إجراءات حوكمة تقنية المعلومات وانموذج مقترح في ضوء اهداف اطار COBIT

أ.د كريمه علي كاظم الجوهر* احمد جاسم حمودي**

المستخلص:

تُعَرَّف الرقابة الداخلية حسب معيار التدقيق الدولي 315 الموسوم بـ "فهم الوحدة الاقتصادية وبيئتها وتقدير مخاطر التحريف المادي" على أنها "العملية التي تُصَمم، وتُنَفَذ، ويتم العمل على إدامتها من قِبَل أولئك المكلفين بالحوكمة، وبالإدارة، ومن قِبَل أفراد آخرين لتوفير تأكيد معقول حول إنجاز الوحدة الاقتصادية لأهدافها مع الأخذ في الحسبان موثوقية الابلاغ المالي، وفعالية وكفاءة العمليات التشغيلية، والالتزام بتطبيق القوانين والتشريعات" ونظرا لتزايد اهمية التاثيرات التي أصبحت تشكلها تقنية المعلومات بالنسبة لاجراءات الرقابة الداخلية ، فانه يكون من الضروري معرفتها وتحليلها لذا جاء اهتمام الباحثان بهذا الموضوع بهدف التعريف باطار COBIT ودوره في تعزيز الحوكمة واجراءات الرقابة الداخلية ، وامكانية الاستفادة من مجالاته واهدافه في تصميم انموذج لاجراءات الرقابة الداخلية يصلح للاسترشاد به في الوحدات الاقتصادية المستعملة لتقنية المعلومات ولتحقيق ذلك اعتمد الباحثان منهج التحليل الوصفي من خلال الاعتماد على المصادر المرتبطة بالموضوع وتم التوصل الى بعض النتائج منها ان المفهوم العام لتقنيات المعلومات يعبر عن مجموعة عناصر تتفاعل فيما بينها من أجل أداء مهام محددة. وان تبني هذه التقنيات يتطلب توفير البيئة المناسبة لفهم المكونات المادية والبرمجيات و توفير موارد مناسبة لتقنية المعلومات، وبُناها التحتية والمهارات المطلوبة.ويمكن الاسترشاد باطارCOBIT في وضع الاجراءات الرقابية المناسبة التي تحقق فاعلية استخدام تلك المكونات

Abstract

Internal control define by the International Standard 315 "understanding economic unity and environment and risk assessment distortion material" as "the process that are designed, implemented, and are working to sustain by those charged with governance, and management, and by other individuals to provide reasonable assurance about the achievement Economic Unity of objectives taking the reliability of financial reporting, and the effectiveness and efficiency of operations, and commitment to the application of laws and legislation "Given the increasing importance of effects that have become posed Information Technology for internal control procedures, it is necessary to know and analyze so came the attention of researchers to this subject in order to profile the framework COBIT and its role in strengthening governance and internal

* الجامعة المستنصرية / كلية الادارة والاقتصاد .

** باحث .

بحث مستل من رسالة ماجستير

مقبول للنشر بتأريخ 2013/9/9

control procedures, and the possibility to take advantage of its scope and objectives in the design of a model for internal control procedures fit to guide the economic units used for Information Technology To achieve this adopted researchers approach descriptive analysis by relying on sources associated with the subject was reached some conclusions from them that general concept of information technology reflects the group elements interact with each other in order to perform specific tasks. And that the adoption of these techniques requires the provision of an appropriate environment to understand the hardware and software and provide adequate resources for the information technology, infrastructure and the skills required. COBIT framework can be guided to develop appropriate regulatory measures that achieve effective use of those components.

المقدمة

ان حوكمة تقنية المعلومات المؤسسية تتعلق بالكيفية التي توفر للمنظمة فرصة السيطرة التامة على تقنيات المعلومات ، بما يمكن المنظومة المعلوماتية من توفير المعلومات التي يحتاجها اصحاب المصلحة بمختلف فئاتهم بطريقة دقيقة وآمنة وبما يدعم اعمال المنظمة ويساندها في تحقيق اهدافها الاستراتيجية ، وأيضا كيف تتمكن المنظمة من توفير حد ادنى من الحماية للمصادر والأدوات المعلوماتية وردع المخاطر التي تهددها ، فالحوكمة باختصار هي رعاية وحماية. ولتحقيق حوكمة يتم تطبيق مجموعة من السياسات والممارسات والإجراءات المدعومة بالهياكل التنظيمية ، والمهام الوظيفية المحددة والمتكاملة لضمان تحقيق الاهداف الاستراتيجية لتقنية المعلومات المنبثقة من الاهداف الاستراتيجية للمنظمة ، مع مجموعة من الضوابط التي تمنع وقوع الاحداث غير المرغوبة ، او تكتشفها بسرعة متى حدثت وتعمل على احتوائها .ولاهمية الموضوع تم تناوله من خلال عدة محاور تطرق المحور الاول لمنهجية البحث اما الثاني فتطرق الى اهم الدراسات السابقة المرتبطة بتقنية المعلومات والرقابة الداخلية ، اما المحور الثالث فلخص الاطار العام للدراسة الذي تم تناول فيه مفهوم حوكمة تقنية المعلومات والحاجه اليها واطار COBIT ومجالاته واهدافه ، اما المحور الرابع فتضمن الانموذج المقترح لانشطة الرقابة الداخلية ، ولخص المحور الخامس اهم الاستنتاجات والتوصيات .

أولا : الإطار المنهجي للبحث

يستلزم البحث العلمي الأكاديمي وضع منهجية توضح الأساس الفكري الذي استند إليه البحث إذ تعد المنهجية بمثابة المسار الذي يوضح توجه البحث للوصول إلى تحقيق الأهداف المحددة وذلك من خلال إيضاح مشكلة، و أهمية البحث و الفرضيات التي استند إليها، وسبل الوصول إلى نتائجه

مشكلة البحث

تواجه الوحدات الاقتصادية مخاطر عديده نتيجة التغيرات في بيئة التشغيل.وإستعمال نظم معلومات جديدة، أو مُحَدَّثَة.وتطبيق تقنيات جديدة، مما يتطلب احكام اجراءات الرقابة الداخلية بالشكل الذي يقلل من هذه المخاطر لذا سيحاول الباحثان معالجة هذه المشكلة من خلال الاجابة على التساؤلات التالية :

ماهو مفهوم حوكمة تقنية المعلومات ؟

ما هي مجالات و اهداف اطار COBIT ؟

هل يمكن الاستفادة من هذا الاطار في تصميم اجراءات للرقابة الداخلية تقلل من مخاطر تقنية المعلومات ؟

اهمية البحث

يُعَد إهتمام الادارة وإدراكها لوظائف نظم تقنية المعلومات ضروريا لوضع أسس حول أهمية الأمور الرقابية على نطاق الوحدة ككل. وقدمت مؤسسة تدقيق ورقابة نظم المعلومات ، إطاراً للأهداف الرقابية لتقنية المعلومات Control Objectives for Information Technology (COBIT)، كانموذج لإدارة ورقابة تقنية المعلومات، والذي يُعَد في نفس الوقت أداة لتقويم حوكمة تقنية المعلومات.و يُعَد اطار COBIT مفيداً للادارة والمدققين من خلال تدعيم وجهة نظرهم عن الرقابة الداخلية، وتقديم رأي ومشورة حول رقابات تقنية المعلومات ، كذلك يُعَد إطار COBIT متمما تكامُليا مع إطار لجنة دعم المنظمات COSO ، وداعِماً إضافيا للرقابة على تقنية المعلومات .

اهداف البحث

يسعى البحث لتحقيق الاهداف التالية

1. التعريف باطار COBIT واهدافه ومجالاته
2. تحديد دور اطار COBITفي تعزيز الحوكمة واجراءات الرقابة الداخلية في ظل استخدام التقنية
3. وضع أنموذج لإجراءات الرقابة الداخلية في ضوء هذا الإطار

فرضية البحث

يستند البحث الى الفرضية التالية :

يمكن وضع أنموذج لاجراءات الرقابة الداخلية تتحكم بتقنية المعلومات من خلال مجالات و اهداف اطار COBIT

منهجية البحث

اعتمد البحث على منهج التحليل الوصفي بالاعتماد على مجموعة من الأدوات البحثية لغرض إكمال متطلباته بالاعتماد على ما هو متوافر من مصادر عربية وأجنبية من دراسات وبحوث علمية محكمة ، فضلا عن النشرات والمعايير التي تصدرها المنظمات المهنية المختصة، والتي تم الحصول عليها من المكتبات وشبكات الانترنت.

ثانيا : دراسات سابقة

1- دراسة (Austen et al.,2000) بعنوان"العلاقة بين تقدير المخاطر وتقنية المعلومات لإكتشاف التحريفات".

هدفت الدراسة على بيان العلاقة بين حوسبة نظم المعلومات المحاسبية وتقدير المخاطر من خلال تحديد نطاق حدوث التحريفات . ومن أبرز ما توصلت إليهِ الدراسة انه توجد عوامل ضمنية ذات صِلة بحدوث التحريفات على مستوى القوائم المالية ومنها درجة الاجتهاد المطلوبة عند تحديد أرصدة الحسابات ' نزاهة الإدارة،و تكون تسويات ما قبل نهاية الفترة المحاسبية، ذات صِلة مع كِبَر حجم أو مقدار التحريفات.و تحتوي النظم المحوسبة جزئياً على تحريفات أكثر بسبب عدم كفاية فصل المهام، وعدم توافق أحكام المدقق مع أحكام الادارة.

2- دراسة (الخيرو 2002)بعنوان (واقع الأنظمة المحاسبية المنفذة بالحاسوب لبعض الوحدات الاقتصادية في العراق ومتطلبات تدقيقها)

يتمثل هدف البحث في الاسهام بتحسين مهنة المحاسبة ومراقبة الحسابات وتطويرهما وذلك من خلال دراسة المعوقات الحالية المتعلقة باستعمال الحاسوب (من قبل المحاسبين وتدقيق تلك الأنظمة بالحاسوب من قبل مراقبي الحسابات) في بيئة العراق وسبل تلافيها أو الحد منها لتتناسب مع متطلبات العصر الحالي والمستقبل على وجه التحديد وقد توصل الباحث إلى العديد من الاستنتاجات أهمها انه لابد لمراقبي الحسابات إن يأخذوا تطورات الحاسوب بالحسبان حيث يعرض ذلك كفاءة أعمال التدقيق إلى المخاطر، وكذلك ازدياد استعمال الحاسوب من قبل الوحدات الاقتصادية والمحاسبين بشكل اكبر من استعمال مراقبي الحسابات مما يمثل فجوة بينهما، وأيضا إن مهنه المحاسبة في عالم اليوم تعمل في بيئة معقدة ومتغيرة باستمرار ولغرض تحقيق النشاط المطلوب للمهنة فان على محاسب اليوم ومحاسب الغد العمل على تطوير معرفته لمواجهة التحديات الصعبة، التي تنتظره ومنها التمتع بمهارات استعمال الحاسوب لكي يواكب ما وصل إليه عالمنا اليوم .

3- دراسة (Bedard et al.,2003) بعنوان" عوامل خطر نظم المعلومات، وتقدير المخاطر، وقرارات تخطيط التدقيق".

ركزت الدراسة بصورة خاصة على خطر وجود ثغرات في أمن النظم، وخطر عدم كفاية المعلومات المقدمة من قِبل نظام المعلومات المحاسبي للوحدة الاقتصادية. بالاعتماد على المدققين الخارجيين لِعَيِّنة من زبائن فعليين.و توصلت الدراسة الى إرتباط عملية تحديد خطر عدم كفاية المعلومات مع نمط الإدارة، والجدارة Competence، والمحافظة على انتشار نظام المعلومات، وكفاية التوثيق.ويُصاحب تقديرات خطر عدم كفاية المعلومات عدد من العوامل في مقدمتها طبيعة نشاط الأعمال ودرجة تعقيده.و يعتمد المدققون (عينة الدراسة) على الاختبارات الرقابية لتقدير مخاطر أمن المعالجة الالكترونية للبيانات.

4- دراسة (ابو موسى 2006) بعنوان"مخاطر أمن نظم المعلومات المحاسبية الالكترونية – دراسة ميدانية في منشآت سعودية"

هدفت الدراسة الى معرفة وإختبار المخاطر الرئيسة والمهمة التي تهدد أمن نظم المعلومات المحاسبية الالكترونية في المنشآت السعودية و تَعَرَّضت الوحدات الاقتصادية عينة الدراسة الى خسائر مالية كبيرة بسبب إنتهاكات أمن نظم المعلومات المحوسبة من قِبل أفراد داخل وخارج المنشآت.ومن أهم المخاطر التي هددت أمن نظم المعلومات المحوسبة للوحدات الاقتصادية عينة البحث، الإدخال الخاطىء للبيانات عن قصد أو

غير قصد، فضلا عن التدمير غير المتعمد للبيانات من قِبل الأفراد العاملين.'والإستعمال المتكرر لنفس كلمات السر Passwords،و إدخال الفيروسات الى النظم المحوسبة،و تدمير مخرجات النظم المحوسبة.و كشف معلومات مهمة وسرية الى أفراد غير مُصَرّح لهم الاطلاع عليها.و توجيه بعض مخرجات الحاسوب الى أفراد غير مُصَرّح لهم تسلمها أو الإطلاع عليها.

5- دراسة (حسون2009)بعنوان (نظام الرقابة الداخلية في ظل التشغيل الالكتروني للبيانات المحاسبية وأداء مراقب الحسابات- بحث تطبيقي في شركة نفط الجنوب ش.ع

هدفت الدراسة إلى فحص نظام الرقابة الداخلية في ظل التشغيل الالكتروني، والى معرفة التحديات التي تواجه مراقب الحسابات عند فحصه لنظام الرقابة الداخلية في ظل التشغيل الالكتروني، فضلا عن التحديات، التي تواجهه لاستعمال طرائق التدقيق من خلال الحاسوب والتدقيق بوساطة الحاسوب، لكي يعزز الثقة بالقوائم المالية للشركة ومن أهم الاستنتاجات التي توصل لها الباحث ان إجراءات الرقابة العامة و إجراءات الرقابة على التطبيقات في ظل التشغيل الالكتروني في الشركة مقبولة، فضلا عن أن هناك قلة في إجراءات قسم التدقيق الداخلي على التشغيل الالكتروني في الشركة، وكذلك لا يمتلك مراقبي الحسابات مهارات الحاسوب اللازمة لغرض تقويم نظام الرقابة الداخلية في ظل التشغيل الالكتروني للتأهيل الحالي لمراقبي الحسابات بما يتناسب مع بيئة النظم المحاسبية

6- دراسة(فرج 2011)بعنوان دور المدقق في تقدير مخاطر التدقيق في ظل استعمال تقنية المعلومات بالتطبيق على مصرف الائتمان العراقي

هدفت الدراسة في تعميق البحث والتحليل في مجال إعتماد الوحدات الاقتصادية المعاصرة على تقنية المعلومات في أداء أنشطتها المتعددة وقد إنعكس ذلك على أنظمة معلوماتها والرقابات المرتبطة بها إذ مَرَّتْ بتغيرات مهمة خلال السنوات الأخيرة،

وقد أوجدت المعالجة الالكترونية للبيانات متغيرات وعوامل مؤثرة جديدة منها ما يتعلق بطبيعة مخاطر التحريفات المادية (مخاطر ارتكاب أخطاء وتزوير). فضلا عن احتمال حدوث مخاطر تُصَنَّفْ على أنها مخاطر ضمنية، ومخاطر رقابة، ومخاطر اكتشاف. إذ يتعين على المدقق أخذ هذه المخاطر في الحسبان عبر تحليلها ودراستها، وفهم العلاقة ما بين تقنية المعلومات المطبقة والمخاطر المؤثرة فيها. وبما يجنب تعرض المدقق إلى مساءلة قانونية تترتب عليها خسائر مباشرة متمثلة بتعويضات إلى متضررين وخسائر غير مباشر متمثلة بفقدان المدقق سمعته المهنية .

واستخدمت الباحثة انموذج من ستة مراحل يمر بها عمل مراقب الحسابات عند تحليل وتقدير مخاطر تقنية المعلومات لمصرف الإئتمان العراقي وبما يساهم بدورهِ في تقدير مخاطر التدقيق. وتوصلت الدراسة الى بعض النتائج منها تَكُون رقابات نظم تقنية المعلومات فعالة من منظور المدقق عندما تحافظ على تكامل المعلومات مع أمن البيانات التي تعالجها. ويتطلب الحصول على معلومات صحيحة، تَـوَفُر مجموعة متنوعة من رقابات تُنفذ لغرض فحص دقة وإكتمال، وتفويض الصلاحيات ذات الصلة بالمعاملات. وتُصنف الرقابات ذات الصلة بالمعالجة الالكترونية للبيانات إلى مجموعتين هما رقابات عامة، ورقابات تطبيقية .

ثالثا :الاطار العام للبحث

ابعاد مفهوم حوكمة تقنية المعلومات

تمثل الحوكمة كاصطلاح عام، توصيف أدوار لأشخاص مؤتمنين على الإشراف، وتوصيفا لما يُمارَس من رقابة وتوجيه في وحدة إقتصادية ما (علي: 2009: ص 680). يَكُون المُكَلَـفون بالحوكمة خاضعين للمساءلة الإعتيادية عن تحقيق أهداف الوحدة الاقتصادية، والإبلاغ المالي، وتقديم تقارير الى أطراف معنية بأنشطتها، (IFAC: 2008: p.147).

وينظر آخرون الى حوكمة الوحدة الاقتصادية باعتبارها بناء هيكلي Structure يخدم في مجال ضمان تسلم حملة الأسهم من الأقلية معلومات موثوقة عن قيمة الوحدة الإقتصادية، وبأن مدرائها وكبار حملة الأسهم فيها لا يُضَلِلونهم بشأن قيمة إستثماراتهم. و تحفيز المدراء على تعظيم قيمة الوحدة الاقتصادية بدلا من الإهتمام بأهدافهم الشخصية (Bushman and Smith: 2003: p.65).

أما حوكمة تقنية المعلومات، فقد عُـرِّفَت من قِبَل معهد حوكمة تقنية المعلومات على أنها مسؤولية تشتمل على القيادة، والهيكل التنظيمي، وعمليات المعالجة التي تَضْمَن تحقيق الوحدة الاقتصادية لأهدافها عن طريق إضافة قيمة أثناء تحقيق موازنة للخطر مقابل كل من عائد تقنية المعلومات، وعمليات المعالجة الخاصة بهذه التقنية. توفر حوكمة تقنية المعلومات هيكلاً يربط بين عمليات معالجة تقنية المعلومات، وموارد تقنية المعلومات، والمعلومات ذات الصلة بإستراتيجيات الوحدة الاقتصادية وأهدافها (ITGI: 2005: p.5).

ويوضح تعريف آخر حوكمة تقنية المعلومات بإعتبارها تحديد صلاحية صنع القرار وإطار المساءلة للتشجيع على سلوك مرغوب فيه لإستعمال تقنية المعلومات (Weill and Ross: 2004).

وينظر(Simonsson and Johnson: 2006: p.2) الى حوكمة تقنية المعلومات على أنها تمثل ترتيب إستراتيجي لتقنية المعلومات بما يتسق مع نشاط الأعمال وينتج عن ذلك أقصى قيمة لنشاط الأعمال من خلال تطوير وإدامة رقابة فعالة لتقنية المعلومات وتحقيق المساءلة، وإدارة الأداء، وإدارة المخاطر.

في ضوء ما ذكر آنفاً يرى الباحثان أن مجلس الادارة والمستويات العليا، والمدراء التنفيذيين مسؤولون عن ضمان استعمال الوحدة الاقتصادية عمليات معالجة تحقق انسجام نظم تقنية المعلومات مع استراتيجيات وأهداف الوحدة الاقتصادية.

ومنْ أجل تلبية إلتزامات الادارة التي تُعَد متجسدة ضمنيا في حوكمة تقنية المعلومات، ينبغي على الادارة التركيز على مجالات عديدة مهمة وكالآتي (Turner and Weickgenannt: 2009: p.21):

1. تحقيق إنسجام تقنية المعلومات مع استراتيجية الوحدة الاقتصادية.
2. جعل الاستراتيجية والأهداف تتجهان نزولاً نحو أهداف المستويات المختلفة في الوحدة الاقتصادية.
3. وضع هياكل تنظيمية للوحدة الاقتصادية ولوحداتها الفرعية التابعة بما يُسَهِّل تنفيذ الاستراتيجيات وتحقيق الأهداف.
4. تأكيد تَبَنِّي هيكل رقابة لتقنية المعلومات والعمل على تطبيقه.

تُعَد نظم تقنية المعلومات في بيئة الأعمال المعاصرة، من العوامل المهمة والحساسة لإنجاح الوحدات الاقتصادية التي توظف هذه التقنيات. إذ يُمكِن لنظم تقنية المعلومات تَحسين الكفاءة والفاعلية وتخفيض التكاليف. إن الوحدات الاقتصادية التي تفشل في الاستفادة المناسبة من المنافع الكامنة في نظم تقنية المعلومات، يمكن أن تفقد حصة سوقية لمصلحة المنافسين، فضلا عن احتمالات خروجها من نطاق التنافس. على هذا الأساس تصبح الوحدة الاقتصادية مطالبة بالتحري المستمر وتقويم ما متاح من إمكانات لإستعمال أحدث تقنية للمعلومات، وذلك سعياً لإختيار ما هو مناسب من نظم تقنية المعلومات لتنفيذ عملياتها وتحقيق أهدافها، فضلا عن العمل على اتخاذ قرارات بشأن مسائل من قبيل أية حزمة برمجيات من الأفضل شراؤها، وتوقيت التوسع في النظام المحاسبي للوحدة الاقتصادية. يُمكِن القول بأن إنجاز ذلك يمكن أن يتحقق من خلال الآتي (Turner and Weickgenannt: 2009: pp.204-205):

1. التقويم المستمر للمقابلة بين الأهداف الاستراتيجية ونظم تقنية معلومات الوحدة الاقتصادية.
2. معرفة التطورات في نظم تقنية المعلومات، التي يمكن أن ترفع قدرة الوصول للأهداف الاستراتيجية للوحدة.
3. ترتيب أولوية لإجراء تغييرات في نظم تقنية المعلومات المستخدمة.
4. وضع خطة لتطوير وتصميم التغييرات ذات الأولوية القصوى في تقنية المعلومات.
5. تنفيذ وإدامة نظم تقنية المعلومات.
6. العودة دائما إلى الخطوة الاولى (التقويم المستمر).

توجد مجموعة نقاط يتعين على الادارة أخذها في الحسبان عند اعتبار تقنية المعلومات عاملا حاسما في نجاح الوحدة الاقتصادية للأمد الطويل وهي كالآتي (ITGI: 2003: p.20):

1. توجيه أنشطة أعمال الوحدة الاقتصادية بطريقة تحقق تداخل وتواصل منسجم مع تقنية المعلومات.
2. تعيين وتوصيل الأهداف الاستراتيجية للوحدة الاقتصادية للأمد الطويل، إلى الأطراف ذات العلاقة.
3. العمل على ضمان الإلمام التام بأحدث تطورات تقنية المعلومات من منظور نشاط أعمال الوحدة الاقتصادية.
4. الحرص على مناقشة موضوع تقنية المعلومات باستمرار ضمن أجندة الادارة، والتعامل معه بطريقة بناءة.
5. تحديد مقدار وطريقة الاستثمار في تقنية المعلومات بالمقارنة مع استثمارات المنافسين.
6. تكوين رؤية واضحة عن الاستثمارات الرئيسة في تقنية المعلومات من منظور المخاطرة (مخاطر الأمن مثلا) ، والعائد (عائد في صورة وفورات كلفة ضد الاختراق الأمني) .
7. تسلم تقارير منتظمة حول تقدم العمل في مشاريع رئيسة لتقنية المعلومات.
8. تسلم تقارير أداء تقنية المعلومات بما توضح ما اضافته من قيمة للعمل.
9. توفير موارد مناسبة لتقنية المعلومات ، وبُناها التحتية والمهارات اللازمة للإيفاء بالأهداف الاستراتيجية المطلوبة.

من أجل ضمان دعم نظم تقنية المعلومات للأهداف الاستراتيجية طويلة الأمد والعمليات التشغيلية اليومية، فإن الادارة تكون مُلزمة بإجراء تقويم مستمر للأوضاع السائدة.

الحاجة الى حوكمة تقنية المعلومات

لتوضيح الحاجة الى حوكمة تقنية المعلومات في المنظمات سيتم التطرق الى بعض العناصر التي تشكل مبررات امام الادارة لتحقيق مستوى من السيطرة على تقنية المعلومات ، وتدفعها للتعامل مع موضوع امن المعلومات بصورة جدية (عقل ، 2011، 12-17) :

1. الاعتماد التام والمتزايد على نظم المعلومات والاتصال : ان اجراءات الاعمال في الغالب يدوية او شبه يدوية اي تستند على اجراءات ومهمات عمل تعتمد على التوثيق الورقي بكل ما فيه من محدودية وتعرف اجراءات الاعمال بانها الطريقة التي يتم فيها انتاج منتج او تقديم خدمة ، وهي الوصفة التي يتم فيها جمع المدخلات خلطها معا لانتاج المنتج سواء اكان وثيقة ام خدمة ، وبعد دخول تقنية المعلومات للمنظمات اصبح تمكين هذه الاجراءات آليا ويتم ذلك من خلال نظم معلوماتية تحتفظ بالمعلومات وتشاركها بين جميع الاطراف ومع ضبط تسلسل العمليات وتقنن الاجراءات على المعاملة وفقا للضوابط ، وتقنن ايضا استخدام السلطة الممنوحة للعاملين وفقا للوائح من خلال منح وحجب صلاحيات الاستخدام في الاجراءات الالية ، لكن هناك مخاطر من اساءة استخدام النظم المعلوماتية ، مما يستدعي ضرورة عزل المعلومات عن ايدي العابثين لتحقيق مستوى مقبول من الامن المعلوماتي وهذا ما يعبر عنه بالسلامة او النزاهة **Integrity** اي ان تكون المعلومات محمية ومصونة.
2. قيمة المعلومات الاستراتيجية : ان اي تقصير في توفير المعلومات او حدوث خلل في معالجة البيانات سيكون له اثر سلبي على سمعة المنظمة ، وسوف تتزعزع الثقة بقيادتها وفرقها الادارية لذا على القياديين الانتباه الى ضرورة التعامل مع المنظومة الالكترونية في المنظمة كأحد اهم الاصول الاستراتيجية وعليهم دعمها وتوفير مستلزماتها الفنية والبشرية والقيادية ، وإدراك اهمية استدامتها وحمايتها من المخاطر المختلفة.
3. تزايد قيمة الاستثمارات في التقنيات : نظرا لأهمية المعلومات للمنظمة ، فأنها تعمل على توفير متطلباتها الفنية والبشرية وهي بذلك تستثمر ميزانيات ضخمة ، وان هذه الاستثمارات تتعاظم يوما بعد يوم ، علية ينبغي حمايتها وتوفير سياسات واليات لإقرار ومراقبة هذه الاستثمارات ذات القيمة العالية ، مع وجود حاجة ملحة لتوفير اسس علمية وتطبيقية لدعم اتخاذ القرار وتفسير القيمة التي سوف تضيفها هذه الاستثمارات التقنية على اعمال المنظمة وكيف ستقوم بخدمة اهدافها الاستراتيجية.
4. الخسائر الناتجة عن توقف المنظومة المعلوماتية : ان توفر منظومة معلوماتية وجاهزيتها للخدمة في الاوقات المحددة وبالجودة المطلوبة يمكن ان نطلق عليه التوفر او الجاهزية **(Availability)** ، وان عدم توافر المنظومة المعلوماتية في الخدمة يتسبب بخسائر مادية ومعنوية للمنظمة ، ويقيس الخبراء الاثر المالي لتوقف المنظومة تقنية المعلومات على المنظمة من خلال استخدام الوسائل الاحصائية والمحاسبة الادارية في بناء انموذج للتكاليف والإيرادات في تقدير قيمة الاثار المترتبة على توقف هذه المنظومة.
5. فرص التجارة الالكترونية بأنواعها : ان تنامي حجم التجارة الالكترونية بمظاهرها المختلفة يتطلب توفير منظومة معلوماتية آمنة ، وذات فاعلية ، وكفاءة تنال ثقة المتعاملين وتحقق عائدا على الاستثمارات المستعملة بناء هذه المنظومة ، وهذا يساهم في تعزيز الميزة التنافسية للمنظمة ويقدم لها فرصة لتوسيع قاعدة العملاء والحصول على رضاهم وثقتهم.

ويرى الباحثان وجود اهمية كبيرة عند تحقيق اعلى درجات السيطرة على تقنية المعلومات وذلك لتوظيفها في خدمة المنظمة وبالتالي الحاجة الى تبني اطار عمل لتحقيق هذه السيطرة ، اذ يمكن استخدام اطار **COBIT** لتحقيق هذا الغرض.

وتركز حوكمة تقنية المعلومات على ثلاث رقابات مهمة هي البناء التنظيمي لتقنية المعلومات، وأمن تقنية المعلومات، وخطة مواجهة الكوارث **(Hall: 2007: p.275)**.

أولاً: البناء التنظيمي لتقنية المعلومات

يتضمن البناء التنظيمي لتقنية المعلومات، المواقع التنظيمية، والمسؤوليات ذات العلاقة وهي موضحة بالجدول (1). إذ يشتمل هذا البناء على خمس مواقع رئيسة ذات مسؤوليات عديدة، وهذه المواقع هي مدير تقنية المعلومات، وتطوير النظم الذي يشتمل على محللا للنظم ومبرمجا، وتشغيل تقنية المعلومات التي تشتمل على مشغل حاسوب وأمين مكتبة ومدير شبكة اتصالات، ورقابة البيانات التي تشتمل على فريق رقابة البيانات ومدير قاعدة البيانات، ومدير أمن المعلومات.

جدول (1)
المواقع التنظيمية للأفراد العاملين في تقنية المعلومات ومسؤولياتهم

الموقع التنظيمي لتقنية المعلومات	المسؤوليات المرتبطة بالموقع التنظيمي
مدير تقنية المعلومات	فحص كافة الرقابات، المصادقة على النظم، وضع خطط قصيرة وطويلة الأمد
تطوير النظم: تشتمل على	
• مُحلِل النظم	تقويم النظم الحالية، تصميم نظم جديدة، وضع خطط عامة للنظم، وضع مواصفات المبرمجين
• مبرمج	تصميم وتوثيق البرامج، تصميم وتطوير خرائط تدفق البيانات عبر الحاسوب
تشغيل تقنية المعلومات: تشتمل على	
• مشغل حاسوب	يشغل مكونات الحاسوب المادية، تنفيذ البرامج استنادا لتعليمات التشغيل
• أمين مكتبة تقنية المعلومات	إدامة توثيق النظم والبرامج والملفات التي بعهدته
• مدير شبكة الاتصالات	تخطيط وإدامة مواقع للشبكة ذات صلة بالوحدة الاقتصادية
رقابات البيانات: تشتمل على	
• فريق رقابة البيانات	رقابة تصاريح دخول المستخدمين، متابعة الدخول والرقابة على المعالجة والمخرجات
• مدير قاعدة البيانات	تصميم وتنظيم قاعدة البيانات، تحديد رقابات دخول واستعمال قاعدة البيانات
مدير أمن المعلومات	إدارة أمن نظم تقنية المعلومات بضمنها أمن كل من المكونات المادية والبرمجيات، ملاحظة الوصول للبرامج والبيانات ومتابعة حالات الاختراق الأمني

المصدر: Boynton et al.,: 2001: p.339.

ثانياً : أمن تقنية المعلومات

تتضمن الرقابات ذات الصلة بـأمن تقنية المعلومات الآتي:

1. **فصل ملائم بين الوظائف. تعمل الوحـدة الاقتصادية على الفصل بين الوظائف المختلفة في تقنية المعلومات بهدف منع تجميع أو دمج وظائف من قبيل المعالجة، ومنح التفويض، والتسجيل لدى شخص واحد فقط.و يبين الجدول (2) أمثلة لحالات الفصـل بين الوظائـف في مواقـع تقنية المعلومـات. إذ يُظـهِـر الجدول نوع الفصل الذي ينبغي مراعاته في المواقع التنظيمية والأسباب المقابلـة التي تـُبرر فصل الوظـائف.**

جدول (2)
أمثلة لأنواع الفصل بين المواقع التنظيمية للعاملين في تقنية المعلومات ومبررات الفصل

نوع الفصل في المواقع التنظيمية	أسباب الفصل بين وظائف المواقع التنظيمية
فصل وظيفة تطوير النظم عن المعالجة بالحاسوب	إن تأدية نفس الموظف للوظيفتين معا يوجد إحتمال لارتكاب تزوير يصعب إكتشافه لأن قدرة القائم بالتزوير على محو آثار التزوير تكون أوسع.
فصل وظيفة إدارة قاعدة البيانات عن الوظائف الأخرى لتقنية المعلومات	يكون مدير قاعدة البيانات مسؤولا عن عدد من الوظائف الحساسة متعلقة بأمن قاعدة البيانات، بضمن ذلك وضع مخطط لقاعدة البيانات، وتكوين رؤية عن مستخدم البيانات (ضمن مخططات فرعية)، والتصريح إلى مستخدمين بالوصول إلى بيانات، ومراقبة استعمال قاعدة البيانات، وتخطيط التوسعات المستقبلية. إن تفويض أداء هذه الوظائف وغيرها إلى أشخاص آخرين يؤدون وظائف غير توافقية، يهدد أمن قاعدة البيانات.
فصل وظيفة إدارة قاعدة البيانات عن مهام تطوير النظم	يعمل المبرمجون على ايجاد تطبيقات للوصول إلى قاعدة البيانات وتحديثها واسترجاع البيانات منها. لغرض الوصول إلى قاعدة البيانات، يحتاج كل من مدير قاعدة البيانات والمبرمج إلى إتفاق حول مواصفات وجداول (تمثل رؤية المستخدم للبيانات) بهدف جعل محتويات القاعدة متاحة للتطبيق أو متاحة للمستخدم المعني. يتطلب إنجاز هذه الوظائف مراجعة نظامية لاحتياجات المستخدم من البيانات فضلا عن مراجعة الجوانب الأمنية. إن تعيين مسؤولية التعرف على رؤية المستخدم إلى أفراد مسؤولين عن إعداد البرامج يمكن أن يُضعِف رقابات الوصول في نظم إدارة قاعدة البيانات.

المصدر: Hall: 2007: pp.276-277.

2. رقابات مادية على الوصول، وتتضمن هذه الآتي (Romney and Steinbart: 2003: p.237):
أ. وضع معدات الحاسوب في غرف يمكن إقفالها، وحصر الدخول إليها بالأفراد المصرح لهم.
ب. وجود مدخل واحد أو مدخلين كحد أقصى إلى مركز تقنية المعلومات، مع جعل المداخل قابلة للمراقبة والاقفال.
ج. تطبيق سياقات صحيحة لمطالبة المصرح لهم بدخول مركز تقنية المعلومات بهويات تعريفية (باج الأمن).
د. إلزام المراجعين بالتوقيع في سجل الدخول عند دخولهم ومغادرتهم مركز تقنية المعلومات، وكتابة وصف مختصر عنهم ضمن سياسات الأمن للوحدة الاقتصادية، ووضع باجات خاصة بهم ومرافقتهم للأماكن التي يقصدونها.
هـ. استعمال نظام الانذار الأمني للكشف عن أي دخول غير مصرح به إلى نظام تقنية المعلومات.
و. نصب أقفال على الحواسيب الشخصية وبقية أجهزة الحاسوب.
ز. تقييد الوصول من خارج الشبكة إلى البرامج والمعدات.
ح. وضع معدات ومكونات أخرى مهمة للنظام بعيدا عن أية مواد قابلة للإشتعال.
ط. نصب أجهزة الانذار ضد الحرائق، واستعمال وسائل إطفاء للحريق لا تدمر معدات الحاسوب.
3. رقابات على الوصول المنطقي للبيانات
ينبغي السماح للمستخدمين المصرح لهم فقط بالوصول إلى بيانات، مما يعني أدائهم لوظائف معينة مصرح لهم بها من قبيل القراءة، والنسخ، والإضافة، والحذف وغيرها. إذ من المهم حماية البيانات من الخارجيين بالنسبة للوحدة الاقتصادية، كأن تخترق شركة منافسة النظام وتتصفح البيانات.

ثالثاً: خطة مواجهة الكوارث

تهدف خطة مواجهة الكوارث إلى تخفيض الأضرار والتكاليف، فضلا عن وضع وسائل بديلة مؤقتة لمعالجة المعلومات، ولمواصلة العمل الاعتيادي بأسرع وقت ممكن، وتدريب العاملين على كيفية التعامل مع الظروف غير الاعتيادية (حالات من قبيل الحرب، أو الفيضان، أو الزلزال)، والاختبار الدوري المناسب لخطط الطوارىء، ومراجعة خطة التعافي من الكارثة (Williams et al.,: 1997: p.554). تشتمل خطة التعافي من الكارثة على الخطوات الآتية (Romney and Steinbart: 2003: p.257)، (Wilkinson et al.,: 2000: pp.329-331):
1. تحديد أولويات التعافي. بموجبها تُحَدَد التطبيقات والمكونات المادية والبرمجيات التي تضمن استمرار الوحدة الاقتصادية في العمل، أثناء وبعد إنتهاء الكارثة.
2. توفير غطاء تأميني للحصول على التمويل اللازم لإستبدال المعدات والبرمجيات المتضررة.
3. الاحتفاظ المستمر بملفات إحتياطية من البيانات والبرامج (ملفات دعم)، تُخَزّن في مواقع آمنة بعيدا عن المركز الرئيس للحاسوب، لإستعمالها إذا ما أصابت النظام أية كارثة.
4. تحديد موظف تنسيق يكون مسؤولا عن التطبيق المُنَسَق لخطة التعافي بكافة مراحلها. يحدد هذا الموظف مسؤوليات فريق العمل الذي تُناط به أنشطة مواجهة الكارثة والتعافي منها. يأخذ هذا الفريق على عاتقه إيجاد المواقع البديلة، وتحديد البرامج، والتسهيلات اللازمة لتوصيل البيانات واسترداد السجلات الحيوية.
5. الاحتفاظ بتسهيلات إضافية (منشآت ومعدات من حواسيب واتصالات)، كأن تُعقَد إتفاقات مع وحدات تمتلك تسهيلات متوافقة مع تلك التي تستعملها الوحدة. يتم بموجب هذه الاتفاقات استعمال تسهيلات الطرف الآخر في معالجة البيانات في حال حدوث كارثة ما. كبديل يمكن أيضا الحصول على تسهيلات عن طريق التعاقد مع متعهد يوفر مواقع طارئة لاستعمالها في حالة الكارثة أو الظروف غير الاعتيادية. يمكن للوحدة الاقتصادية أيضا إستعمال ما يُعرَف بالمواقع الساخنة والمواقع الباردة. يُمَثِل الموقع الساخن منشأة تُؤَهل لكي تفي بمتطلبات المُستَخدِم. أما الموقع البارد فإنه يوفر ما مطلوب لنصب الحواسيب وتجهيز الطاقة وتوفير أجهزة التكييف ضمن وقت قصير للحفاظ على استمرارية العمل (Haag et al.,: 2007: p.338).
6. فحص ومراجعة خطة التعافي دوريا فضلا عن اختبارها عن طريق محاكاة الكارثة.
7. التوثيق الكامل لخطة التعافي من الكارثة والاحتفاظ بنسخ عديدة منها في مواقع بديلة آمنة.

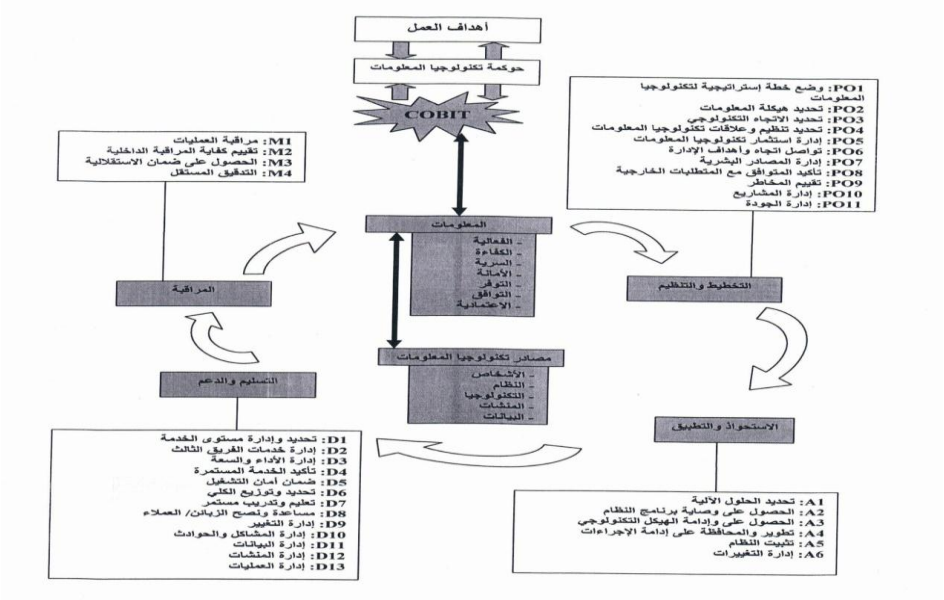
اطار COBIT لحوكمة تقنية المعلومات وتعزيز الرقابة الداخلية:

تم اصدار هذا الاطار من قبل جمعية تدقيق ورقابة نظم المعلومات (ISACA) في عام 1996 ، ثم قامت بتأسيس معهد حوكمة تقنية المعلومات في عام 1998 ، الذي اصدر النسخة الثانية منه في نفس العام ، ومن ثم النسخة الثالثة في عام 2000 ، والتي تعد نسخة متكاملة وشاملة ، ثم تم اصدار نسخة رابعة في

عام 2005 ، وأخيرا تم اصدار النسخة الخامسة في عام 2011 . يمتلك إطار COBIT أربعة وثلاثين هدفاً رقابيا ، ينبثق منها 215 هدفا فرعيا تتضمن ضوابط وممارسات تطبيقية مثلى ، وتمثل هذه الاهداف مجموعة من الضوابط المهمة لتحقيق الحوكمة . جُمِعَت هذه المعالجات ضمن أربع مجالات هي التخطيط والتنظيم ، والاستحواذ والتنفيذ ، والتوصيل والدعم ، والمتابعة ، ويقدم الاطار مؤشرات اداء ومنهجية للتقييم والمراجعة ، كما تتكامل الاهداف مع احتياجات المنظمة وأعمالها ، والشكل التالي يوضح هذا الاطار

شكل 1

اطار COBIT



المصدر (COBIT 4.1, 2007, 26)

مجالات تركيز حوكمة تقنية المعلومات (IT Governance Focus Areas)

اشار اطار COBIT الى وجود خمسة مجالات يتم التركيز عليها عند حوكمة تقنية المعلومات وهي (COBIT 4.1, 2007, 6):

1. **التوافق الاستراتيجي (Strategic Alignment): يركز على ضمان الربط بين المنظمة وخطط تقنية المعلومات ، وتحديد وادامة والتحقق من القيمة المقترحة (Proposition) والمواءمة بين عمليات تقنية المعلومات والعمليات التشغيلية للمنظمة.**
2. **الوصول الى القيمة (Value Delivary) : وتتمثل في تنفيذ القيمة المقترحة في كافة اجزاء دورة الايصال ، لضمان ايصال تقنية المعلومات للمنافع المنشودة من خلال الاستراتيجية ، مع التركيز على الاستفادة المثلى من التكاليف وتثبيت القيمة الاساسية لتقنية المعلومات.**
3. **ادارة الموارد (Resource Management) : وتتضمن الاستثمار الامثل في والادارة السليمة للموارد الهامة لتقنية المعلومات وهي التطبيقات ، المعلومات ، والبنى التحتية ، والبشر. وتتعلق القضايا الرئيسة بالاستفادة المثلى من المعرفة والبنى التحتية.**
4. **ادارة المخاطر (Risk Management) : وتتطلب التوعية بالمخاطر من قبل الاداريين البارزين في الشركة ، والفهم الواضح للمخاطر التي قد تتعرض لها المنظمة ، فهم متطلبات الامتثال والشفافية للمخاطر الهامة في المنظمة وتضمينها لمسؤوليات ادارة المخاطر في المنظمة.**
5. **قياس الاداء (Performance Measurement) : وتتضمن متابعة تنفيذ الاستراتيجية، واستكمال المشروع ، واستخدام الموارد، واداء العلمية وتقديم الخدمات، وذلك باستخدام، على سبيل المثال، بطاقات الأداء المتوازن والتي تترجم الاستراتيجية إلى اجراءات لتحقيق أهداف يمكن قياسها خارج المحاسبة التقليدية.**

وتتميز المنظومة المعلوماتية التي تتمتع بالحوكمة الخاضعة للسيطرة بمجموعة من المميزات وهي (عقل ، 2011 ، 18-19) :

1. **دعم اعمال المنظمة بما يزيد الارباح ويضبط النفقات.**
2. **بناء ميزة تنافسية مستمرة للمنظمة.**
3. **تسهيل تحقيق اهداف الادارة من استخدام تقنية المعلومات والاستثمار فيها.**
4. **توفير رابط قابل للقياس بين اهداف المنظمة وأهداف تقنية المعلومات والاتصالات فيها.**

5. فتح افآق جديدة للتوسع الافقي والعمودي للمنظمة.
6. حماية استثمارات المنظمة ونجاح مشاريع تقنية المعلومات ، والسيطرة على مخاطر تقنية المعلومات ، ودعم استمرارية الاعمال في جميع الظروف.
7. تنظيم نشاطات ومهمات فريق تقنية المعلومات في اطار اجرائي واضح ومتفق عليه.
8. قياس اداء تقنيات المعلومات والاتصالات والتعرف على اهم مناطق وفرص التحسين عبر الاستفادة من مصادر التقنية المختلفة.

معاييرجودة المعلومات

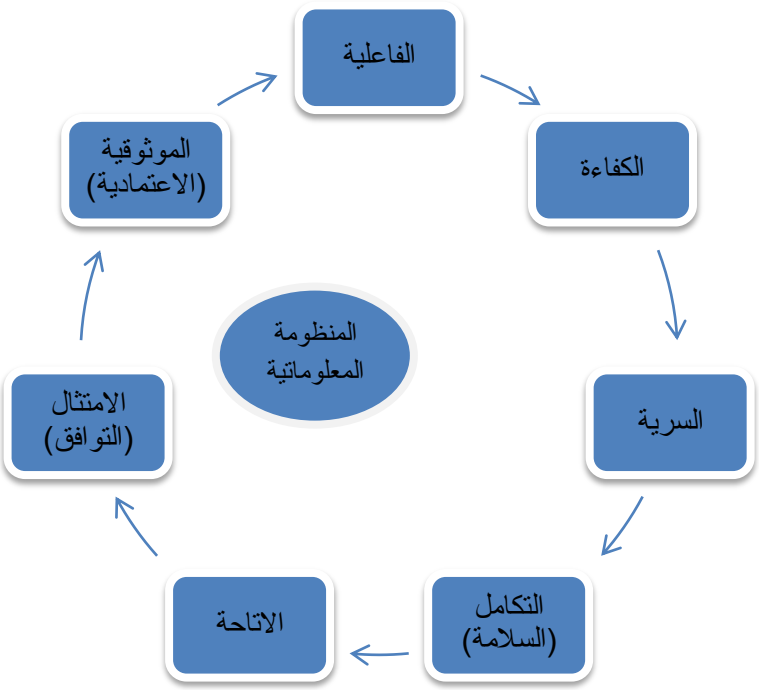
اشار إطار COBIT أن تحقيق اعمال المنظمة وحوكمة الأهداف يتطلب ضوابط كافية على موارد تقنية المعلومات لضمان تقديم معلومات للإدارة تلبي سبعة معايير رئيسية وهي (Marshal, stainbart, (2012,239) (COBIT 4.1, 2007,10):

1. الفاعلية (Effectiveness) : وهي القدرة على الاتيان بالفعل لإنتاج منتج ملموس او غير ملموس ، اما صفات المنظومة المعلوماتية ذات الفاعلية فتتلخص في قدرة المنظومة على توفير المعلومات التي تحتاجها المنظمة لتحقيق اهدافها الاستراتيجية والتشغيلية ، وان المعلومات يجب ان تكون ملائمة وان تقدم في الوقت المناسب.
2. الكفاءة (Efficiency): يتخذ هذا المفهوم بعدا اقتصاديا ، اذ ينبغي ان تحقق تقنية المعلومات الفاعلة جدوى اقتصادية للمنظمة ، من خلال تحقيق اعلى عائد على الاستثمار فيها ، وتقديم الخدمة ضمن مصاريف تشغيلية مقبولة تتناسب مع قدرة المنظمة واحتياجاتها ، وكذلك تتضمن حسن استغلال وتوظيف المصادر المادية والبشرية .
3. السرية (Confidentiality) : ويشمل التدابير اللازمة لمنع الاشخاص غير المصرح لهم على المعلومات الحساسة او السرية (عقل ، 2011 ،25) . وعلى المنظمة ادراك حساسية المعلومات وضرورة تبني مبدأ منح الحد الادنى من الصلاحيات للمستخدمين ، وان يكون الوصول للمعلومات مستندا الى حاجة المستخدم للمعلومات وفقا لمقتضيات وطبيعة عمله .
4. التكامل (السلامة) (Integrity) : ويتضمن هذا المفهوم جوانب متعددة منها ان المنظومة المعلوماتية تتمتع بمستوى من النزاهة والاستقلالية ، وتحافظ على صحة البيانات التي تجمعها وتحتويها ، وان لا تسمح بأي تعديل او اختراق سواء على مستوى النظم ام البنية التحتية ، وان يتمتع الفريق الفني بالنزاهة والاستقلالية ، وان يتم حفظ واسترجاع وتعديل وإلغاء البيانات من خلال الاطراف ذات الصلاحية بدون التجاوز على ذلك. كما يتضمن هذا المفهوم اكتمال المنظومة المعلوماتية وتماسكها ووحدتها ، وتقديم المعلومة الدقيقة في اي وقت ومن خلال اي قناة من قنوات الوصول للبيانات مما يمنحها موثوقية لدى الاطراف المستفيدة من المعلومات ويمنح المنظمة والأفراد العاملين فيها المصداقية فيما يقدمونه من معلومات ، وبخلاف ذلك تكون المنظومة المعلوماتية ضعيفة ولا يمكن الاعتماد عليها دون التحقق من المعلومة . ان تحقق هذا المعيار يحتاج الى تخطيط سليم وتنسيق تام من قبل القياديين والتنفيذيين والفنيين.
5. الاتاحة (Availability) : ويتضمن هذا المفهوم قدرة المنظومة المعلوماتية على توفير المعلومات لمن يحتاجها في الاوقات والأماكن المطلوبة وفقا لمصلحة العمل ، اي توفير المعلومات خلال ساعات العمل الرسمي او على مدار الساعة وبأقل قدر من الانقطاع في الخدمات ، فضلا عن قدرة الفرق التقنية على استعادة الجاهزية بعد حدوث الاعطال المفاجئة والناتجة عن اسباب متعددة منها الاعطال التقنية او سوء التشغيل او اهمال الفرق التقنية ، او الناتجة عن استنزاف الموارد التقنية وتحميلها بأكثر من طاقتها ، كما يمكن ان تنتج عن الحوادث الامنية والاختراقات ...الخ ، وعلى الادارة حصر ومجابهة هذه الاخطار بالحلول الرادعة والتخطيط السليم لاستمرارية الاعمال في المنظمة ، وتدريب العاملين على التعامل مع المواقف المختلفة المتوقع حدوثها.
6. الامتثال (التوافق) (Compliance): يأتي هذا المفهوم لاستكمال معايير جودة المعلومات وينبغي ان تتوافق هذه المعايير مع مجموعة من المعايير المؤسسية والنموذجية والتشريعية ، اذ ينبغي ان تتوافق المنظومة المعلوماتية اولا مع سياسات واستراتيجيات المنظمة ، مثل سياسات المشتريات والتوظيف ، والتوجهات الاستراتيجية التقنية ، فضلا عن التوافق مع النظم والتشريعات المقررة من الجهات الرسمية تجنبا لأية مساءلات او مخالفات قد تؤثر سلبا على المنظمة. ويرى الباحثان ان على المنظمة حصر اية متطلبات قائمة او مستجدة والسعي الى للتوافق معها لتحقيق الحوكمة في تقنية المعلومات.
7. الموثوقية (Reliability) : ويشمل هذا المفهوم تكامل اجزاء المنظومة المعلوماتية وتماسكها لتشكل قاعدة الاعمال في المنظمة بحيث يمكن الاعتماد عليها في اداء الاعمال اليومية والاعتماد علة مخرجاتها من بيانات وإحصائيات وتقارير لخدمة اعمالها التشغيلية والإستراتيجية ، ودعم اتخاذ القرارات

بالاعتماد على البيانات الكمية التي توفرها المنظومة المعلوماتية بعد ادخالها ومعالجتها وتقديمها في قوالب ، تخدم عمليات التخطيطي الاستراتيجي لأعمال المنظمة ، ومن ثم تصبح التقنية اداة فاعلة لدى المنظمة تسهم في تحقيق الميزة التنافسية المستمرة ، ومع تزايد الاعتماد على تقنية فان مفهوم الاعتمادية يمتد ليشمل قدرة المنظومة على التوسع والشمول للاحتياجات المتجددة لإدارات الاعمال ، والامتداد المتوازن افقيا وعموديا في البيانات والتطبيقات والتجهيزات والكوادر البشرية نتيجة لهذا التوسع الحتمي في نشاط المنظمة وبخلاف ذلك تصبح المنظومة المعلوماتية عائقا امام التوسع في اعمال المنظمة ونشاطاتها. والشكل التالي يوضح هذه المعايير.

شكل 2

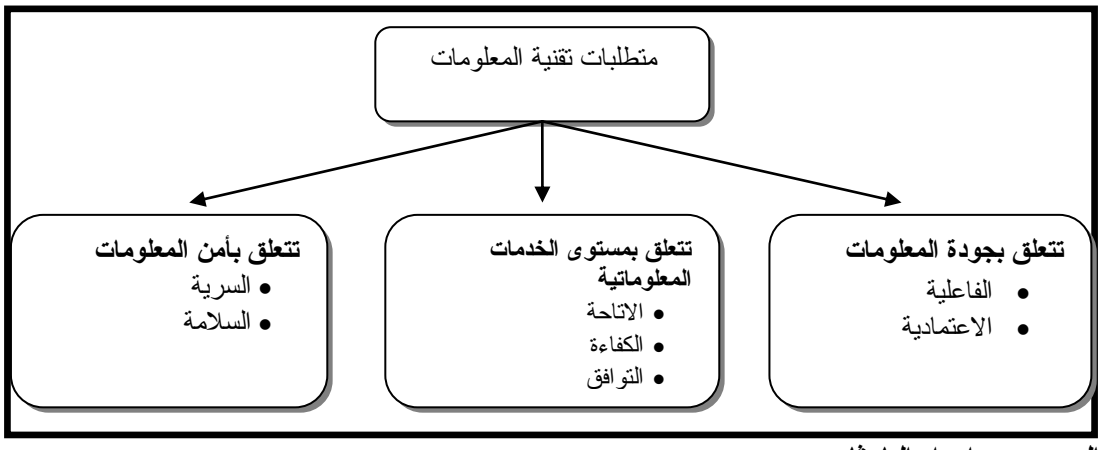
معايير جودة تقنية المعلومات



ويرى الباحثان ان هناك ثلاثة متطلبات اساسية بناءا على هذه المعايير السبعة وهي متطلبات تتعلق بجودة المعلومة اذ يمكن اعتبار (الكفاءة) كمعيار اساسي في هذا النطاق ، متطلبات تتعلق بمستوى الخدمة المعلوماتية ويمكن ان يدخل في هذه المتطلبات الاتاحة والاعتمادية والتوافق والفاعلية ، وأخيرا متطلبات تتعلق بأمن المعلومات ويمكن اعتبار السرية والسلامة .

شكل 3

متطلبات تقنية المعلومات



المصدر من اعداد الباحثان

عناصر المنظومة المعلوماتية

وفقا لإطار COBIT تتكون المنظومة المعلوماتية من اربعة عناصر وهي (COBIT 4.1, 2007, 12):

1. المعلومات Information .
2. التطبيقات Applications .
3. البنية التحتية Infrastructure .
4. الافراد (الناس) People .

أولا : المعلومات:

يقصد بالمعلومات مجموعة من البيانات المنظمة والمنسقة ، او هي بيانات تمت معالجتها ثم تطبيقها وتحليلها وتنظيمها وتلخيصها بشكل يسمح باستخدامها والاستفادة منها اذ اصبحت ذات معنى لمستخدميها ، وينبغي التفرقة بين المعلومات والبيانات من جهة والمعرفة من جهة اخرى ، فالبيانات هي مواد وحقائق اولية خام ليست ذات قيمة بشكلها الاولي ما لم تتحول الى معلومة مفهومة ومفيدة ، او هي مجموعة من الحقائق والمشاهدات قد تكون ارقاما او كلمات او رموز او حروف. ويمكن ان تجمع البيانات عن طريق الملاحظة او المشاهدة وتخزن بأسلوب معين ويمكن ان تعبر عن حقائق حالية او تاريخية او مستقبلية. اما المعرفة فهي عبارة عن معلومات تم تنظيمها ومعالجتها لتحويلها الى خبرة او معرفة مبتكرة لا تعرف عنها شئ من قبل ، او تصف شيئا يوسع من معارفنا السابقة او يعدل منها (الحسبان ، 2013، 37). ويرى الباحثان وجود علاقة بين المفاهيم الثلاثة اذ يتم تحويل البيانات بعد معالجتها الى معلومات ومن ثم تحويل المعلومات بعد تنظيمها ومعالجتها الى معرفة ، اي ان البيانات تعتبر مادة خام للمعلومات والمعلومات تعتبر مادة خام للمعرفة ، وتجدر الاشارة الى ان ما يعد معلومات الى شخص ما قد يعتبره شخصا اخر بيانات لا يمكن الاستفادة منها ، وفي هذا الصدد يرى الحسبان استخدام معيارين للتمييز بين البيانات والمعلومات اولهما درجة الاستفادة والثاني اجراء المعالجة (الحسبان ، مصدر سابق ، 38).

وفي عصر المعلومات اصبح لزاما على المنظمات توثيق ما لديها من معلومات ضمن قواعد بيانات منظمة وتحويل هذه المعلومات الى معارف ، وتسهيل الوصول اليها كي يتم الاستفادة منها ، وعلى الادارة تعزيز مفهوم ملكية البيانات لدى الادارات والعاملين في المنظمة ليدركوا مسؤولياتهم اتجاه البيانات التي يملكونها او التي تقع تحت ادارتهم وعليهم حصر وتصنيف البيانات للتمكن من حمايتها بمساعدة فرق تقنية المعلومات (عقل ، 2011 ، 45-46).

ثانيا : التطبيقات :

التطبيقات هي مجموعة من النظم الممكنة لإجراءات الاعمال وما يساندها من اجراءات يدوية شاملة وسياسات الاستخدام والتعليمات وإجراءات التشغيل ، وتتكون التطبيقات من حزم البرامج التي تتعامل مع قواعد البيانات حفظا واسترجاعا ، وقد يتم بناء هذه البرامج والنظم داخل المنظمة ضمن ما يعرف بالتطوير الداخلي ، او يتم توفيرها من خلال تركيب حزم البرامج الجاهزة وتوليفها لتتناسب مع احتياجات المنظمة ، او قد تكون البرامج مزيجا من النوعين لتأسيس منظومة من التطبيقات لإدارة اعمال المنظمة بصورة آلية.

وبقدر تعلق الامر بحوكمة تقنية المعلومات فان التطبيقات تكاد تكون اساس اعمال المنظمة المحوسبة وعلى القياديين الاهتمام بتوفير حزم البرامجيات المناسبة ، ودعم تطبيقها ، وتفعيل ما امكن من عمليات محوسبة وإجراءات الية توفرها هذه التطبيقات ، لان تكاليف توفير هذه التطبيقات للاستخدام تعد استثمارا من قبل المنظمة ، وإذا لم يتم استثمارها ستتحول هذه الاستثمارات الى نفقات غير ذات جدوى.(عقل ، 2011 ، ص47)

ثالثا : البنية التحتية :

تشكل البنية التحتية القاعدة الاساس التي تساهم في تقديم جميع الخدمات المعلومات والاتصالات ، اذ تشمل الخوادم (Servers) والمحطات الطرفية (Terminals) ، وأجهزة الحاسب الشخصية ، ووسائط حفظ البيانات ، كما تشمل البنية التحتية الشبكية احدى المكونات الرئيسة والتي تشمل مقسمات التبادل الرقمي ، وأجهزة الارسال والتوزيع الشبكي ، وما يرافقها من نظم لمراقبة وصيانة حركة المعلومات في الشبكة ، كما تشمل البنية التحتية اجهزة التزويد بالطاقة وأجهزة الامن والسلامة والحماية للمرافق المعلوماتية التي تحتوي مكونات البنية التحتية والعاملين على تشغيلها .

وتتطلب حوكمة تقنية المعلومات ضرورة سعي القياديين في المنظمة الى توفير البنية التحتية وبالقدرات والإمكانيات التي تحتاجها اعمال المنظمة وضرورة توفير متطلباتها التشغيلية من عناصر بشرية وتراخيص استخدام ، وذلك من اجل تأسيس بنية تحتية معلوماتية تخدم اعمال المنظمة وتحقيق استراتيجيتها.

رابعا : الافراد (البشر) :

يعد العنصر البشري محور العناصر المعلوماتية اذ ان التقنية وجدت لخدمته ويمكن تقسيم العنصر البشري حسب صلته بتقنية المعلومات الى ثلاث فئات وهي (عقل ، 2011 ، 48) :

1. **مالكو البيانات (Data Owners).**
2. **خادمو البيانات (Data Custodians).**
3. **مستخدمو البيانات (Data Users).**

يمارس في بعض الاحيان نفس الشخص اكثر من دور واحد ، وقد ينتمي لبعض الفئات عناصر بشرية من خارج المنظمة ، ويساعد هذا التقسيم على بناء هيكلية للمسؤولية المؤسسية عن حماية البيانات ، والأدوار القياسية التي ينبغي ان تناط بكل فئة من اجل تحقيق الامن المعلوماتي للمنظمة ، وان المتلقي الاساس للخدمات المعلوماتية هم اصحاب المصلحة بكافة فئاتهم وفي نفس الوقت يشكلون مصدرا مهما للمخاطر الامنية التي تهدد المنظومة المعلوماتية للمنظمة.

وفيما يخص حوكمة تقنية المعلومات ينبغي على المنظمة العناية بهذا الموضوع من خلال مجموعة من الامور على رأسها التعرف على البيانات الموجودة لديها وتصنيفها ومن ثمة تحديد مستويات السرية والإطلاع المسموح به وغير المسموح ، وظروف وسياسات الاحتفاظ بالبيانات ، اذ ان حماية البيانات تفرض على المنظمة تكاليف مختلفة ، كما ينبغي عدم الافراط في حماية البيانات غير المهمة ، كما ينبغي التوقف عن حماية البيانات بعد تقادم الزمن او اتلافها اذا تطلب الامر ذلك.

وعلى المنظمة التأكد نسبيا من نزاهة العاملين في خدمة البيانات من فنيين وفرق تشغيل ، سواء اكانوا موظفين لديها ام العاملين في مكاتب المقاولين الذين تم التعاقد معهم لتقديم الخدمات الفنية والتقنية ، وعلى المنظمة تبني سياسات وإجراءات للتوظيف والتعاقد مع العاملين والمقاولين تراعي المسائل الامنية مع ضرورة تثقيف العاملين وتأهيلهم للتعامل مع مسائل امن المعلومات وفقا للأدوار المنوطة بهم ، وتوضيح مهام فرق تقنية المعلومات ومهام الادارات ومالكو البيانات والمستفيدين منها ، ومراقبة صلاحيات الدخول للنظم دوريا وتخصيص آليات لمنح وحجب الصلاحيات بصورة فاعلة وآمنة. وعلى المنظمة عدم اهمال التعامل مع حوادث امن المعلومات ، واتخاذ الاجراءات الرادعة بحق مرتكبيها ، وتطوير قدراتها القانونية والحقوقية في هذا المجال.

مجالات الحوكمة ضمن اطار COBIT

تم التحدث عن المنظومة المعلوماتية ومكنوناتها الاربعة وتعرفنا على المعايير السبعة التي ينبغي ان تتميز بها المعلومات كي يتم اعتبارها معلومة جيدة والتي تكون بالكامل تحت سيطرة المنظمة لتحقيق الهدف من الاستثمار في تقنية المعلومات ، اذ تشكل معايير الجودة مؤشرات اداء استراتيجية للمنظومة المعلوماتية ، ولكي نتمكن من الارتقاء بمستوى هذه المؤشرات لابد من تنسيق ادوار اصحاب المصلحة ضمن مجالات وإجراءات محددة يقترحها اطار COBIT لتحقيق الحوكمة وهي اربعة مجالات (Hurt, 2010, p: 297):

1. **التخطيط والتنظيم Plan and Organize**
2. **الاستحواذ والتطبيق Acquisition and Implementation**
3. **التوصيل والدعم Delivery and Support**
4. **المراقبة والتطوير Monitoring and Evaluation**

جاءت تسمية اطار COBIT من الاحرف الاولى Control OBjectives for Information and Related Technologies والتي تعني الاهداف الرقابية للمعلومات والتقنيات المتعلقة بها ، والمقصود بالأهداف الرقابية (الهدف الرقابي) اي اجراء او ممارسة او هيكلية سواء اكانت يدوية ام الية يتم تصميمها وضبطها لتضمن بطريقة مقبولة تحقيق اهداف المنظمة ومنع وقوع اي احداث غير مرغوبة او يتم اكتشافها وتصحيحها عند حدوثها. (COBIT 4.1, 2007, p: 5)

المجال الاول : التخطيط والتنظيم:

يغطي هذا المجال إستراتيجيات وتكتيكات متعلقة بالتعرف على الطريقة التي يمكن أن تقدم من خلالها تقنية المعلومات ، أفضل مساهمة في إنجاز أهداف أنشطة الأعمال ، فضلا عن معرفة الرؤيا الاستراتيجية المطلوب تحقيقها وتوصيلها وإدارتها بالنسبة الى مختلف جوانب تقنية المعلومات. فضلا عن وضع التنظيم الصحيح والبنية التحتية لتقنية المعلومات في موضعها المناسب (فرج ، 2011 ، 116)، ويتضمن هذا المجال 10 هدفا وهي تهدف للمواءمة الاستراتيجية بين التقنية واعمال المنظمة من خلال وجود حد ادنى من التخطيط (قصير ، ومتوسط الاجل) ، وقيام المنظمة بتوفير الهياكل التنظيمية لجهاز التقنية ، والتواصل فيما يتعلق باستراتيجيات التقنية مع الادارات وشركاء الاعمال ، فضلا عن قيام المنظمة بتوفير

سياسات الموارد البشرية الخاصة بفريق تقنية المعلومات ، وسياسات الجودة الخاصة بالتقنية ، وسياسة امن المعلومات (عقل ، 2011 ، 59). ويتضمن هذا المجال الاهداف الاتية:

1. تحديد الخطة الاستراتيجية لتقنية المعلومات.
2. تحديد الهيكل الاساسي للمعلومات.
3. تحديد التوجهات التقنية.
4. تحديد وتنظيم عمليات تقنية المعلومات وعلاقاتها.
5. ادارة الاستثمار في تقنية المعلومات.
6. توصيل اهداف وتوجهات الادارة.
7. ادارة الموارد البشرية لتقنية المعلومات.
8. ادارة الجودة.
9. تقدير وادارة مخاطر تقنية المعلومات.
10. ادارة المشروعات.

المجال الثاني : الاستحواذ والتنفيذ:

لغرض تكوين رؤية إستراتيجية عن تقنية المعلومات ، فإن الأمر يتطلب معرفة الحلول التي تقدمها تقنية المعلومات ، وإمتلاكها وتطويرها ، وبما يجعل تنفيذها يتكامل ضمن عمليات المعالجة لأنشطة الأعمال. فضلا عن شمول تغييرات وإدامة النظم الحالية بهذه الرؤية للتأكد من إستمراريتها في تلبية الحلول الموضوعة لأهداف أنشطة الأعمال (فرج ، 2011، 117)، ويشمل هذا المجال تحقيق الحوكمة في مشاريع توريد وتطبيق الحلول التقنية وضبط العلاقات مع المقاولين ، تطوير واستبدال وصيانة النظم القائمة بنظم حديثة كما يشمل تكامل النظم مع اجراءات الاعمال ، وادارة التغيير المطلوب لتطبيق النظم على مستوى ادارات الاعمال والعمليات الخاصة بالتقنية (عقل ، 2011 ، 60) ويتضمن هذا المجال الاهداف الاتية :

1. تحديد الحلول المؤتمتة.
2. اقتناء وصيانة البرامج التطبيقية.
3. اقتناء وصيانة البنية التحتية.
4. تمكين عمليات التشغيل والاستخدام.
5. الحصول على موارد تقنية المعلومات.
6. ادارة التغيير.
7. تنصيب واعتماد الحلول والتغييرات.

المجال الثالث : التوصيل والدعم :

يُعنى هذا المجال بالتزويد الفعلي للخدمات المطلوبة ، والتي تتضمن خدمة التوصيل ، وإدارة أمن الخدمة واستمرارية توفيرها للمستخدمين ، وإدارة البيانات والمنشآت التشغيلية (فرج ، 2011، 117) ، ويشمل هذا المجال تحقيق الحوكمة اثناء تقديم الخدمات المعلوماتية ، سواء اكانت الخدمات ذات الصفة الفنية البحتة ، ام اللوجستية والمساندة للمستخدمين . ويشمل ادارة اتفاقيات الخدمات والمقاولين والعمليات الخاصة باستمرارية الخدمات المعلوماتية ، وإدارة الاعدادات (الترتيبات) Configuration المتعلقة بالمتغيرات الخاصة بالنظم والأجهزة لضبطها كي تعمل بالتناسق مع بعضها ، ويشمل تدريب العاملين وتطوير مهاراتهم ، ادارة المخاطر والأحداث الطارئة ، وإدارة الجودة ، وتحسين الاداء ، ويشمل هذا المجال 13 هدف وهي كالاتي:

1. تحديد وإدارة مستويات الخدمة.
2. ادارة خدمات الطرف الثالث (المقاولين ومقدمي الخدمات).
3. ادارة الاداء والطاقة الاستيعابية.
4. تأكيد استمرارية الخدمات.
5. تاكييد امن النظم.
6. تحديد وتخصيص التكاليف.
7. تاهيل وتدريب العاملين.
8. ادارية الخدمات الرئسية والاحداث الثانوية.
9. ادارة التهيئة (المواصفات).
10. ادارة المشاكل (المخاطر والاحداث الطارئة).
11. ادارة البيانات.
12. ادارة بيئة التجهيزات الفنية (المادية).
13. ادارة العمليات التشغيلية.

المجال الرابع : المتابعة والتقويم :

تتطلب جميع عمليات المعالجة بموجب تقنية المعلومات ، أن يتم الوصول لهذه التقنيات وفق سياقات منتظمة فيما يتعلق بجودتها وإمتثالها لمتطلبات الرقابة. ويتصدى مجال المتابعة والتقويم للجوانب المتعلقة بإدارة الأداء ، ومتابعة الرقابة الداخلية ، والإمتثال للتشريعات ، وتوفير الحوكمة (فرج ، 2011 ، 118) ، ولكي تتمكن المنظمة من الاستمرار بتحسين وتطوير مستوى الحوكمة ، تم تقديم مجموعة من الاهداف لبناء مؤشرات اداء تقيس مستوى تطبيق الحوكمة استنادا الى مفهوم بطاقة الاداء المتوازن وتتضمن هذه الاهداف تقييم مستوى الاجراءات التقنية وتحسينها ، وتنفيذ عمليات التدقيق الداخلي والخارجي دوريا لتأكيد التوافق مع المتطلبات والسياسات المختارة للتطبيق وتتضمن الاهداف الاتية :

1. متابعة وتقييم اداء تقنية المعلومات.
2. متابعة وتقييم الرقابة الداخلية.
3. تأكيد الالتزام بالمتطلبات الخارجية.
4. توفير حوكمة تقنية المعلومات.

رابعا :الانموذج المقترح

من خلال العرض السابق يمكن ترجمة تلك الاهداف الى اجراءات رقابة داخلية وفقا لمجالاتها الاربعة ويمكن ايضا ترجمة تلك الاجراءات الى اسئلة لفحص انشطة الرقابة الداخلية في الوحدات التي تستخدم التقنيات الحديثة في انظمتها :

التخطيط والتنظيم

1- وضع خطة سنوية تحدد احتياجات المشروع من الانظمة المؤتمته
2- ايجاد جهاز يتولى ادارة وتنظيم الانظمة المؤتمتة والتنسيق مع المستويات الادارية الاخرى
3- استخدام برامج التعليم المهني المستمر لتطوير العاملين على كل البرامج المستحدثة
4- وجود تعليمات محددة لاليات الاستثمار في استخدام وتطوير التقنية
5- قيام جهاز التدقيق الداخلي بمتابعة جودة الوحدات الادارية التي تستخدم التقنية الحديثة
6- وضع معايير لقياس الجودة
7- قيام جهاز التدقيق الداخلي بالمشاركة مع الجهات الفنية بتحليل المخاطر المرتبطة باستخدامات التقنية
8- التنسيق مع سياسات ادارة الموارد البشرية في رفد الاقسام بالمؤهلات المطلوبة
9- تحديد اجراءات تقسيم العمل للفصل بين الوظائف التي لها علاقة بتقنية المعلومات
10- تحديد خطوط الاتصال العمودي والافقي بين المستويات الادارية
11- تحديد صلاحيات محددة على عملية انشاء برامج جديدة او تعديلها
12- وجود فصل بين وظائف المبرمجين
13- وجود توصيف وظيفي لكل موظف يحدد واجباته ومسؤولياته
14- تحديد الضوابط لدخول الموظفين الى مواقع الاجهزة
15- التخطيط السريع والفعال للاستجابة إلى أزمات المعالجة الحاسوبية
16- تحديد دور الادارة تجاه الاستثمار،من خلال قياس المنافع، والمخاطر المصاحبة للمعالجة الحاسوبية للبيانات

الاستحواذ والتنفيذ

1- مشاركة الاقسام الفنية مع الادارة في وضع البدائل لاستخدامات التقنية
2- وضع بيئة ملائمة لحفظ البرامج من خلال استخدام اماكن مخصصة لهذا الغرض
3- توثيق برامج العمل
4- تحديد اجراءات تعديل البرامج والجهات المخولة والموافقات التي يتم الحصول عليها
5- وجود ابنية مناسبة ومكيفة تتلائم مع الاجهزة مثال ذلك مستوى الرطوبة، والحرارة، والماء، والطاقة الكهربائية، والتلوث، والمواد الكيمياوية)
6- الاحتفاظ بنسخ من البرامج الاساسية والمعدلة
7- وجود ضوابط بشان استخدام كلمة السر من قبل الموظفين
8- عدم نقل الاجهزة الى مكان اخر الا بموافقة الجهة المسؤولة
9- تحديد عملية استرجاع نسخ من البيانات الاصلية بالشخص المسؤول عنها حصريا
10-وجود سياسات تدريب وتطوير الموظفين
11- الفصل بين وظائف الجهات التي تتولى الشراء عن الجهات التي تحتفظ بالاجهزه
12-وجود دليل للاستخدام
13- الاحتفاظ بنسخ اضافية للبرامج ووسائل الادخال والاخراج والاحتفاظ بها في اماكن امينة خارج النظام
14- التأمين لحماية البرامج والملفات، وتقييد الوصول إلى سجلات وملفات الحاسوب.

التوصيل والدعم

1- مراجعة شكاوى المواطنين الخاصة بجودة الخدمات المقدمه وتحليل اسبابها
2- تقييم فاعلية الخدمات بشكل دوري
3- وضع خطة طوارئ لضمان استمرارية الخدمات
4- وجود ضوابط رقابية للوصول الى النماذج المهمة من التقارير
5- تحديد جهة تتولى عملية اتلاف الوثائق المهمة
6- ايجاد سياسات امنية من قبل ادارة المشروع
7- تحديد الجهات التي تتولى احتساب تكاليف ومنافع البدائل لاستحواذ او تبديل اوصيانة الاجهزة
8- وضع خطط مستقبلية بمجالات تطوير اعمال المشروع ومدى الحاجة الى تقنيات جديدة
9- دراسة الطاقة الاستيعابية للتقنية المستخدمة قبل الموافقة على استخدامات جديدة
10- ايجاد تغيير مستمر في الاجراءات الرقابية الموضوعة
11- تحديد تعليمات واضحة لتوزيع المخرجات
12- تحديث برامج اكتشاف الفيروسات بشكل يواكب التطورات بانواع المخاطر
13- تحديد إجراءات الادارة في الترقية، وتحفيز العاملين المسؤولين

المتابعة والتقويم

1- قيام جهاز التدقيق الداخلي بفحص انشطة الرقابة الداخلية
2- دراسة التشريعات واثرها على تعديل البرامج
3- الاطلاع على تجارب الاخرين في استخدام التقنية وامكانية الاستفادة منها في تطوير تقنية المشروع
4- ضرورة التشغيل الموازي للانظمة القديم مع الحديثة حتى يتم التاكد من نجاح الانظمة الجديدة
5- وجود صيانة مستمرة للاجهزة
6- تحليل الاخطاء المكتشفة ومعرفة اسبابها واجراءات تلافيها
7- تدريب الموظفين على الاحداث الطارئة والاجراءات التي يجب القيام بها
8- تحليل تقارير المدقق الخارجي ومتابعة حل ملاحظاته
9- التاكد من الدوران الوظيفي للوظائف المهمة والخطرة
10- فحص مستوى الحماية المتوفرة في الاجهزه والتعليمات للمحافظة على النزاهة، والسرية، والاتاحة للنظام وبياناته
11- دراسة بيئة عمل الشبكات والاتصالات واثرها على الانظمة المطبقة
12- دراسة وتقييم القرارات المتخذة من قِبـَل الادارة للتعامل مع المخاطر والاجراءات المتخذة لتلافيهـــا أو التخفيف من آثارها.

خامسا :الاستنتاجات والتوصيات

الاستنتاجات

1- يعتبر اطار COBIT اطار عالمي يوفر التوجيه بشان استخدام افضل الممارسات للتحكم في تقنية المعلومات.
2- يعتبر اطار COBIT اطار متكامل مع اطار لجنة COSO في توفير انشطة رقابة داخلية تقلل من مخاطر استخدام التقنية في انظمة المعلومات بشكل عام وانظمة المعلومات المحاسبية بشكل خاص .
3- ان تبني تقنية المعلومات في الوحدات الحكومية اصبح حاجة ملحة في سبيل التحسين المستمر في كفاءة اداء تلك الوحدات وتوجيه أنشطة أعمالها بما يحقق التواصل المنسجم مع التطورات العالمية.
4- يُعَبِر المفهوم العام لتقنيات المعلومات عن مجموعة عناصر تتفاعل فيما بينها من أجل أداء مهام محددة. وان تبني هذه التقنيات يتطلب توفير البيئة المناسبة لفهم المكونات المادية والبرمجيات و توفير موارد مناسبة لتقنية المعلومات، وبُناها التحتية والمهارات المطلوبة.
5- من الضروري ادراك الادارات بالاضافة الى منافع استعمال تقنية المعلومات ، الى المخاطر المرتبطة باعتماد هذه التقنيات. وتحليلها لكي تستطيع تصميم انشطة رقابة داخلية كفوءة .

التوصيات :

1- يمكن للمدقق الداخلي والخارجي الاستعانة باطار COBIT في تصميم قوائم الاستقصاء او اي وسيلة اخرى لفحص انشطة الرقابة الداخلية في ظل الاستخدامات التقنية .
2- من الضروري تدريب العاملين في الوحدات الاقتصادية على الاستخدامات الحديثة لتقنية المعلومات لمواكبة التطورات الحديثة وتحسين اداء تلك الوحدات .
3- من الضروري مساهمة اجهزة التدقيق الداخلي في تحليل مخاطر تقنية المعلومات بشكل دوري من اجل تعزيز انشطة الرقابة الداخلية مما يتطلب ضرورة تاهيلهم بشكل يتناسب مع تلك التقنيات .
4- من الضروري مساهمة نقابة المحاسبين والمدققين ومجلس الاشراف على مهنة مراقبة الحسابات والجامعات لوضع البرامج التدريبية العملية للمدققين باستخدامات الحاسوب
5- متابعة مكاتب التدقيق للاصدارات المحلية والدولية المرتبطة بتقنية المعلومات

المصادر:

المصادر العربية

1. الحسبان ، عطا الله احمد ، نظم المعلومات المحاسبية ، دار اليازوري ، 2013، عمان ، الاردن.
2. حسون علي صدام ،نظام الرقابة الداخلية في ظل التشغيل الالكتروني للبيانات المحاسبية واداء مراقب الحسابات،بحث تطبيقي في شركة نفط الجنوب مقدم إلى هيئة الأمناء في المعهدالعربي للمحاسبين القانونيين وهوجزء من متطلبات نيل شهادة ا لمحاسبة القانونية، 2009
3. الخيرو ، مقدام عصام يونس، واقع الأنظمة المحاسبية المنفذة بالحاسوب لبعض الوحدات الاقتصادية في العراق ومتطلبات تدقيقها، بحث مقدم إلى هيئة الأمناء في المعهد العربي للمحاسبين القانونيين وهو جزء من متطلبات الحصول على شهادة المحاسبة القانونية،2002م.
4. فرج ، سهاد صبيح ،دور المدقق في تقدير مخاطر التدقيق في ظل استعمال تقنية المعلومات بالتطبيق على مصرف الإئـتمـان العراقي اطروحة دكتوراه مقدمةإ لى مجلس كلية الإدارة والاقتصاد / جامعة بغداد 2011
5. علي، عبدالوهاب نصر، (2009)، موسوعة المراجعة الخارجية الحديثة وفقا لمعايير المراجعة العربية والدولية والأمريكية ، الدار الجامعية، (الجزء الخامس).
6. عقل ، محمد عقل ، مقدمة في حوكمة تقنية المعلومات باستخدام نموذج كوبت الاصدار الرابع 2007، المملكة العربية السعودية ، الطبعة الاولى ، 2011

المصادر الاجنبية

1. Austen, Lizabeth A., Aasmund Eilifsen, and William F. Messier Jr., (2000), "The Relationship of Risk Assessments and Information Technology to Detected Misstatements", www.ssrn.
2. Abu-Musa, Ahmad, (2006), "Investigating the Perceived Threats of Computerized Accounting Information Systems in Developing Countries: An Empirical Study on Saudi Organizations", Journal King Saud University-Computer & Information Science, Vol. 18, pp1-26
3. Bedard, Jean C., Cynthia Jackson, and Lynford Graham, (2003), "Information Systems Risk Factors, Risk Assessments, and Audit Planning Decisions", pp.1-29, www.ssrn.
4. Bushman, Robert M., and Abbie J. Smith, (2003), "Transparency, Financial Accounting Information, and Corporate Governance", Federal Reserve Bank of New York (FRBNY) Economic Policy review, (April), pp. 65-87
5. Boynton, William C., Raymond N. Johnson, and Walter G. Kell, (2001), Modern Auditing, John Wiley & Sons, Inc., (7th ed
6. Hall, James A., (2007), Accounting Information Systems, Thomson / South-western, (5th ed.).
7. Haag, Stephen, Maeve Cummings, and Amy Phillips, (2007), Management Information Systems for the Information Age, McGraw-Hill/Irwin Inc., (6th ed).
8. Hurt, Robart L. ,2010, Accounting Information System Basic Concepts and Current Issues, McGraw-Hill Irwin.
9. Information Technology Governance Institute (ITGI), (2005), Control Objectives, Released by the COBIT Steering Committee and the IT Governance Institute.
10. IT Governance Institute (ITGI), (2003), "Board Briefing on IT Governance", www.itgi.org
11. IT Governance Institute (ITGI), (2007), Executive Summary COBIT 4.1, www.itgi.org.
12. International Federation of Accountants (IFAC), (2008), Handbook of International Auditing, Assurance, and Ethics Pronouncements,
13. IFAC International Publications. Weill, P., and Ross J. W., (2004), IT Governance-How Top Performers Manage IT Decision Rights for Superior Results, Harvard Business School Press.
14. Romney, Marshall B., and Paul John Steinbart, (2003) , Accounting Information Systems, Prentice – Hall, Inc., (9th ed)
15. Romney, Marshall B., and Paul John Steinbart, (2012) , Accounting Information Systems, Prentice – Hall, Inc., (12th ed)
16. Turner, Leslie, and Weickgenannt Andrea, (2009), Accounting Information Systems: Control and Processes, John Wiley & Sons, Inc.
17. Webb, P., Pollard, C., and Ridley G., (2006), "Attempting to Define IT Governance: Wisdom or Folly", Proceedings of the 39th Hawaii International Conference on System Sciences.
18. Wilkinson, Joseph W., Michael J. Cerullo, Vasant Raval, and Bernard Wong-On-Wing, (2000), Accounting Information Systems, John Wiley & Sons, Inc., (4th ed.).

.....

.....

.....