مخاطر تكنولوجيا المعلومات من حيث الأطر والمعايير

رحاب عادل صلاح الدين أمين

مدرس مساعد بمعهد المدينة العالي للإدارة والتكنولوجيا بشبرامنت

يطلق مصطلح "الخطر" – في الغالب – على حدوث حدث ما غير مرغوب فيه. ولقد عرف معيار إدارة المخاطر الصادر عن معهد إدارة المخاطر، الخطر بأنه: احتمال حدوث حدث ما، والآثار المترتبة عليه. هذا، ويمكن القول بأن منهج إدارة المخاطر لابد أن يأخذ بعين الاعتبار، السمات الإيجابية والسلبية للمخاطر.

هنا يبدأ تصنيف المخاطر لأنواع عديدة، لعل محور النقاش في هذه الدراسة يتمثل في مخاطر تكنولوجيا المعلومات وسبل الحد منها عن طريق إطلاق حوكمة تكنولوجيا المعلومات لإدارة هذا الخطر المستحدث. والذي نشأ من التطور التكنولوجي على المستوى العالمي.

أنواع نظم المعلومات المحاسبية الإلكترونية

نظم المعلومات المحاسبية الإلكترونية الكبيرة: يتم استخدامها في تشغيل بيانات شركات حجم نشاطها كبير.

نظم المعلومات المحاسبية الإلكترونية الصغيرة: تستخدم الحاسبات الشخصية بما تمتلكه من قدرات كبيرة، واقتصادية ذات غرض عام.

نظم المعلومات المحاسبية المؤجرة: هناك بعض الشركات لا يتوافر لديها التسهيلات المالية اللازمة لتمويل عمليات شراء الحاسبات الإلكترونية، أو المنفعة من وراء شراء هذه الحاسبات. أي لا تبرر التكلفة لذلك فإنها تتعاقد مع مؤسسات تقدم خدمات حاسباتها الإلكترونية بمقابل مادي، أو تقديم خدمات مثل: أخذ البيانات، وتشغيلها على برامج لديها ثم إرسال النتائج للعميل (ابوشيبة، الفطيمي، ٢٠١٧).

مزايا استخدام تكنولوجيا المعلومات

١. رفع مستوى الأداء، والإنتاجية في الشركات.

٢. زيادة قيمة الشركة.

٣. فعالية اتخاذ القرارات.

٤. تنمية العمل.

٥. إعادة هندسة عمليات التشغيل.

٦. تدعيم نجاح الشركات في المجالات الإدارية، والتنظيمية المعقدة.

٧. تنمية السلوك الإيجابي لأفراد الشركة.

٨. تحسين إدارة الجودة الشاملة.

٩. تحسين إدارة المعلومات، والمعارف.

١٠. تحسين، وتطوير الخدمات المقدمة للعملاء (عوض، ٢٠١٦).

مخاطر استخدام تكنولوجيا المعلومات

١. مخاطر البنية التحتية المتعلقة بأنواع الأجهزة، والبرامج، والشبكات، وتعرضها لمخاطر مثل: التلف، أو الفقد الناتج من التقادم التكنولوجي، أو تغير تردد التيار الكهربائي.

٢. مخاطر الاختراق بالفيروسات.

٣. مخاطر الغش، والتلاعب.

٤. مخاطر الإفصاح الإلكتروني.

٥. مخاطر الموارد البشرية، وأهمية وجود عنصر بشري مؤهل للتعامل مع التكنولوجيا.

٦. مخاطر الثقة في المعلومات (عوض، ٢٠١٦).

مجالات للخطر المعلوماتي

١. الملفات الورقية: على الرغم من استخدام الحاسب الآلي، إلا أن الملفات الورقية مازالت تمثل نسبة كبيرة، وأهم التهديدات التي تمثلها عدم تصنيف الملفات، عدم سرية المعلومات، ومكان الحفظ.

٢. المعلومات: تعرض المعلومات للحذف، أو النسخ، أو التشويه، أو السرقة.

٣. الأجهزة: المخاطر التي تصاحب كافة المعدات، والأدوات المادية، وأهم التهديدات التي يمثلها الاستخدام الخاطىء، أو التصرف غير السليم، أو الحماية غير الجيدة، أو السرقة.

٤. الاتصالات: وتشمل شبكات الاتصال التي تربط أجهزة التقنية بعضها البعض، وتتيح فرصة اختراق النظم، ومحور الخطر هنا هو الشخص القائم بالاستخدام ومدى نزاهة المشاركين.

٥. البرامج: تتمثل الخطورة في حذف برنامج عرضي، أو عن غير قصد، أو سرقة برنامج. (بوقرة، ٢٠١٦).

حوكمة تكنولوجيا المعلومات

عرفها معهد حوكمة تكنولوجيا المعلومات IT Governance Institute عام ٢٠٠٣ على أنها مسؤولية من مسؤوليات مجلس الإدارة، والادارة التنفيذية وهي جزء مكمل لحوكمة الشركات وتتألف من القيادة، والهيكليات التنظيمية، والعمليات، وتضمن أن تكنولوجيا المعلومات بالمنظمة تساند، وتبرز أهداف، واستراتيجيات الشركة.

تصنيف مخاطر تكنولوجيا المعلومات

١. مخاطر إضافة قيمة/ فائدة لتكنولوجيا المعلومات IT Benefit / Value Enablement Risk: وهى تلك المخاطر المتعلقة بالفرص الضائعة لاستخدام تكنولوجيا المعلومات في تحسين كفاءة، أو فعالية العمليات التجارية.

٢. مخاطر تقديم مشروع وبرامج تكنولوجيا المعلومات IT Program and Project Delivery Risk: هى تلك المخاطر المتعلقة بمساهمة تكنولوجيا المعلومات في تقديم حلول جديدة، أو تحسين حلول قائمة لمشاكل الأعمال التجارية وتكون عادة في شكل مشاريع، أو برامج كجزء من المحافظ الاستثمارية.

٣. مخاطر عمليات تكنولوجيا المعلومات وتقديم الخدمات IT Operations and Service Delivery Risk: وهى تلك المخاطر المتعلقة بجميع جوانب أداء نظم، وخدمات المعلومات، والتي يمكن أن تؤثر سلبياُ (بالتدمير، أو التخفيض) على قيمة الشركة. (زيود وآخرون، ٢٠١٤).

مخاطر المدخلات مخاطر	مخاطر تشغيل البيانات	مخاطر المخرجات
- الإدخال غير المتعمد (غير المقصود) لبيانات غير سليمة بوساطة الموظفين. - الإدخال المتعمد (المقصود) لبيانات غير سليمة بوساطة الموظفين. - التدمير غير المتعمد للبيانات بوساطة الموظفين. - التدمير المتعمد (المقصود) للبيانات بوساطة الموظفين.	وهي المخاطر التي تتعلق بالمرحلة الثانية من مراحل النظام، وهي مرحلة تشغيل، ومعالجة البيانات المخزنة في ذاكرة الحاسب، وتتمثل تلك المخاطر في البنود التالية: - الوصول غير الشرعي (غير المرخص به) للبيانات، والنظام بوساطة الموظفين. - الوصول غير الشرعي للبيانات، والنظام بوساطة أشخاص من خارج المنشأة. - اشتراك العديد من الموظفين في نفس كلمة السر. - إدخال فيروس الكمبيوتر للنظام المحاسبي، والتأثير على عملية تشغيل بيانات النظام. - اعتراض وصول البيانات من أجهزة الخوادم إلى أجهزة المستخدمين.	تتعلق تلك المخاطر بمرحلة مخرجات عمليات معالجة البيانات، وما يصدر عن هذه المرحلة من قوائم للحسابات، أو تقارير، واشرطة، وملفات، وكيفية استلام تلك المخرجات. - تدمير بنود معينة من المخرجات. - خلق مخرجات زائفة غير صحيحة. - سرقة البيانات/ المعلومات. - عمل نسخ غير مصرح (مرخص) بها من المخرجات. - الكشف غير المرخص به لبيانات عن طريق عرضها على شاشات العرض، أو طبعها على الورق. - طبع، وتوزيع المعلومات بوساطة أشخاص غير مصرح لهم بذلك. - المطبوعات والمعلومات الموزعة يتم توجيهها خطأ إلى اشخاص غير مخولين باستلام نسخة منها. - تسليم المستندات الحساسة إلى أشخاص لا تتوافر فيهم الناحية الأمنية.

معايير حوكمة أمن المعلومات

١. ظهرت COSO (Committee of sponsoring organization of the Treadway Commission) في عام ١٩٨٥ لتعزيز فاعلية الرقابة الداخلية. إلا أن COSO قد أدركت مدى أهمية المعلومات، وضرورة الرقابة عليها فقامت بالتعاون مع ISACA Information System audit & Control Association لإيجاد أطر تحكم مسؤليات المستخدمين من الأمن، والحماية، والرقابة، ودور المعلومات في عملية إتخاذ القرارات فتم إطلاق COBIT: Control Objective for Information related technology عام 1996.

٢. وآخر ما توصلت إليه ISACA كان COBIT5 عام ٢٠١٢ وهو يتعامل مع ٣٤ هدفًا بين الحاكمية، والإدارة ويسعى لخلق القيمة من خلال استغلال الموارد، وتقليل المخاطر، وتحقيق المنافع،

ويربط الأهداف التكنولوجية مع الأهداف الخاصة بالشركة، واحتياجات المساهمين. (حداد، ٢٠١٣).

٣. كما كان لمعايير الأيزو ISO / IEC 27K دور هام في حوكمة أمن المعلومات: وقبل الوصول إليها يجب تقديم نبذة عنها فهى سلسلة من المعايير التي أصدرتها المنظمة الدولية للمعايير (ISO) وتم تطويرها بالتعاون مع اللجنة الدولية IEC وهى معايير متعلقة بأمن المعلومات، وتعمل على تقديم الارشادات المقبولة عامة بشأن الممارسات الجيدة لأنظمة إدارة أمن المعلومات المصممة لحماية سرية، وسلامة وتوافر محتوى المعلومات، ونظم المعلومات.

أولاً: إطار COBIT

يعد إطار عمل COBIT من أهم التطورات للرقابة الداخلية في مجال حوكمة تكنولوجيا المعلومات، إذ يهدف هذا الإطار إلى مجموعة من أفضل ممارسات الحوكمة لنظم المعلومات الإلكترونية، والتكنولوجية، ويرجع ظهوره لمنتصف التسعينات من القرن الماضى. (الحسناوي والموسوي، ٢٠١٧).

معايير المعلومات وفقًا لإطار عمل COBIT

الفعالية، الكفاءة، الموثوقية، الالتزام، السرية، سلامة المعلومات، التوافر (نصور، ٢٠١٥).

اهداف الرقابة التي يحققها اطار عمل COBIT

١. تهتم بالنتائج التي يراد تحقيقها من وجود نظام رقابي داخلي.

٢. تهتم برفع التقارير الآلية أى فيما يتعلق بنظام المعلومات المحاسبية.

٣. تبحث في الالتزام بالقوانين واللوائح، لكل من المواضيع المالية، وغير المالية. وتعد الرقابة على الالتزام بالقوانين، واللوائح هامة في منع أعمال الاحتيال، والأعمال غير القانونية.

مزايا اعتماد إطار عمل COBIT كإطار للحوكمة.

١. الرقابة المحكمة على معلومات الشركة، والتكنولوجيا المرتبطة بها.

٢. مراقبة، ومتابعة ما تحققه تكنولوجيا المعلومات من منافع للمنظمة.

٣. إدارة أداء تكنولوجيا المعلومات بشكل أفضل.

٤. إدارة موارد تكنولوجيا المعلومات بشكل أفضل.

٥. إدارة المخاطر المرتبطة بتكنولوجيا المعلومات بشكل أفضل.

٦. تحقيق قيمة مضافة لأعمال الشركة.

٧. إتاحة الفرصة لإدارة الشركة للقيام بالمقارنة المرجعية Benchmark فيما يتعلق بحماية تكنولوجيا المعلومات، والرقابة عليها.

٨. اطمئنان مستخدمي خدمات تكنولوجيا المعلومات على كفاية الحماية، وتوفير الرقابة المناسبة.

٩. يستطيع المراجع إبداء رأيه بالرقابة الداخلية، وتقديم نصائحه على مدى توافر الأمن لتكنولوجيا المعلومات ويقدم COBIT تفاصيل، ونماذج سهلة الاستعمال لحوكمة تكنولوجيا المعلومات. (يعقوب ونعيم، ٢٠١٤. عوض، ٢٠١٦).

أبعاد وعمليات COBIT

INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION, 2012, P.

أبعاد COBIT	عمليات COBIT	
التقييم، والتوجيه، والمراقبة المستمرة Evaluate, Direct&Monitor	وضع إطار عمل للحوكمة	EDM1
	التأكد من تحقيق قيمة مثالية	EDM2
	التأكد من تحسين المخاطر	EDM3
	التأكد من استغلال الموارد بالطرق المثلي	EDM4
	التأكد من شفافية أصحاب المصالح	EDM5
	تحديد إطار عمل لإدارة تكنولوجيا المعلومات	APO1
	تحديد الاستراتيجية	APO2
	إدارة هندسة المشروع	APO3
	إدارة الابتكار	APO4
	إدارة المحفظة	APO5
	إدارة الموازنة، والتكاليف	APO6
	إدارة الموارد البشرية	APO7
	إدارة العلاقات	APO8
	إدارة اتفاقيات الخدمات	APO9
	إدارة الموردين	APO10
	إدارة الجودة	APO11
	إدارة المخاطر	APO12
الأنشاء، والاقتناء، والتطبيق Build, Acquire&Implement	إدارة البرامج، والمشروعات	BAI1
	تحديد المتطلبات	BAI2
	تحديد وإنشاء الحلول	BAI3
	دراسة تكنولوجيا المعلومات المراد تطبيقها	BAI4
	إدارة التغير المؤسسي	BAI5
	إدارة التغييرات	BAI6
	إدارة تقبل التغير، والانتقال	BAI7
	إدارة المعرفة	BAI8

التسليم، والخدمة، والدعم Deliver, Service &Support	إدارة التشغيل إدارة الأصول إدارة التدريب إدارة طلبات الخدمات، والحوادث إدارة المشاكل إدارة الاستمرارية إدارة أمن الخدمات إدارة رقابة العملية	DSS1 DSS2 DSS3 DSS4 DSS5 DSS6 DSS7 DSS8
المراقبة، والتقويم، والتقييم Monitor,Evaluate &Assess	مراقبة وتقويم الأداء مراقبة نظام الرقابة الداخلية مراقبة، وتقييم الالتزام بالمتطلبات الخارجية	MEA1 MEA2 MEA3

ثانيًا : معايير الأيزو ISO

١. معيار (ISO / IEC 27001:2013): تم تعديل هذا المعيار، وأصدر في ستمبر ٢٠١٣ وهو يحدد بشكل رسمى المتطلبات الإلزامية لنظام إدارة أمن المعلومات. كما يوفر هذا المعيار إطاراً للإدارة الشاملة الذى تقوم الشركة من خلاله بتحديد، ومعالجة المخاطر الأمنية للمعلومات، ويضمن أن الترتيبات الأمنية تم ضبطها بدقة لمواكبة التغييرات الأمنية التي تحدث، واكتشاف نقاط الضعف.

٢. معيار (ISO / IEC 27002:2013) : يعرف هذا المعيار في السابق ب ISO 17799 وتم تعديله في عام ٢٠٠٥ ثم في عام ٢٠١٣ ليظهر بهذه الصورة، وهو معيار يوضح الممارسات الجيدة لأمن المعلومات، ويعمل على تقديم إرشادات توجيهية مفصلة حول كيفية تنفيذ إطار إدارة الأمن، وكيفية الالتزام بالقوانين واللوائح، والمعايير، ويتعلق هذا المعيار بأمن جميع أشكال المعلومات مثل: بيانات الكمبيوتر، والوثائق، والمعرفة، والملكية الفكرية، وليس فقط أمن تكنولوجيا المعلومات.

٣. معيار (ISO / IEC 27016: 2014): إصدر هذا المعيار في ٢٠١٤ ويهدف إلى تقديم المبادىء التوجيهية القائمة على الممارسات الجيدة المقبولة عمومًا، والتي يمكن استخدامها، وفهمها من قبل أصحاب الخبرة في مجال أمن المعلومات، والمديرين، وذلك لمناقشة الخطوات الإجرائية، والبدائل المتاحة لبرنامج أمن المعلومات من حيث النتائج المالية المتوقعة، وبمعنى آخر فإن هذا المعيار يهدف إلى تقديم مبادىء توجيهية حول كيفية قيام الشركات باتخاذ قرارات لحماية أمن المعلومات، وفهم النتائج الاقتصادية لهذه القرارات في إطار متطلبات التنافس على الموارد.

٤. معيار ISO/IEC 27038:2014 أصدر هذا المعيار في مارس ٢٠١٤ ويسمى أيضًا بمعيار التنقيح Redaction ويعني إبعاد المعلومات الحساسة مثل: أسماء المواقع التي يجب أن تظل مجهولة، ومختلف المعلومات الشخصية التي يجب أن تبقى سرية للغاية من داخل الملفات الأصلية حتى لا يتم نشرها لأطراف ثالثة، أو لعامة الناس. ويهدف هذا المعيار إلى تحديد الخصائص التكنولوجية للقيام بعملية التنقيح الرقمى على الوثائق الرقمية. كما يحدد متطلبات أدوات برامج التنقيح، وطرق الفحص، والاختيار التي تمت على عمليات التنقيح الرقمى التي تم الانتهاء منها بشكل آمن.

ثالثًا: معيار (ITIL) INFORMATION TECHNOLOGY INFRASTRUCTURE LIBRARY

يعتبر معيار ITIL مكتبة البنية التحتية لتكنولوجيا المعلومات من أكثر المناهج قبولاً في العالم لإدارة خدمات تكنولوجيا المعلومات، تم وضعه من قبل مكتب التجارة الحكومى في المملكة المتحدة، وهو عبارة عن مجموعة من الأرشادات لأفضل الممارسات في مجال إدارة خدمات تكنولوجيا المعلومات، فهو يصنف العمليات والوظائف، والهياكل التي تعمل على تدعيم خدمات تكنولوجيا المعلومات من وجهة نظر مقدمي الخدمة، ويعتبر أمن المعلومات واحداً من العديد من العمليات التي يصنفها معيار ITIL ويتكون معيار ITIL من ثمانية جوانب رئيسة هي: دعم الخدمة، وتوصيل الخدمة، وإدارة البنية التحتية لتكنولوجيا المعلومات والاتصالات، وإدارة الأصول (البرمجيات)، والتخطيط لتنفيذ إدارة الخدمات، والتنفيذ على نطاق صغير.

نظرة عامة

إن قيام الشركات بتطبيق معايير حوكمة أمن المعلومات متمثلة في معايير الأيزو ISO/IEC 27K ومعيار COBIT5 ومعيار ITIL كإطار عمل متكامل لحوكمة أمن المعلومات حيث لا يمكن لأحد من تلك المعايير منفرداً أن يفي باحتياجات ومتطلبات الشركة في تحقيق أهدافها سوف يحقق لها العديد من الفوائد، والمميزات وتحقيق للأهداف الاستراتيجية المرجوة في تطبيق حوكمة أمن المعلومات، وفي الحد من المخاطر التي تتعرض لها أنظمة المعلومات الإلكترونية بصفة عامة، وأنظمة المعلومات المحاسبية الإلكترونية على وجه التحديد، وتحقيق رؤية، وأهداف الشركة الاستراتيجية. (زيود وآخرون، ٢٠١٤)

دور محوري لقانون (SOX) SARBANES- OXLEY

يعد هذا القانون ذا أهمية بالغة لتكنولوجيا المعلومات وإن الهدف منه العمل على حماية وإصلاح وظيفة شركات المحاسبة العامة من أجل الوصول لقرارات آمنة. وقد وقع كقانون للرقابة الداخلية عام ٢٠٠٢ شاملاً على معايير موثوقية لتطبيقها على الشركات لحماية المستثمرين من حالات الغش، والتلاعب، وزيادة ثقتهم في إفصاح الشركات. ويركز تحديداً SOX على التقارير المالية، والتي تعد إلكترونيًا لزيادة الثقة بها. (منصور، ٢٠١٥)

تقدير مخاطر نظم تكنولوجيا المعلومات

عند القيام بتقدير مخاطر نظم تكنولوجيا المعلومات: لابد من أن تقوم المنشأة بتحديد الحدث الذي ينطوي على قدر من الخطورة، واحتمال وقوع هذا الحدث. ومن العوامل الهامة التي ينبغي وضعها في الاعتبار حال تقدير احتمال حدوث الخطر/ الآثار المترتبة عليه:

٥. عدم توافر برامج التطبيقات الملائمة.

٦. ارتفاع مستوى تعقد برامج التطبيقات الخاصة بنظم تكنولوجيا المعلومات.

٧. عمر نظام تكنولوجيا المعلومات/ برامج التطبيقات.

٨. المشاكل السابقة التي كان يعاني منها نظام تكنولوجيا المعلومات/ برامج التطبيقات.

إدارة المخاطر في أمن المعلومات

يعد وقوع المخاطر الأمنية من المؤثرات السلبية في أداء أى نظام للمعلومات، لذلك لابد من مواجهتها، ومن هنا نشأ مفهوم إدارة المخاطر في مجال أمن المعلومات، والاستجابة للمخاطر من خلال الخطوات التالية:

١. تجنب المخاطر: عن طريق تجنب استخدام تقنيات لا تستطيع المنظمة حماية النظام من المخاطر المحتملة الناتجة عن استخدامها. (مثلاً عدم قدرة المنظمة على استخدام تطبيقات التشفير، وحماية البيانات من الاعتداء الخارجى فمن الأفضل عدم ربط النظام بشبكة الانترنت، والاكتفاء بشبكة محلية على مستوى المنظمة).

٢. تقليل المخاطر: من خلال تنفيذ ضوابط التخفيف من المخاطر أى استخدام وسائل حماية قوية، والالتزام بمعايير أمن المعلومات العالمية، والتوصيات المرتبطة بها عند تطوير نظم المعلومات.

٣. قبول المخاطر ضمن الحدود المقبولة : إذا كانت تكلفة التأمين تزيد عن العائد المتوقع، يتطلب ذلك تقييم الأصول المعلوماتية للشركة، وتحديد قيمتها، وتكلفة المخاطر التي قد تتعرض لها، ولا مانع من قبول بعض المخاطر التي تزيد تكلفة تأمينها عن تكلفة تلك المخاطر في حال حدوثها، ويتتم توثيق ذلك، ومراجعته في المستقبل.

٤. نقل المخاطر ليتحملها طرف آخر: على سبيل المثال: التأمين على التكنولوجيا المستخدمة لدى شركة التأمين.

٥. وقف العمل بالنظام والبدء بتطوير نظام أكثر أمانًا: وهذا يحدث في حالة وقوع المخاطر، وتفشل سبل الحماية المتبعة من منعها مما يلحق ضررًا كبيرًا في نظام المعلومات، ومكوناته المختلفة بسبب الثغرات الأمنية المتعددة. (الذنيبات، ٢٠١٥)

إجراءات الرقابة الداخلية على أنظمة تكنولوجيا المعلومات

يمكن أن تصنف إجراءات الرقابة الداخلية التي تصمم على أنظمة تكنولوجيا المعلومات إلى الفئات التالية:

٦. إجراءات الأمن (Security Controls): التي تهدف إلى منع الوصول، والتعديل غير المرخص به/ أو إلحاق الضرر بالمعلومات.

٧. إجراءات النزاهة (Integrity Controls): التي تهدف إلى التحقق من مدى دقة، واتساق المعلومات الخاصة بالشركة، وخلوها من الغش، والفساد.

٨. إجراءات الطوارئ (Contingency Controls): التي تهدف إلى التحقق من إجراء النسخ الاحتياطي للمعلومات الخاصة بالمنشأة، ووجود خطة لإستعادة أنشطة، وعمليات المنشأة بعد حدوث آية أزمة عارضة.

٩. إجراءات الرقابة العامة (General Controls): التي تهدف إلى التحقق من مدى فعالية نظم تكنولوجيا المعلومات بصورة عامة، والتحقق كذلك من الاستخدام الملائم لأنظمة الحاسب الآلي.

١٠. إجراءات الرقابة الداخلية الخاصة ببرامج التطبيقات (Application Controls): والتي تصمم خصيصًا على كل برنامج، لمنع، واكتشاف، وتصحيح أية أخطاء في التشغيل.

١١. Software control: والتي تهدف إلى منع الوصول غير المرخص به إلى نظم Software الخاصة بالشركة.

١٢. إجراءات الرقابة الداخلية الخاصة بشبكات الاتصال (Network Controls): التي تهدف إلى منع الوصول غير المرخص به إلى البيانات التي يتم تداولها عبر شبكات الاتصال.

المراجع

١. زيود، وآخرون، (٢٠١٤). تحديد مستوى حوكمة تكنولوجيا المعلومات المطبق في المصرف التجاري السوري باللاذقية وفق إطار عمل COBIT. مجلة جامعة تشرين للبحوث والدراسات التعليمية. المجلد ٣٦. العدد ٢. ص ١٨٩-٢١٠.

٢. حداد، حسام باسم يوسف، (٢٠١٣). مستوى حاكمية تكنولوجيا المعلومات وأثره على مستوى الأداء المالي للبنوك العاملة في الأردن دراسة ميدانية باستخدام أهداف الرقابة للمعلومات والتكنولوجيا المرتبطة بها COBIT5. رسالة ماجستير. كلية الدراسات العليا والبحث العلمي. جامعة الزرقاء.

٣. الحسناوي، عقيل حمزة حبيب، الموسوي، انعام محسن، (٢٠١٧). دور حوكمة تقنيات المعلومات في تقليل مخاطر تدقيق نظم معلومات المحاسبة المحوسب في ظل إطار عمل (COBIT) للرقابة الداخلية. مجلة كلية الإدارة والاقتصاد للدراسات الاقتصادية والمالية. المجلد ٩، العدد ٣.

٤. نصور، ريم محمد، (٢٠١٥). أثر حوكمة تقنيات المعلومات علي جودة التقارير المالية دراسة ميدانية. رسالة دكتوراه. جامعة تشرين. كلية الاقتصاد. سوريا.

٥. يعقوب، فيحاء عبد الله، نعيم، علي حميدا، (٢٠١٤). دليل مقترح لتدقيق النظام المحاسبي المؤتمت علي وفق أطار COBIT. مجلة دراسات محاسبية ومالية. المجلد ٩. العدد ٢٨. ص ٨٩- ١٢٠.

٦. عوض، أيه عادل محمد، (٢٠١٦). أثر حوكمة تكنولوجيا المعلومات على تحليل التكلفة والعائد لقرارات الاستثمار الداخلي في نظم المعلومات المحاسبية. رسالة ماجستير. كلية التجارة. جامعة القاهرة.