معظم المصارف الليبية التي تعمل وفقاً للمنظومة المصرفية الموحدة بها نظام رقابة لا يمكن من خلاله تخفيض الوصول المادي وحماية حجرات وأجهزة وتجهيزات الحاسب الآلي من الوصول غير المصرح به، مما يدل علي عدم فعالية آليات الرقابة في تخفيض الوصول المادي، وهذا بعكس ما توصلت اليه نتائج المراجعين الداخليين ومشرفي المنظومة.

3- أظهرت نتائج الملاحظة أن معظم المصارف الليبية التي تعمل وفقاً للمنظومة المصرفية الموحدة بها نظام رقابة يمكن من خلاله تخفيض الوصول المنطقي وحماية أجهزة الحاسب

الآلي من الاستخدام غير المصرح به، مما يدل علي فعالية آليات الرقابة في تخفيض الوصول المنطقي، وهذا ما أكدته نتائج المراجعين الداخليين ومشرفي المنظومة أيضاً.

4- أظهرت نتائج الملاحظة أن معظم المصارف الليبية التي تعمل وفقاً للمنظومة المصرفية الموحدة بها نظام رقابة يمكن من خلاله تحسين أمن البيانات وحمايتها سواء كانت هذه البيانات موجودة علي أجهزة الحاسب الآلي أو محفوظة في صورة رقمية أو في صورة ورقية، مما يدل علي فعالية آليات الرقابة في تحسين أمن البيانات، وهذا ما أكدته نتائج المراجعين الداخليين ونتائج مشرفي المنظومة أيضاً.

5- أظهرت نتائج الملاحظة أن معظم المصارف الليبية التي تعمل وفقاً للمنظومة المصرفية الموحدة بها نظام رقابة لا يمكن من خلاله تطبيق معايير التوثيق في بناء نظام يتضمن الإجراءات الرقابية الملائمة لبيئة النظام وتطبيقاته، مما يدل علي عدم فعالية آليات الرقابة في تطبيق معايير التوثيق، وهذا ما أكدته نتائج المراجعين الداخليين ونتائج مشرفي المنظومة أيضاً.

6- أظهرت نتائج الملاحظة أن معظم المصارف الليبية التي تعمل وفقاً للمنظومة المصرفية الموحدة بها نظام رقابة لا يمكن من خلاله التغلب علي آثار أي كارثة محتملة الحدوث وتتضمن تلك الخطة كل التطبيقات والبرامج والأجهزة الضرورية للحفاظ علي تشغيل المصرف في الحالات الطارئة، مما يدل علي عدم فعالية آليات الرقابة في التغلب علي آثار الكارثة، وهذا بعكس ما توصلت إليه نتائج المراجعين الداخليين ونتائج مشرفي المنظومة أيضاً.

7- أظهرت نتائج الملاحظة أن معظم المصارف الليبية التي تعمل وفقاً للمنظومة المصرفية الموحدة بها نظام رقابة لا يمكن من خلاله التقليل من الاختراقات الأمنية في عمليات التجارة الالكترونية والاتصالات والانترنت، مما يدل علي عدم فعالية آليات الرقابة للمنظومة المصرفية الموحدة، وهذا خلاف ما توصلت إليه نتائج في المنظومة أيضاً.

8- أظهرت نتائج الملاحظة أن معظم المصارف الليبية التي تعمل وفقاً للمنظومة المصرفية الموحدة بها نظام رقابة لا يمكن من خلاله تحسين أمن النتائج وحماية مخرجات الحاسب الآلي من الوصول غير المصرح به، وهذا يدل علي عدم فعالية آليات الرقابة في تحسين أمن النتائج، وهذا خلاف ما توصلت إليه نتائج المراجعين الداخليين ونتائج مشرفي المنظومة أيضاً.

9- أظهرت نتائج الملاحظة أن معظم المصارف الليبية التي تعمل وفقاً للمنظومة المصرفية الموحدة بها نظام رقابة لا يمكن من خلاله تحسين أمن خدمات التعهيد ومعالجة المشاكل

التقنية التي قد تطرأ علي النظام، ورقابة أنشطة موفر خدمات التعهيد لضمان سرية وسلامة النظام، مما يدل علي عدم فعالية آليات الرقابة في أمن خدمات التعهيد، وهذا ما أكدته نتائج المراجعين الداخليين ونتائج مشرفي المنظومة أيضاً.

وبذلك إذا ما أخذت النتائج المتحصل عليها من الاستبيان فأنها تؤيد وجود فعالية في نظام الرقابة بالمنظومة المصرفية الموحدة المستخدمة في المصارف المشاركة بالدراسة، ولكن حقيقة الأمر وفقاً لما توصلت إلية الملاحظة وهي الأكثر موضوعية فأن آليات الرقابة بالمنظومة المصرفية الموحدة بها قصور وضعف كبيرين.

5.3 محـــددات الدراســة:

من أهم محددات الدراسة استخدامها الاستبيان كإحدى وسائل تجميع البيانات وبالتالي فأن النتائج التي تم التوصل إليها تؤخذ في ظل نقاط الضعف التي تخص الاستبيان، والتي حددها بوحوش (1995) في الآتي.

1- البطء، فهي تحتاج إلي وقت طويل ومجهود شاق للحصول علي البيانات.
2- تواجه صعوبات جمة نابعة من رغبة المشاركين في تضخيم الأحداث.
3- مكلفة مالياً لأنها تحتاج إلي التنقل لمقابلة المشاركين في الدراسة.
4- نجاحها يعتمد علي رغبة المشاركين وقدرتهم على التعبير بدقه عن ما يريد الإفصاح عنه.

فضلاً عن النتائج التي توصلت إليها هذه الدراسة من خلال الملاحظة أظهرت عدم واقعية ومصداقية وموضوعية البيانات التي تم تجميعها بوسيلة الاستبيان.

كما تتمثل محددات الدراسة في صعوبة الحصول علي بيانات الدراسة الأمر الذي ترتب عليه مشاركة فرع واحد من فروع المنطقة الغربية، مما ينتج عنه صعوبة تعميم النتائج علي كامل القطاع المصرفي الليبي.

كما اقتصرت الدراسة علي استكشاف واقع الرقابة في المنظومة المصرفية الموحدة المطبقة في المصارف الليبية، وبالتالي يخرج عن نطاق الدراسة تصميم نظام رقابة لهذا النظام.

5.4 توصيــات الدراســـة:

في ضوء أهداف الدراسة وطبيعة مشكلتها وبناءً علي النتائج التي تم التوصل إليها يوصى بالاتي:

1. أن تقوم المصارف بتخصيص اهتمام كبير بموضوع الرقابة علي المنظومة المصرفية الموحدة وتلافي نقاط الضعف فيها.

2. توعية المراجعين الداخليين ومشرفي المنظومة المصرفية الموحدة العاملين في المصارف الليبية بالدور المنتظر منهم في تقييم نظم الرقابة للمنظومة المصرفية الموحدة، وتحديد الإخطار التي تهددها، والمشاركة في اختيار الضوابط الرقابية الملائمة لمواجهة هذه الإخطار، والمشاركة في إعداد برامج لتوعية إدارات المصارف الليبية والعاملين بها بأهمية أمن المعلومات المحاسبية.

3. ضرورة اهتمام مصرف ليبيا المركزي والجامعات الليبية بصقل القدرات العلمية للمحاسبين والمراجعين وأخصائيين تقنية المعلومات في مجال الرقابة في نظم المعلومات المحاسبية الالكترونية.

4. توفير برامج تدريب مهني متخصص للمراجعين الداخليين وأخصائي تقنية المعلومات في مجال رقابة المعلومات المحاسبية الالكترونية، بهدف إعداد كوادر قادرين علي القيام بالأدوار المطلوبة منهم في مجال رقابة نظم المعلومات المحاسبية الالكترونية.

5. يجب توجيه مزيد من البحث الأكاديمي نحو البحوث التي تعالج الموضوعات الحديثة في مجال الرقابة في نظم المعلومات المحاسبية وأثرها علي الإحكام المهنية عند تقييم نظام الرقابة الداخلية.

6. تبني كليات الاقتصاد بمختلف الجامعات الليبية وخاصة أقسام المحاسبة بالتعاون مع مصرف ليبيا المركزي بإقامة الندوات والمؤتمرات العلمية التي تناقش التهديدات الرقابية لنظم المعلومات المحاسبية الإلكترونية، وسبل واستراتيجيات التعامل معها وإدارتها.

7. نظراً لما وضحته الدراسة من عدم موضوعية البيانات المجمعة اعتماداً علي الاستبيان يوصى باستخدام وسائل تجميع أكثر موضوعية في البيئة الليبية، حتى تتوصل البحوث إلي نتائج تعكس الواقع وتتيح معالجة المشاكل والصعوبات ووضع الحلول المناسبة لها مما يسمح بالتطوير.

قائمة المراجع

المراجع

أولاً: المراجع العربية:

- الجبالى، م: (2002) الاتجاهات الحديثة فئ ظل المتغيرات التكنولوجية في نظم المعلومات المحاسبية: مجلة العلمية للاقتصاد والتجارة العدد الأول كلية التجارة جامعة عين شمس.
- الحكيم، س: (2010) امكانية الرقابة علي نظم المعلومات المحاسبية ذات الطابع الاقتصادي: مجلة جامعة دمشق الاقتصادية، المجلد 26، العدد الاول.
- السقا، أ: (1997) المراجعة الداخلية – الجوانب المالية والتشغيلية: الجمعية السعودية للمحاسبين.
- الالوسي، ح: (1428) المعايير الدولية للمراجعة أهميتها..وكيفية التعامل معها عربياً: مجلة أكاديمية الدراسات العليا والبحوث الاقتصادية، العدد السابع، ص ص 244- 267.
- الدرسي، م: (2008) مدى إدراك إدارات المصارف التجارية الليبية لمخاطر التشغيل المصرفي: رسالة ماجستير غير منشورة أكاديمية الدراسات العليا بنغازي.
- الشريف، إ: (2006) متطلبات تطوير مهنة المحاسبة في ليبيا، المؤتمر الوطني الأول حول المحاسبة: غرفة التجارة والصناعة طرابلس، ص ص 6- 8.
- الشريف، إ: (2012) نظام هارفارد للمراجع، حلقة نقاش، أكاديمية الدراسات العليا بنغازي.
- الشريف، ح: (2006) مخاطر نظم المعلومات المحاسبية الالكترونية: رسالة ماجستير كلية التجارة الجامعة الإسلامية غزة.
- الفرطاس، أ: (2002) مدى توفير إجراءات الرقابة الداخلية الحاسبية في الأنظمة الإلية المستخدمة في فروع المصارف التجارية الليبية العامة بمدينة بنغازي: رسالة ماجستير غير منشورة أكاديمية الدراسات العليا بنغازي.
- الفيتوري، غ: (2007) مدى توافر مقومات تطبيق مدخل التكلفة علي أساس النشاط في المصارف التجارية الليبية: رسالة ماجستير غير منشورة كلية الاقتصاد جامعة قاريونس.
- بلقاسم، م: (2006) أثر تكنولوجيا المعلومات علي أداء المراجع: المؤتمر الوطني الأول حول المحاسبة- غرفة التجارة والصناعة طرابلس ليبيا.

- بوحوش، ع: (1995) مناهج البحث العلمي وطرق إعداد البحوث: ديوان المطبوعات الجامعية الجزائر.
- جل، أ: (2010) مدى فاعلية نظم المعلومات المحاسبية في المصارف التجارية العراقية الأهلية من وجهة نظر الإدارة: رسالة ماجستير كلية الإعمال جامعة الشرق الأوسط.
- حمادة، ر: (2010) أثر الضوابط الرقابية العامة لنظم المعلومات المحاسبية الالكترونية في زيادة موثوقية المعلومات المحاسبية: مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، المجلد 26، العدد الأول.
- حمني، ح: (2006) آليات رقابة البنك المركزي علي البنوك التجارية وفعاليتها: رسالة ماجستير كلية العلوم الاقتصادية قسنطينة.
- حسين، أ: (2005) نظم المعلومات المحاسبية الإطار الفكري والنظم التطبيقية: كلية التجارة جامعة الإسكندرية.
- رسلان، م . الشيشني، ح: (2005) مبادئ المراجعة مدخل معاصر: كلية التجارة جامعة طنطا.
- صندوق النقد الدولي :(1994) متطلبات الرقابة الداخلية في المصارف: الاجتماع الرابع، ص ص. 8-10، [علي الانترنت]، متوفر علي http://www.amf.org/at/acbspubs [2013/01/24].
- راضى، م . السقا، أ: (2005) الاتجاهات الحديثة في المراجعة المالية: كلية التجارة جامعة طنطا.
- طلبه، م: (2004) الحاسب ونظم المعلومات الإدارية: مجموعة كتب الدلتا.
- عبد المجيد، م: (1999) مسؤولية مراقب الحسابات عن اكتشاف الأخطاء والغش فى ظل النظم الالكترونية: بدون ناشر.
- قطناني، خ: (2007) البيئة المصرفية وأثرها علي كفاءة وفعالية نظم المعلومات المحاسبية دراسة تحليلية علي المصارف التجارية في الأردن: مجلة الأكاديمية العربية للعلوم المالية والمصرفية، المجلد العاشر، العدد الأول.
- لمين، ع: (2008) مساهمة المراجعة الداخلية في تقييم نظام المعلومات المحاسبي للمؤسسة الوطنية للتجهيزات الصناعية: رسالة ماجستير جامعة الجزائر، كلية العلوم الاقتصادية.

- مبارك، ب. وبوشوشة، هـ: (2009) دور جودة أمن المعلومات المحاسبية في إدارة الأزمة المالية العالمية: المؤتمر العلمي الدولي السابع، جامعة الزرقاء الأردن.
- محمود، أ: (2006) مراجعة الحسابات في ظل بيئة التجارة الالكترونية والتقرير المالي الالكتروني: مجلة الاقتصاد و العلوم السياسية العدد الخامس جامعة الفاتح.
- مؤمن، س: (2007) الإحصاء ألاستنتاجي: الطبعة الثانية، دار الكتب الوطنية بنغازي ليبيا.

ثانياً: المراجع الأجنبية:

- Crott, M : (1998) The Foundations Of Social Research, London, Sage.

- Grotty, J. and Johnson, P : (1997) Research Methods for Managers, London, Paul Chapman.

- Hennessry . Johan l : (1961) Recording of Lease Obligation and Related Property rights, The Journal of Accountancy.

- Hopper, T. and Powell, A : (1985) Making Sense of Research Into the Organizational and Social Aspects of Management Accounting A revie of ins Underlying Assumptions, Journal of Management Studies, 22 (5), 429-56.

- Hussey, J. Hssey, R : (1997) Business Research, UK, Antony Rowe.

- Fredrik. B: (2001**)** Implementing Information Security Management Systems, An Empirical Study of Critical Success Factors, http://WWW.Google.com. [22/05/2012].

- ISO/IEC, 27002: (2005) Information Technology Security Techniques, Code of Practice For Information Security Management, available at http://www.iso27001security.com/html/27002.html [15/05/2012].

- ISO/IEC, 27000: (2009) Information Technology, Security Techniques, information Security Management Systems, Overview and Vocabulary, First Edition, Reference number ISO/IEC2700:2009(E), available at http://www.iso.com [15/05/2012].

- Jacobs، J. Weiner، S: (1997) The CPA, s Role in Disaster Recovery Planning, The CPA Journal Online, Avalibale at http://www.nysscpa.org\cpajournal\1997\1197\features\f201197 [17/08/2012].

- Ko، S. Geuk، L. Yun، J: (2005) Development of an Intelligent Security Evalution Indices System for an Enterprise Organization, Computer Scinence, LNAI.3682, PP.1029-1035, Available at http://www.springerlink.com/content/1gau2db6rjj99c7t/ [08/08/2012].

- United States General Accounting Office، (GAO): (2003) Information Security Computer Control Over Key Treasury Internet Payment System, Available at: HTTP://WWW.Gao.gov. [22/07/2012].

- Wakefiled، R: (2000) IT Security Issues, The CPA Journal,

November, Available Online: http://www.nysscpa.org/cpajournal/ 2000 [04/07/2012].

- Wayne, A: (2002) Barnett's Independent Bank & Trust Blue Water, Texas Information Security Policy, march, available at http://www.google.com [15/08/2012].

- Luehlfing، S: (2000) Defending the security of the Accounting System، The CPA Journal October، Available Online: http://www.nysscpa.org/cpajournal/2000/1000/dept/d106200a.htm [12/05/2012].

- Chapin، A. Steven، A: (2005) How Can Security Be Measured?، Information Systems Control Journal، Available at: http://www.isaca.com [25/07/2012].

- Cerullo، M: (2005) Threat Assessment and Security Measures Justification for Advanced IT Networks، Available at: http://WWW.isaca.com [22/07/2013].

- National institute of Stander and Technology: (2008), Guide For Assessing The Security Controls In Federal Information Systems, U.S. Department of Commerce Special Publication 800-53A. Washinton DC:

نقلاً عن الدكتور مصطفى، أ: (2009) المجلة العلمية Government Printing Office. July.
للاقتصاد والتجارة، كلية الاقتصاد- جامعة عين شمس.

الملاحق

ملحــق رقــم (1)

استمــارة الاستبيــان

ملحق رقم (1)

استمارة الاستبيان

أولاً: البيانات الشخصية:

- المؤهل العلمي..... - عدد سنوات الخبرة.....
- المركز الوظيفي..... - عدد الدورات التدريبية .....

ثانياً: أسئلة استمارة الاستبيان:

المجموعة الأولي: إجراءات رقابة خفض الخطأ والغش:

م	الإجراء الرقابي	غير هام جداً	غير مهم	محايد	هام	هام جداً
1	الفصل الجيد بين وظائف تطوير نظم المعلومات، والوظائف المحاسبية.					
2	تناوب الواجبات لتقليل فرص حدوث الغش وزيادة فرص اكتشاف الخطأ.					
3	إعطاء إجازات إجبارية للعاملين لتخفيض احتمال الغش.					
4	التأكد من الصحيفة الجنائية للعاملين المصرح لهم الوصول للبيانات الهامة.					
5	وجود إشراف علي الوظائف الرقابية.					

6 - هل ترى هذه الإجراءات كافية لرقابة الوصول المادي؟ نعم ☐ لا ☐

في حالة أنها غير كافية رجاء ذكر السبب

.....

.....

المجموعة الثانية: إجراءات رقابة الوصول المادي:

م	الإجراء الرقابي	غير هام جداً	غير مهم	محايد	هام	هام جداً
1	وضع جهاز الخادم (Server) والمعدات الهامة في حجرات مغلقة بإحكام.					
2	وضع سجلات دخول وخروج حجرات الحاسب الآلي والمتابعة من الموظف المختص.					
3	وجود سجلات للزائرين يحتوي على البيانات الكافية وأسباب الزيارة.					

4	وجود تامين ضد السرقة والمخاطر الأخرى تغطي أجهزة الحاسب الآلي.					
5	تركيب أجهزة إنذار على معدات أجهزة الحاسب الآلي.					

6 -هل ترى هذه الإجراءات كافية لرقابة الوصول المادي؟ نعم ☐ لا ☐

في حالة أنها غير كافية رجاء ذكر السبب

.....

.....

المجموعة الثالثة: إجراءات رقابة الوصول المنطقي:

م	الإجراء الرقابي	غيرهام جداً	غير مهم	محايد	هام	هام جداً
1	كل مستخدم له الهوية (ID) وكلمة المرور الخاص به التي يصعب تخمينها.					
2	تغيير كلمات المرور بصورة دورية علي الأقل (90) يوم.					
3	احتواء كلمة المرور علي الأقل (6) أحرف واحدهم على الأقل رقمي.					
4	وضع شاشات توقف بكلمات مرور (Sceen Saver).					
5	توعية العاملين بضرورة عدم كتابة المرور أو إظهار علي الشاشة أو تداولها فيما بينهم.					
6	تحديد الأشخاص المصرح لهم منح تغيير هويات التعريف وكلمات المرور للمستخدمين.					
7	تحديد الأشخاص المفوض لهم الوصول إلي معلومات المصرف وتوفير الهويات اللازمة لذلك.					
8	منع النسخ غير المصرح به لرخص البرامج.					
9	منع استخدام نسخ غير أصلية من البرامج.					
10	توفير إجراءات رقابية لحماية أشرطة الأمن المخزنة في النظام والتي تستخدم من قبل النظام للتحقق من الصحة.					
11	استخدام برنامج ربط الشبكات الخاص الافتراضي (Virtual private networking) لمنع الوصول غير المصرح به.					
12	استخدام أنظمة تعقب المتطفلين لتوفير متابعة مستمرة لشبكة المصرف والاكتشاف المبكر للاختراقات الرقابية المحتملة.					
13	إجراء فحوصات رقابية للمخاطر المحتملة بصورة دورية والتقرير عن تلك المخاطر ونتائج الفحص للإدارة العليا.					
14	استخدام إجراءات التحقق من المسلك لضمان عدم إرسال الرسائل الكترونية إلي عناوين خاطئة.					
15	استخدام تقنيات التقرير عن الرسائل لإعلام الراسل إن الرسائل المرسلة تم استلامها.					
16	التحديد الإلكتروني لكل الشبكات الطرفية.					
17	في حالة الحاجة إلي تجاوز الإجراءات الرقابية لابد التأكد من توافر التصريح الملائم لذلك التجاوز.					

18- هل ترى هذه الإجراءات كافية لرقابة الوصول المادي؟ نعم ☐ لا ☐

في حالة أنها غير كافية رجاء ذكر السبب

.....

.....

المجموعة الرابعة: إجراءات رقابة أمن البيانات:

م	الإجراء الرقابي	غيرهام جداً	غير مهم	محايد	هام	هام جداً
1	تخزين الملفات في أماكن محمية من الحريق و الأتربة وأي ظروف ضارة.					
2	إعداد واستخدام دليل جيد للبيانات.					
3	تقسيم البيانات علي حسب أهميتها وتحديد مستوي الحماية المطلوب لكل نوع.					
4	تشفير البيانات الهامة.					
5	تحديد المستخدم المصرح له الحصول علي كل نوع من المعلومات، وتحديد التوقيت الملائم ومكان تواجدها.					
6	توفير إجراءات الحماية من الكتابة لضمان عدم إعادة الكتابة علي البيانات المخزنة أو حذفها.					
7	توفير جداول زمنية لإعداد نسخ احتياطية من البيانات وحفظها بصورة جيدة.					
8	منع استخدام لغات البرمجة المتقدمة التي قد تغيير من البيانات.					
9	تطبيق الإجراءات الرقابية الملائمة عند المناولة اليدوية للبيانات بين الانقسام المختلفة وبين المركز الرئيسي والفروع.					
10	متابعة البيانات الهامة بصورة دورية.					
11	حماية الأقراص المغناطيسية للنسخ الاحتياطية وحفظها في خزائن آمنة.					

12-هل ترى هذه الإجراءات كافية لرقابة الوصول المادي؟ نعم ☐ لا ☐

في حالة أنها غير كافية رجاء ذكر السبب

.....

.....

المجموعة الخامسة: إجراءات رقابة معايير التوثيق:

م	الإجراء الرقابي	غيرهام جداً	غير مهم	محايد	هام	هام جداً
1	التحديد الجيد للمعايير والإجراءات الخاصة بعمليات التخزين والمناولة للبيانات.					
2	تزويد المستخدمين بالتوجيهات اللازمة للتبليغ عن أي اختراقات أمنية للنظام.					
3	التحديد الجيد للإجراءات المتبعة في حالة عدم الالتزام بالسياسات الرقابية.					

4- هل ترى هذه الإجراءات كافية لرقابة الوصول المادي؟ نعم ☐ لا ☐

في حالة أنها غير كافية رجاء ذكر السبب

.....

.....

المجموعة السادسة: خطة التغلب علي اثأر الكارثة:

م	الإجراء الرقابي	غيرهام جداً	غير مهم	محايد	هام	هام جداً
1	التطبيقات والأجهزة والبرامج الضرورية للحفاظ على استمرار المصرف في حالة حدوث أي حالات طارئة.					
2	التحديد الجيد لكل الأنشطة اللازمة لاستعادة الإعمال وتتابع تنفيذ تلك الأنشطة والوقت اللازم لتنفيذ كل نشاط.					
3	الأماكن التي يمكن من خلالها متابعة مزاولة نشاط المصرف في حالة ما إذا كان الضرر يلحق بمباني المصرف					
4	إجراء فحص واختبار دوري لخطة التغلب على آثار الكارثة للتأكد من إمكانية تنفيذها في الواقع العملي.					
5	الاحتفاظ بالبرامج الأصلية في أماكن آمنة خارج المصرف حتى يمكن الاستفادة من تلك البرامج عند حدوث الكارثة.					
6	توفير نسخ احتياطية من كل الملفات والبرامج مخزنة خارج المصرف لتمكين المصرف من استعادة الملفات والبرامج المدمرة أو التي تم فقدها عند حدوث الكارثة.					
7	توفير إجراءات رقابية ملائمة تطبق على خروج وعودة ملفات البيانات والبرامج كم أماكن تخزينها إلي أماكن استخدامها.					
8	التحديد الواضح للأشخاص المسئولين عند تنفيذ خطة التغلب علي آثار الكارثة مع تحديد مسؤولية كل فرد من هؤلاء الأشخاص.					
9	توافر بوليصة تامين شاملة تغطي تكاليف أجهزة ومعدات الحاسب الآلي بالإضافة إلي تكاليف انقطاع الإعمال الذي قد ينتج من حدوث كوارث بالحاسب الآلي.					

10- هل ترى هذه الإجراءات كافية لرقابة الوصول المادي؟ نعم ☐ لا ☐

في حالة إنها غير كافية رجاء ذكر السبب

.....

.....

المجموعة السابعة: إجراءات الرقابة الخاصة بالانترنت والاتصالات والمصارف الالكترونية:

م	الإجراء الرقابي	غيرهام جداً	غير مهم	محايد	هام	هام جداً
1	وضع برامج الحماية ضد الفيروسات بما فيها البرامج الخاصة بفحص رسائل البريد الالكتروني الواردة، بالإضافة إلي التحديث المستمر لتلك البرامج.					
2	استخدام حوائط النار (أجهزة - برامج) لرقابة وحماية الاتصالات بين الشبكة الداخلية والشبكات الخارجية مثل الانترنت.					

3	وضع حد للصفقات النقدية الالكترونية التي تتم في اليوم الواحد علي نفس الحساب.					
4	توفير بطاقتي هوية (ID) لكل مستخدم لعمليات المصرف الالكترونية الأولي تستخدم في الاستعلامات العامة والثانية تستخدم في إجراء التحويلات والصفقات النقدية.					
5	تنشيط الحسابات الالكترونية يتم بعد التسجيل علي الموقع ويستطيع المستخدم الخروج بالخاصية الملائمة (Sign out) أو بعد مرور وقت قصير جداً من التوقف عن الاستخدام.					
6	حصر التحويلات النقدية علي الحسابات في نفس المصرف (المرسل والمرسل إليه في نفس المصرف).					
7	يتم منع الدخول علي حساب بعد ثلاث محاولات غير ناجحة لإدخال الهوية مع تسجيل تلك المحاولات حتى يتم متابعتها.					
8	يتم وقف التعامل علي أي حساب غير مستخدم لمدة 6 شهور.					
9	استخدام التشفير لتشفير المعلومات السرية والخاصة وهويات المستخدمين وكلمات المرور.					

10- هل ترى هذه الإجراءات كافية لرقابة الوصول المادي؟ نعم ☐ لا ☐

في حالة أنها غير كافية رجاء ذكر السبب

.....

.....

المجموعة الثامنة: إجراءات رقابة النتائج:

م	الإجراء الرقابي	غيرهام جداً	غير مهم	محايد	هام	هام جداً
1	كل مخرجات أنظمة المعلومات الهامة يتم الاحتفاظ بها في حجرات مقفلة.					
2	الدخول المصرح به للمعلومات الهامة يجب أن يتم مراقبته وتحديده للمستخدمين المصرح لهم خلال فترة التصريح.					
3	طباعة وتوزيع النسخ الورقية لمخرجات المنظومة يتم ختمها بالتوقيت والتاريخ في ظل إشراف ملائم.					
4	استخدام الآلات المخصصة للتخلص من الورق للتخلص من الأوراق التي تم الانتهاء منها.					
5	إجراء مراجعة عشوائية للمدخلات والمخرجات للتحقق من التشغيل الصحيح.					

6- هل ترى هذه الإجراءات كافية لرقابة الوصول المادي؟ نعم ☐ لا ☐

في حالة أنها غير كافية رجاء ذكر السبب

.....

.....

المجموعة التاسعة: أمن خدامات التعهيد:

م	الإجراء الرقابي	غيرهام جداً	غير مهم	محايد	هام	هام جداً
1	وجود تحديد واضح لمسؤوليات والتزامات كلا الطرفين في تعاقدات خدمات التعهيد،					
2	توثيق متطلبات الرقابة المستهدفة من قبل المصرف والتي يجب أن يلتزم بها موفر خدمات التعهيد.					
3	توفير التصريحات اللازمة لمقدم خدمات التعهيد حتى يتمكن من أداء الإعمال المكلف بها.					
4	تحديد مستوى الأداء الرقابي.					
5	تقييم الأداء الرقابي لموفر خدمات التعهيد من قبل المصرف.					

6- هل ترى هذه الإجراءات كافية لرقابة الوصول المادي؟ نعم ☐ لا ☐

في حالة أنها غير كافية رجاء ذكر السبب

.....

.....

ملحــق رقـــم (2)

مشروع نظام المدفوعات الوطني في المصارف الليبية

ملحق رقم (2)

مشروع نظام المدفوعات الوطني في المصارف الليبية

في إطار توجه مصرف ليبيا المركزي نحو تفعيل الاستفادة من تطورات تكنولوجيا المعلومات، وتحسين بنية العمل المصرفي، شرع المصرف المركزي والمصارف التجارية في تنفيذ برنامج يطمح إلى تطوير أنظمة الخدمات المصرفية بما يتوافق مع التطورات التكنولوجية، وهو ما يعرف **"بمشروع نظام المدفوعات الوطني"** وقد انبثقت من هذا النظام خمس مكونات أساسية وهى:

أولاً: منظومة التسوية الإجمالية الفورية Real Time Gross (RTGS) Settlement:

تعمل هذه المنظومة على تحويل الأموال عالية القيمة في نفس الوقت بين المصـــارف، وقد حدد مصرف ليبيا المركزي قيمة الحوالة بأكثر من (10,000) د.ل، مع توفر خدمة التوقيعات الإلكترونية وتشفير البيانات وتمكين المصارف المُشاركة من إدارة السيولة ومراقبة الحوالات الخاصة بها، وتم العمل الفعلي بهذه المنظومة بتاريخ 2008/4/1 م، ومن مميزات العمل بهذه المنظومة ما يلي:

1- خفض التكاليف والوقت باستعمال الخدمات الإلكترونية المتطورة.

2- خفض نسبة المخاطرة في الأنشطة التجارية والمدفوعات.

3- تسهيل وسائل منح وإدارة القروض ومخصصات المشاريع.

4- تسريع صرف المعاشات والمنح والمخصصات والقروض.

5- تسهيل إعداد الميزانيات للقطاعات الوطنية.

6- تمكين المصرف المركزي من مراقبة الخدمات والحسابات.

7- تمكين الأفراد والشركات والجهات العامة من تحصيل رسوم الخدمات آلياً.

المصارف المشاركة هي مصرف ليبيا المركزي، ومصرف الجمهورية، ومصرف الصحارى، والمصرف التجاري الوطني، ومصرف الوحدة، ومصرف شمال أفريقيا، ومصرف الواحة، ومصرف الأمان، ومصرف الخليج الأول الليبي، والمصرف الزراعي، ومصرف الادخار والاستثمار العقاري، ومصرف التجارة والتنمية، وشركة الصرافة والخدمات المالية، ومصرف السرايا، ومصرف الوفاء، ومصرف المتحد للتجارة والاستثمار، والمصرف الليبي الخارجي.

أما المصارف الجاري استكمال مشاركتها في نظام (RTGS) هي مصرف التنمية، والمصرف الريفي، ومصرف الإجماع العربي، والمصرف التجاري العربي، ومصرف المتوسط، والمصرف الليبي القطري.

ثانياً: منظومة المقاصة الإلكترونية Automated Cleaning House(ACH):

تُستخدم منظـــومة الدفع الإلكتـــروني لتنفيذ ومعالجـــة الحـــــوالات صغيرة القيمة **(Low Value)** وكثيرة العدد **(High Volum)**، أقل من (10,000) د.ل، ويتم من خلال هذه المنظومة تنفيذ جملة من الحوالات المتكررة مثل:(المرتبات، فواتير الكهرباء، ... الـخ)، كمـــا بدأ العمل الفعلـي بهذه المنظومـــة بتـــاريخ 2008/8/17 م ويُرَّحل صـــــافي التعامـلات إلـــى منظومـــة التسويـــة الفوريـــة (RTGS) خلال فترتين للتبادل، الأولى عند الساعة 11 صباحاً والثانـية عند الساعة 1:30 ظهراً، والتي ستقوم بتسوية المبالغ بين المصارف بشكل نهائي، ومن مميزات هذه المنظومة ما يلي:

1- خفض التكاليف والوقت باستعمال الخدمات الإلكترونية المتطورة.

2- خفض نسبة المخاطرة في الأنشطة التجارية والمدفوعات.

3- تسهيل وسائل منح وإدارة القروض ومخصصات المشاريع.

4- تسريع صرف المعاشات والمنح والمخصصات والقروض.

5- تسهيل إعداد الميزانيات للقطاعات الوطنية.

6- تمكين المصرف المركزي من مراقبة الخدمات والحسابات.

7- تمكين الأفراد والشركات والجهات العامة من تحصيل رسوم الخدمات آلياً.

أما المصارف المشاركة هي مصرف ليبيا المركزي، ومصرف الجمهورية، ومصرف الصحارى، والمصرف التجاري الوطني، ومصرف الوحدة، ومصرف شمال أفريقيا، ومصرف الواحة، ومصرف الأمان، ومصرف الخليج الأول الليبي، ومصرف الادخار والاستثمار العقاري، ومصرف التجارة والتنمية، وشركة الصرافة والخدمات المالية، ومصرف السرايا، ومصرف المتحد للتجارة والاستثمار.

والمصارف الجاري استكمال مشاركتها في نظام (ACH) **هي** مصرف التنمية، والمصرف الليبي الخارجي، ومصرف الوفاء، والمصرف الريفي، ومصرف الإجماع العربي، والمصرف التجاري العربي، ومصرف المتوسط، والمصرف الليبي القطري.

ثالثاً: منظومة معالجة الصكوك أليا Automated Checks (ACP) Processing:

تعمل هذه المنظومة على مقاصة الصكوك بين المصارف إلكترونياً باعتماد أسلوب المسح الضوئي والملفات الرقمية وترحيل صافي العمليات إلى منظومة المقاصة الآلية بما يسمح بتسوية قيم الصكوك بين المصارف بكل يسر وأمان، ومن فوائد العمل بهذه المنظومة ما يلي:

1- خفض التكاليف والوقت باستعمال الخدمات الإلكترونية المتطورة.

2- خفض نسبة المخاطرة في الأنشطة التجارية والمدفوعات.

3- تسهيل وسائل منح وإدارة القروض ومخصصات المشاريع.

4- تسريع صرف المعاشات والمنح والمخصصات والقروض.

5- تسهيل إعداد الميزانيات للقطاعات الوطنية.

6- تمكين المصرف المركزي من مراقبة الخدمات والحسابات.

7- تمكين الأفراد والشركات والجهات العامة من تحصيل رسوم الخدمات آلياً.

المصارف المشاركة هي مصرف ليبيا المركزي، ومصرف الجمهورية، ومصرف الصحارى، والمصرف التجاري الوطني، ومصرف الوحدة، ومصرف شمال أفريقيا، ومصرف الواحة، ومصرف ألامان، ومصرف الخليج الأول الليبي، والمصرف الزراعي، ومصرف الادخار والاستثمار العقاري، ومصرف التجارة والتنمية، وشركة الصرافة والخدمات المالية، ومصرف السرايا، ومصرف المتحد للتجارة والاستثمار، والمصرف الليبي الخارجي، والمصرف الليبي القطري.

رابعاً: نظام آلات السحب الذاتي ونقاط البيع وإدارة البطاقات Automatic Teller (ATM) Machine:

توفر هذه المنظومة بنية أساسية لموزع السحب الذاتي الوطني، الذي يمكن عن طريقه الوصول لكافة حسابات الزبائن الموجودة بأي من المصارف العاملة وإنجاز عمليات السحب النقدي للمبالغ المالية عن طريق آلات السحب الذاتي، باستخدام البطاقة الوطنية من خلال الشبكات، بالإضافة إلى استخدام بطاقات عالمية مثل **Card Master** و**Visa** من خلال الشبكات العالمية، وكذلك تمكين التجار وزبائنهم والشركات من توفير الخدمات وإتمام عمليات تسديد قسائم الخدمات إلكترونياً باستخدام نقاط البيع وإنجاز كافة العمليات المالية الإلكترونية المُتعارف عليها عالمياً، ومن فوائد العمل بهذه المنظومة ما يلي:

1- خفض التكاليف والوقت باستعمال الخدمات الإلكترونية المتطورة.

2- خفض نسبة المخاطرة في الأنشطة التجارية والمدفوعات.

3- تسهيل وسائل منح وإدارة القروض ومخصصات المشاريع.

4- تسريع صرف المعاشات والمنح والمخصصات والقروض.

5- تسهيل إعداد الميزانيات للقطاعات الوطنية.

6- تمكين المصرف المركزي من مراقبة الخدمات والحسابات.

7- تمكين الإفراد والشركات والجهات العامة من تحصيل رسوم الخدمات آلياً.

أما المصارف المشاركة هي مصرف ليبيا المركزي، ومصرف الجمهورية، ومصرف الصحارى، والمصرف التجاري الوطني، ومصرف الوحدة، مصرف شمال أفريقيا، ومصرف الواحة، ومصرف الأمان، ومصرف الخليج الأول الليبي، والمصرف الزراعي، ومصرف الادخار والاستثمار العقاري، ومصرف التجارة والتنمية، وشركة الصرافة والخدمات المالية، ومصرف السرايا، ومصرف المتحد للتجارة والاستثمار، والمصرف الليبي الخارجي، والمصرف الليبي القطري.

خامساً: المنظومة المصرفية الموحدة أو المتكاملة Core Banking (FLEXCUBE) System:

تم اختيار تطبيق المنظومة المصرفية المتكاملة (المصرف الشامل) الذي يعتمد على مزود لخدمة التطبيقات (**Application Service Provider- ASP**) التي تعمل بها المنظومة، والذي يُغطي العمليات المصرفية للأفراد والشركات معاً والخدمات المصرفية الإلكترونية، وأهم ما يُميز هذا النظام هو دعم تعدد الفروع (أي إمكانية تنفيذ المعاملات المالية عن طريق أي فرع دون الرجوع إلى الفرع الذي به حساب الزبون)، ودعم الحسابات بعملات مختلفة، دعم تعدد وسائل الاتصال والدفع **(Multi channels)**، ومركزية قواعد البيانات الخاصة بالزبائن والحسابات، وستتمكن المصارف عن طريق استخدام هذه المنظومة من تقديم خدمات مميزة للزبائن منها:

1- استخراج مراكز مالية مجمعة لحسابات الزبائن بجميع فروع المصرف الواحد.

2- إمكانية تنفيذ التحويلات المالية آليا بين جميع حسابات الزبون في فروع المصرف بما يعظم فرص الاستثمار للزبائن.

3- تزويد كبار الزبائن من شركات ومؤسسات بملفات إلكترونية تتضمن المركز اليومي والحركة اليومية.

4- تمكين المصارف من الاستجابة السريعة لمتطلبات السوق والزبائن، كما يدعم تقديم الخدمات المصرفية خلال (24) ساعة طوال الأسبوع، وتسهيل التعامل مع الحسابات عن طريق أي فرع من فروع المصرف، توفير خدمة دفع فواتير الخدمات آليا، والإخطار باستخدام الرسائل القصيرة

(**SMS**)، مع دعم الخدمـــات المصرفية عبر شبكة المعلومـــات الدوليـــة (**Internet banking**) في المرحلة القادمة.

5- دعم التخاطب مع المكونات الأساسية لنظام المدفوعات الوطني (نظام المقاصة الالكترونية، موزع آلات السحب الذاتي ونقاط البيع، نظـام التسويات الفورية، نظام معالجة الصكـــوك آلياً)، ودعـــم التخاطب المباشر مع نظام السوفيت **Swift**.

6- تمكين المصارف الليبية من تطبيق السياسات والمعايير المتعلقة بإدارات المخاطر والرقابة الائتمانية ومكافحة غسيل الأموال بفاعلية أكثر.

المصارف المشاركة هي مصرف ليبيا المركزي، ومصرف الجمهورية، ومصرف الصحارى، والمصرف التجاري الوطني، ومصرف الوحدة، ومصرف شمال أفريقيا، ومصرف الواحة، ومصرف الأمان، ومصرف الخليج الأول الليبي، والمصرف الزراعي، ومصرف الادخار والاستثمار العقاري، ومصرف التجارة والتنمية، وشركة الصرافة والخدمات المالية، ومصرف السرايا، ومصرف المتحد للتجارة والاستثمار، والمصرف الليبي الخارجي، والمصرف الليبي القطري.

ملحق رقـــم (3)

اختبـار التوزيـع الطبيــعي

ملحق رقم (3)

اختبار التوزيع الطبيعي

يتبين من بيانات الجداول والمخططات البيانية التالية ما يلي :

أولاً: بالنسبة للمتوسطات استجابات المراجعين الداخليين:

فقد تبين أن هذه البيانات موزعة توزيعاً طبيعياً، حيث بلغ الاحتمال المحسوب (Sig.=0.280) كما هو مبين بالجدول (1) وهو أكبر من مستوى الدلالة ألجدوليه ($\alpha = 0.05$)، الأمر الذي يدعونا لقبول فرضية العدم القائلة بأن البيانات تتوزع توزيعاً طبيعياً، حيث تم استخدام اختبار "كولومجروف- سمنروف" البسيط لعينة واحدة.

جدول رقـــم (1)

اختبار التوزيع الطبيعي لمتوسطات استجابات المراجعين الداخليين

One-Sample Kolmogorov-Smirnov Test

		المراجعين الداخليين
Normal Parameters [a,b]	Mean	3.4544
	Std. Deviation	.6287
Kolmogorov-Smirnov Z		.991
Asymp. Sig. (2-tailed)		.280

a. Test distribution is Normal.

b. Calculated from data.

ثانياً: بالنسبة للمتوسطات استجابات مشرفي المنظومات:

تبين أن هذه البيانات موزعة توزيعاً طبيعياً، حيث بلغ الاحتمال المحسوب (Sig.=0.312) كما هو مبين بالجدول (2) وهو أكبر من مستوى الدلالة الجدولية ($\alpha = 0.05$)، الأمر الذي يدعونا لقبول فرضية العدم القائلة بأن البيانات تتوزع توزيعاً طبيعياً، حيث تم استخدام اختبار "كولومجروف- سمنروف" البسيط لعينة واحدة.

جدول رقـــم (2)

اختبار التوزيع الطبيعي لمتوسطات استجابات مشرفي المنظومات

One-Sample Kolmogorov-Smirnov Test

		مشرفي المنظومات
Normal Parameters [a,b]	Mean	3.4744
	Std. Deviation	.7189
Kolmogorov-Smirnov Z		.963
Asymp. Sig. (2-tailed)		.312

a. Test distribution is Normal.

b. Calculated from data.

ثالثاً: بالنسبة للمتوسطات استجابات المراجعين الداخليين ومشرفي المنظومات:

فقد تبين أن هذه البيانات موزعة أيضاً توزيعاً طبيعياً، حيث بلغ الاحتمال المحسوب (Sig.=0.979) لطرفي التوزيع، كما هو مبين بالجدول (3-5) وهو أكبر من مستوى الدلالة الجدولية ($\alpha = 0.05$)، الأمر الذي يدعونا لقبول فرضية العدم القائلة بأن البيانات تتوزع توزيعاً طبيعياً، حيث تم استخدام اختبار "كولومجروف- سمنروف" لعينتين.

جدول رقـــم (3)

اختبار التوزيع الطبيعي كل من المراجعين الداخليين ومشرفي المنظومات

Two-Sample Kolmogorov-Smirnov Test

Test Statistics[a]

	متوسطات المشاهدات
Kolmogorov-Smirnov Z	.471
Asymp. Sig. (2-tailed)	.979

a. Grouping Variable: يغلها فقص

ملاحظة:

كما يمكن معرفة نوع التوزيع طبيعياً أم لا، وذلك من خلال استخدام النسبة بين معامل الالتواء (Skewness) إلى الخطأ المعياري له (Std. Error) ، فإذا وقعت نتيجة هذه النسبة بين قيمتي (t)، بمستوى دلالة $\alpha/2$ أي 0.025 ودرجات حرية 14 أي (n-1)وهذا بعني$(t_{0.025,14})$ وبالبحث في جدول توزيع t فإن قيمة t تبلغ ∓ 2.145 ، حيث نقبل فرض

العدم بأن البيانات تتوزع طبيعياً إذا وقعت النسبة المذكورة في هذا المدى، وإذا وقعت نتيجة النسبة خارج مجال $2.145 \mp$يتم رفض فرض العدم وبالتالي فأن البينات لا تتوزع طبيعياً.

- فبالنسبة للمراجعين الداخليين نجد أن نسبة معامل الالتواء إلى الخطأ المعياري له هي$\frac{-0.782}{0.717} = 1.091-$، (من جدول 3-1)، هذه القيمة تقع ضمن مجال قبول فرض العدم وبذلك فإن البيانات تتوزع طبيعياً.
- وبالنسبة لمشرفي المعامل نجد أن نسبة معامل الالتواء إلى الخطأ المعياري له هي $\frac{-0.875}{0.717} = 1.220-$، (من جدول 3-3)،هذه القيمة تقع ضمن مجال قبول فرض العدم، وبذلك فإن البيانات تتوزع طبيعياً.

Abstract

In spite of what electronic operation systems has achieved due to their multiple advantages in accounting information exchange and operating. These systems created many problems related to supervision of electronic information and in their protection from the unauthorized entry. Therefore, this study tries to know the mechanism of supervision in the united banking systems in Libyan Banks. This study consists of five chapters. The first chapter deals with its introduction, which consists of an introduction, the problems and the purposes of the study , the important, the methodology of the study and its society as well as its sample in addition to the study divisions.

In the second chapter the study introduces the concept, the purposes and the important of supervision in electronic accounting information systems in addition to the components and the basic principles of supervision in information systems. The classification of information systems supervision, security measurements and their development stages and the legal supervision dangers and risks have been known and dealt with. The study also dealt with methods, evaluation and the effecting factors in accounting supervision.

The third chapter deals only with the professional issues related to supervision in information systems and the studies which have specified the mechanism of information supervision systems and the threats which the supervision is subjected to in addition to the continuous changes and the fast technological progress.

The fourth chapter contains the applied study in order to choose the main hypothesis of the study. A questioner list (face to face) has been used. The questioner has been handed over to interior auditors and systems supervisors in addition to the remarks which have been collected from factual work procedures in the Libyan participating banks in the study. The achieved results of the study are represented in refusing the zero hypothesis and accepting the alternative hypothesis by the interior auditors and supervisors of the system. The study results also show the insufficiency of the united banking information system in the Libyan participating banks.

Finally, the fifth chapter presents the study recommendations, which their important concentrate on urge interior auditors and the supervisors of the united banking systems in Libyan banks to pay their attention to their expected role in evaluating of the supervision and monitoring systems. It also specified the dangers and risks which threaten the united banking system. It also requested them to participate in choosing the required suitable supervising rules and regulations to face such dangers and to provide the required specified professional training for the interior auditors and for the technological information specialists in the field of electronic accounting information and data supervision and monitoring in order to prepare and to create capable staff members to practice the required role in electronic accounting information systems.

Benghazi University
Faculty of Economics
Department of Accounting

Monitoring in integrated Banking System

"Applied study on Libyan banks"

By:

TAREK M. Y. EL-MEZINY

Bachelor of Accounting
Faculty of Economics
Benghazi University

Supervisor:

Dr. EDREES A. ALSHRIF

A thesis submitted in partial fulfillment of the requirement of Master's degree in accounting, Faculty of Economics, Benghazi University.

Spring 2013