وزارة التعليم العالي والبحث العلمي
الجامعة التقنية الوسطى
الكلية التقنية الإدارية – بغداد

وقائع المؤتمر العلمي التخصصي الرابع

للكلية التقنية الإدارية – بغداد

للمدة من

2018 / 11/ 29 -28

تحت شعار

الإبداع الإداري لتحقيق الرؤية المستقبلية

لمنظمات الأعمال

المجلد الاول / رقم الايداع (641)

البحوث المنشورة محكمة

الفهرست
المجلد الأول

المحور الإداري			
ت	عنوان البحث	اسم الباحث	الصفحة
1	تسويق الذات للكوادر الطبية من منظور لغة الجسد ودوره في تعجيل شفاء الزبون/دراسة استطلاعية لعينة من المنظمات الصحية في محافظة النجف الاشرف للفترة من 2010-2019	أ. د. مؤيد عبد الحسين الفضل أ.م. اقبال غني محمد	2-24
2	السلوك الاستراتيجي للمديرين وانعكاساته على براعة المنظمات / بحث تحليلي لآراء عينة من القيادات الادارية في معمل سمنت السماوة	أ. د. صالح عبد الرضا رشيد م. م. علي عبد الرزاق لفتة	25-55
3	اثر مرونة الموارد البشرية في تحقيق الريادة الاستراتيجية للمنظمات/بحث استطلاعي في جامعة ذي قار	م. م. طارق كاظم شلاكه أ. م. د. واثق حياوي لايذ م. م. رضوان جبار جودة	56-75
4	اثر التوجه الريادي لدى مدراء شركات التأمين في تحقيق الميزة التنافسية/دراسة حالة في شركة التأمين الوطنية	م. م. مروة جمال عمر السيد علي فوزي موسى	76-91
5	الإستراتيجية الممتدة نحو طموحات الطاقة البديلة في العراق/دراسة استطلاعية في ثلاثة مؤسسات ذات العلاقة بالطاقة بمحافظة البصرة	أ. م. د. هاني فاضل الشاوي	92-135
6	الانتاج النظيف واثره في اداء الاعمال/دراسة ميدانية في الشركة العامة للصناعات النسيجية والجلدية	م.م. جهان سلمان علاوي	136-157
7	قدرة امن المعلومات للنظام ERP في الحفاظ على العمليات الادارية/دراسة حالة في شركة الحكماء لصناعة الادوية والمستلزمات الطبية-نينوى	أ. د. محفوظ حمدون الصواف م. د. علي عبد الفتاح الشاهر	158-183
8	تحسين اداء العمليات وفق نظرية القيود / دراسة ميدانية في الشركة العامة للصناعات القطنية	م.م رؤى علي عبد السادة	184-204
9	مدى فاعلية تطبيق انموذج ادارة تجربة الزبون في شركات الاتصال العراقية/دراسة مقارنة لآراء عينة من العاملين في شركتي اسيا سيل وزين العراق	م. دنيا كريم حسن م. اميرة هاتف حداوي	205-231
10	ادارة المعرفة ودورها في تحقيق الاداء المتميز/بحث استطلاعي في شركة بغداد للمشروبات الغازية	م. م. نـدى ابراهيم نجم	232-258

قدرة أمن المعلومات لنظام ERP في الحفاظ على العمليات الإدارية
دراسة حالة شركة الحكماء لصناعة الادوية والمستلزمات الطبية/ نينوى

أ. د. محفوظ حمدون الصواف
قسم إدارة الاعمال
كلية الإدارة والاقتصاد – جامعة نوروز

م. د. علي عبد الفتاح الشاهر
قسم نظم المعلومات الادارية
كلية الادارة والاقتصاد–جامعة الموصل

المستخلص

يحظى موضوع نظام ERP باهتمام كبير من مختلف المنظمات في الدول المتقدمة والنامية على حد سواء، وذلك لأهميته في مجال تقديم المعلومات إلى كل الأقسام في المنظمة، وعليه يهدف هذا البحث إلى التعرف على قدرة أمن المعلومات لنظام ERP للحفاظ على العمليات الإدارية في شركة الحكماء لصناعة الأدوية والمستلزمات الطبية/ نينوى. وتم اعتماد منهج دراسة الحالة لأجراء البحث، وباستخدام المقابلات والمشاهدات والزيارات الميدانية المتعددة، للوقوف على واقع أمن المعلومات لنظام ERP ، فضلاً عن استخدام قائمة الفحص كأداةٍ لجمع البيانات والمعلومات.

وقد خرجت الدراسة بمجموعة من الاستنتاجات أهمها أن أمن المعلومات لنظام ERP يسهم بشكل كبير في الحفاظ على العمليات الإدارية في الشركة المبحوثة، وذلك بسبب الالتزام بالمعايير والقوانين الخاصة بأمن المعلومات ووفق المواصفات العالمية.

وقدمت الدراسة مجموعة من التوصيات منسجمة مع الاستنتاجات أهمها توسيع الاعتماد على أمن المعلومات للنظم الالكترونية، ومعالجة الضعف في البنية التقنية، فضلاً عن استخدام تنفيذ القوانين الخاصة بالعقوبات الناتجة عن الاخلال في إيصال المعلومات وتبادل الوثائق بين الشركة والجهات ذات العلاقة بها، فضلا عن مجموعة من الدراسات المقترحة للباحثين.

الكلمات المفتاحية: أمن معلومات ERP، نظام تخطيط موارد المنظمة

Abstract

The ERP system is highly regarded by various organizations in both developed and developing countries for its importance in providing information to all departments in the organization. The aim of this research is to identify the information security capability of ERP system to maintain the administrative processes of Al-Hukmaa for the pharmaceutical industry And medical supplies / Nineveh. The case study methodology was used to

conduct the research, using interviews, observations and multiple field visits, to identify the information security reality of ERP system, as well as using the checklist as a tool for collecting data and information.

The study concluded with a set of conclusions, the most important of which is that the information security of ERP system contributes significantly to the maintenance of the management processes in the firm investigated, because of compliance with the standards and laws for information security and in accordance with international standards.

The study presented a set of recommendations in line with the conclusions, the most important of which is the expansion of the reliance on information security for electronic systems, the treatment of weakness in the technical structure, and the implementation of laws on penalties resulting from disruption of information exchange and exchange of documents between the company and related parties, As well as a set of proposed studies for researchers.

Keywords: ERP Information Security, ERP

المقدمة

لعل واحدة من أهم الحقائق المتفق عليها في أدبيات نظم المعلومات، أن تقانة المعلومات أصبحت المحرك الأساس في تطوير العمليات الادارية. وأن تبنّي تقانة جديدة دائماً ما يقود إلى نوع جديد من العمليات التي ترتبط هي الأخرى بتقديم منتج جديد غالبا ما يكون على درجة عالية من التمايز والتغاير، الأمر الذي يمكِّن من الدخول إلى أسواق جديدة وصولاً الى توسيع رقعة الحصة السوقية على النحو الذي يؤدي الى تحقيق الأداء العالي.

من ناحية أخرى، إن مثل هذا الترابط ما كان ليتحقق لولا تكامل نظم معلومات منظمات الأعمال داخلياً وخارجياً. ويتمثل التكامل الداخلي في ربط نظم المعلومات الوظيفية على المستويين التشغيلي والاستراتيجي. أما التكامل الخارجي فيتأتى من ربط نظم معلومات منظمة الأعمال مع نظم معلومات شركاء الأعمال (سواء المجهزين، والموردين، والمصنعيّن، والداعمين اللوجستيين). أما على المستوى التنظيمي، فلقد أدى تكامل نظم المعلومات داخلياً وخارجياً إلى تأسيس نوع جديد من منظمات الأعمال غالبا ما تعنون في أدبيات نظم المعلومات بكونها "منظمات الأعمال الممتدة.

وفي هذا الخصوص يندرج نظام (ERP: Enterprise Resource Planning) ضمن مجموعة نظم المعلومات التي تعمل على تحقيق التكامل العملياتي والمعاملاتي من خلال تكامل كل أوجه نشاطات المنظمة وسماتها كلها داخل قاعدة بيانات مركزية مع قدرته على التكيّف لتتلاءم مع احتياجات الشركة المتعددة والمتنوعة. إذ يعمل نظام ERP على تحقيق الربط والتكامل من خلال توفير آلية تشارك في استخدام منظومة المعلومات المتاحة (بغض النظر عن المجال الوظيفي) من ناحية وآلية تحديث لهذه المعلومات مصحوبة بعرض يوفر خصائص التوقيت والدقة من ناحية

أخرى. فضلاً عن الدعم الذي يوفره على المستوى الاستراتيجي من خلال مستودع البيانات، وكل ذلك يمكن تحقيقه من خلال الامنية المتميزة للمعلومات المقدمة من انظمة المعلومات.

وعليه جاءت الدراسة في أهميتها لكي تتجه نحو دراسة امن المعلومات لنظام ERP على النحو الذي يسهم في الحفاظ على العمليات الادارية.

وتم اختيار شركة الحكماء لصناعة الادوية في محافظة نينوى كميدان للتطبيق، وسيتم توضيح تفاصيل البحث من خلال المحاور الاتية:

الأول: اختص بمنهجية البحث (مشكلته، أهميته وأهدافه، ومنهجه وتقاناته).

الثاني: أشتمل على الإطار النظري للبحث، وأفصح عن وجهة نظر الباحثان حيال موضوعه (أمن المعلومات لنظام ERP) التي أعدوها بعد استعراضهم لآراء الكتاب بخصوصهما.

الثالث: ركز على الإطار الميداني على تشخيص اطار امن المعلومات لنظام ERP وتحليلها.

الرابع: وضم استنتاجات البحث ومقترحاته.

المحور الأول / منهجية البحث

أولاً: مشكلة البحث.

تسعى المنظمات دائماً الى تحسين والمحافظة على عملياتها الادارية من خلال تزويد المستفيدين بالمعلومات المطلوبة عبر تنفيذ نظم المعلومات تتصف بالتكامل ولعل منها نظام ERP. ومن خلال استطلاع اولي قام به الباحثان لشركة الحكماء والمقابلات التي أجريت وجد امتلاك شركة الحكماء لنظام معلومات ERP محوسب يسهم في توفير المعلومات عن العمليات الإدارية في الشركة للمستفيدين. مما حفز الباحثان نحو دراسة أمن المعلومات لنظام ERP. وبشكل عام يمكن تناول المعضلة البحثية من خلال عدد من التساؤلات على النحو الآتي:

1. هل يمتلك نظام ERP في شركة الحكماء الحماية الأمنية اللازمة للحفاظ على المعلومات؟

ثانياً: أهمية الدراسة

تظهر أهمية الدراسة على النحو الآتي:

1. اكتسابها أهمية بالغة في البيئة العراقية لحاجتها الملحة في إبراز دور تقانة المعلومات في حل الاختناقات والارتباكات في العمل والناتجة عن عدم مواكبة التطور، وصعوبة التكامل بين الكم المعلوماتي الهائل بغية منافسة المنظمات الأخرى، فضلاً عن قدرتها على اكتساح المنظمات المحلية الممارسة للأنظمة التقليدية غير القادرة على مواكبة التطور والسرعة في خدمة الزبائن.
2. يعد موضوع أمن المعلومات ذا أهمية كبيرة لما لها من أثر بالغ في نجاح تنفيذ نظام ERP، وبالتالي الحفاظ على ديمومة العمليات الادارية
3. تعد الدراسة واحدة من الدراسات التي تبنت التوجهات المهمة في علوم نظم المعلومات، والتي اشارت اليها البحوث العلمية المنشورة بضرورة تشخيص الجزء الأمني لنظام ERP والتحقق من

مدى فاعليته في دعم العمليات الإدارية للشركة عبر المعلومات الامينة والموثوق بها والمقدمة للمستفيدين.

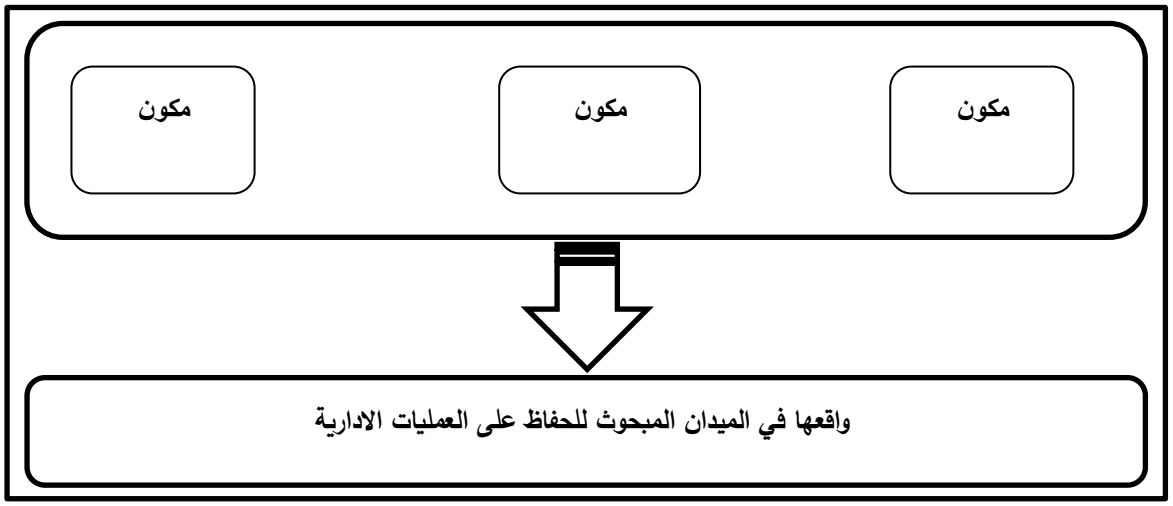
ثالثاً: أهداف الدراسة

اتساقاً مع أهمية الدراسة تتلخص أهداف الدراسة بالآتي:

1. تشخيص وتحديد اطار امن المعلومات لنظام ERP وبيان أهميته لنظام ERP في المنظمة المبحوثة.
2. تقديم نتائج واستنتاجات مبنية على الوقائع الفعلية فضلاً عن المقترحات اللازمة بهذا الخصوص.

رابعاً: المخطط الفرضي للبحث

لأجل معالجة مشكلة البحث وتحقيق أهدافه اعتمد الباحثان مخططاً فرضياً يعكس تحليل أمن المعلومات لنظام ERP وكالاتي:



الشكل (1) المخطط الفرضي للبحث

المصدر: اعداد الباحثان

خامساً: حدود البحث المكانية

عدّت شركة الحكماء بوصفها حدوده المكانية.

سادساً: منهج الدراسة واساليب جمع البيانات وتقاناته وحساب ثبات اداة القياس ومجتمع البحث

تحدد نطاق الدراسة في الجانب العملي بالمنهج الوصفي التحليلي لكونه من مناهج البحث التي تمتاز بالتحليل الشامل والتفصيلي للمشكلة أو الظاهرة قيد البحث، إذ انه يؤكد الموضوعية والابتعاد عن الذات في اختبار الحالة في مجتمع محدد مكاناً وزماناً وموضوعاً، فضلاً عن تعدد سماته من حيث إمكانية الجمع بين أكثر من أسلوب بحثي في آن واحد (Creswell, 2009, 65)، فهو قد يجمع بين الملاحظة، والاستفسار، واستمارة الاستبيان **(انظر الملحق 1)**، والمقابلات الشخصية التي

تؤدي إلى الوصول المباشر إلى المعلومات على نحوٍ مباشر وبأقل مستوى ممكن من التحيز، ويوضح الجدول (1) فقرات الاستبانة والمقياس العلمي المعتمد او مصدر كل فقرة. بينما اعتمد الجانب الأكاديمي من الدراسة على ما متوفر من المراجع والأدبيات الأجنبية من كتب ودوريات ودراسات ولاسيما الحديثة منها، فضلاً عن التصفح في شبكة الانترنت، وكذلك المراسلات عبر البريد الالكتروني لمتابعة آخر المستجدات العلمية ذات العلاقة وبالشكل الذي يسهم في إغناء موضوع الدراسة.

الجدول (1) مصادر بناء الاستبانة

متغيرات البحث	المصادر المعتمدة
البيانات العامة	الباحث
أمن المعلومات لنظام ERP	Chetty, Jacqui & Coetzee, Marijke , 2009; Onieva, J., Zhou, J. & Lopez J., 2008; Tuttle, Brad & Vandervelde, Scott D., 2007; Labuschagne L. & Marnewick C., 2006; Zhen W. & Xin-yu Z., 2007; Aksoy Nejat, 2005; Steel, Cater A. & Tan, Wui-Gee, 2005; Von Solms, Basie, 2005; Vroom, Cheryl & von Solms, Rossouw, 2004; Ridley, Gail, Young, Judy & Carroll, Peter, 2004.

أما فيما يخص تقانات التحليل الاحصائي، فتم الاعتماد على المعادلات الخاصة بقائمة الفحص والمبينة في الجانب الميداني

أما بخصوص معامل ثبات الفا (89%) ما يدل على ان درجة الاتساق الداخلي لإجابات المبحوثين عالية جداً، لأنها اكبر من (60%).

وفيما يتعلق بمجتمع البحث، فتمثل بجميع المدراء في شركة الحكماء، والبالغ عددهم (17) مديراً.

المحور الأول / منهجية البحث

أمن المعلومات نظام ERP

تعد المعلومات واحدة من الموجودات المهمة في المنظمة، لذلك ينبغي للمعلومات القيمة أن تكون محمية بشكل مناسب، كما أن توفر المعلومات مهم للمنظمة، لكن ما الجدوى من هذه المعلومات إذا لم تكن في إطار أمني، فضلاً عن أن بعض المعلومات ينبغي أن تكون سرية فلا يمكن لأي شخص الوصول إليها. ومع ظهور تقانة المعلومات تطورت ادوار المستفيدين في نظم المعلومات من متخصصي تقانة المعلومات لتسهيل الوصول إلى المعلومات، إلى غير موظفي تقانة المعلومات لعمليات المنظمة، والى الأفراد غير المحددين من الخارج (Marnewick, 2008, 70 - 71).

أشار Posthumus & Von Solms إلى أن أمن المعلومات ينظر إليه على انه مسألة تقنية ومن ثم يبدو عدم اهتمام الإدارة العليا به، لكن في الحقيقة أن أمن المعلومات يعد أكثر من مجرد مسألة تقنية، بل ينبغي أن يكون ذا مصدر قلق استراتيجي (Marnewick, 2008, 71).

وللتغلب على قضية أمن المعلومات يجب أن يحضى بتركيز ودعم استراتيجيات الأعمال في المنظمة، فضلاً عن أنه يمكن القيام بذلك من خلال حوكمة المنظمات التي تملي الطريقة التي يتم بها حماية المعلومات ضد الوصول غير المشروع، فحوكمة امن المعلومات هي مجموعة فرعية من حوكمة المنظمات والتي تتعلق بأمن نظم المعلومات (Entrust, 2004, 2).

عليه، فأمن المعلومات من:

- الناحية الأكاديمية: هو ذلك العلم الذي يبحث في نظريات واستراتيجيات توفير الحماية للمعلومات من المخاطر التي تهددها ومن أنشطة الاعتداء عليها (Force, 2010, 10-20).
- الناحية التقنية: الوسائل والأدوات والإجراءات اللازم توفيرها لضمان حماية المعلومات من المخاطر الداخلية والخارجية (Martin, 2003, 3-6).
- الناحية القانونية: هو محل دراسات وتدابير حماية سرية وسلامة محتوى وتوفر المعلومات ومكافحة أنشطة الاعتداء عليها (Barker, 2003, 15).

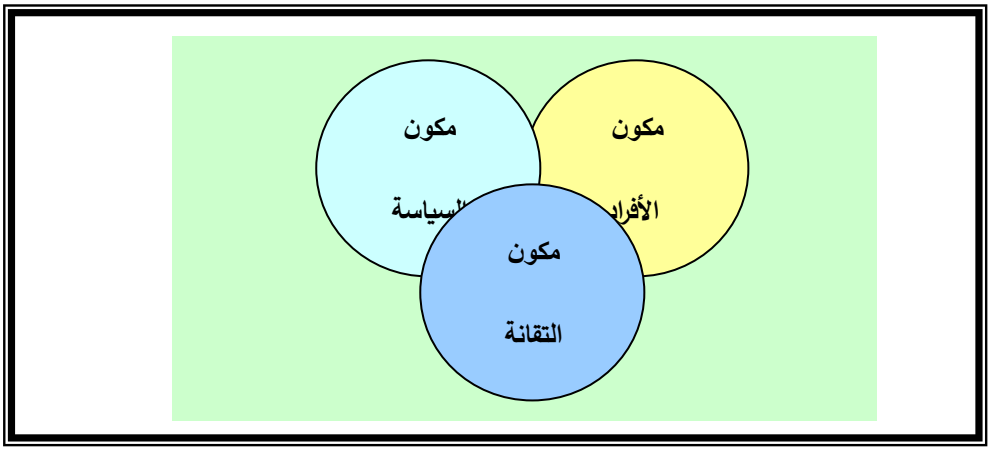
أما بخصوص امن المعلومات في إطار نظام ERP فهو مصدر قلق للعديد من المنظمات، إذ يمكن تصور التنفيذ الناجح لنظام ERP في بيئة المنظمة، لكن هذا التصور غير ذات جدوى إذا كان الأمن المحيط بالنظام ليس في مكانه، لأنه سينعكس على نجاح النظام. عليه، ينبغي تطوير امن نظام ERP لتكون متوافقة مع المعايير العالمية، ويتم ذلك عن طريق معالجة الأهداف الثلاثة الآتية: (Marnewick, 2008, 70)

1. تحديد توفر إطار أمن عام يمكن تطبيقه على نظام ERP، إذ يشكل النظام الجزء الأكبر من نظم تقانة المعلومات والذي يجب أن يلتزم بالسياسات والإجراءات المنفذة من قبل نظم تقانة المعلومات.
2. إن تطبيق نظام ERP لإطار أمن تقانة المعلومات ينبغي أن يتوافق مع تقانة المعلومات وحوكمة المنظمة.
3. تقديم نموذج نظام ERP الأمن عبر تكامل إطار أمن تقانة المعلومات مع نموذج ERP المقترح، وهذا يؤدي إلى ضمان وجود نظام ERP أمن للتعامل معه.

على هذا الأساس، ولغرض الوقوف على أمن المعلومات ضمن نظام ERP، فلابد من دمج نظام ERP في إطار أمن المعلومات وكما في الفقرات الآتية:

1. إطار أمن المعلومات

هنالك أطر أمنية مختلفة وكل واحدٍ منها يعالج حاجة معينة، على سبيل المثال الإطار الأمني للتعلم عن بعد، إطار تحليل امن التجارة الالكترونية، أو الإطار الآمن للمصارف التي تعمل على الانترنت. أما إطار امن المعلومات فيمكن بيانه من خلال الشكل (2) والذي يتضح من خلاله انه مكون من ثلاثة عناصر هي الأفراد (People)، والتقانة، والسياسة. وهذه العناصر مترابطة فيما بينها، فان أي تغيير في واحدة من هذه المكونات يكون لها تأثير على العنصرين الآخرين.



الشكل (2) إطار الأمن

Source: Pal R. & Thakker D., (2002), "Defining an EnptERPrise-Wide Security Framework", http://www.networkmagazineindia.com.

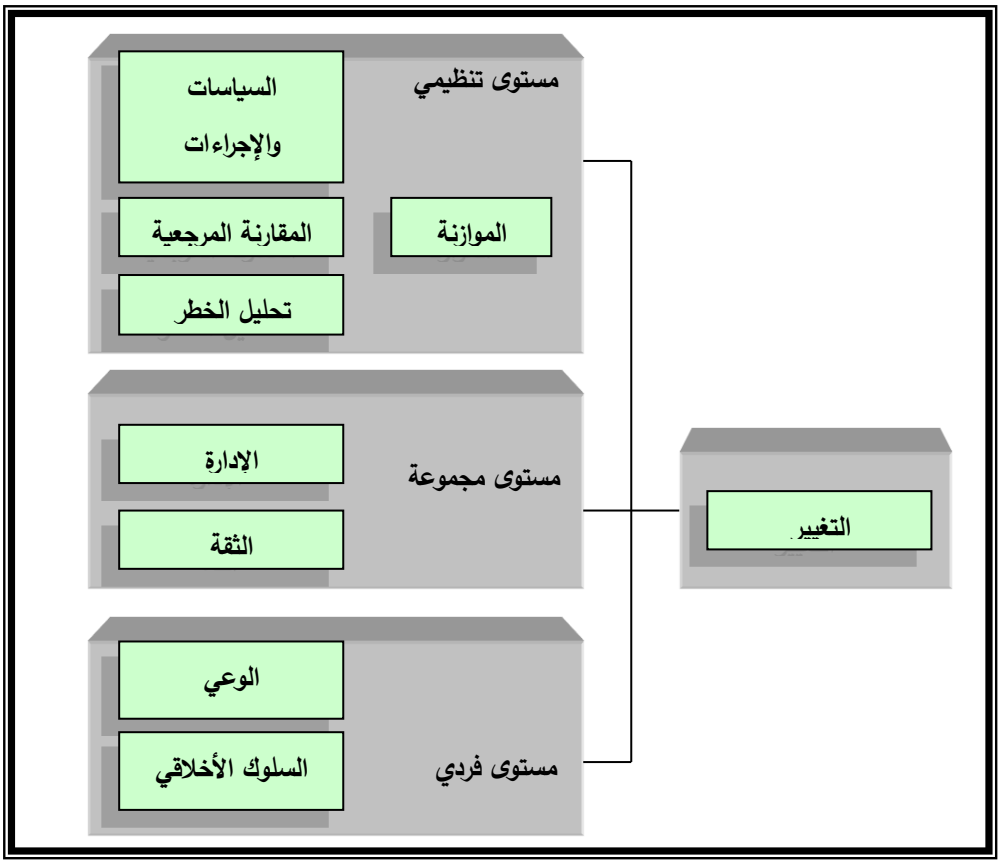
ويمكن بيان هذه المكونات على النحو الأتي:

الأول: مكون الأفراد.

يقسم هذا المكون إلى مجموعتين، المجموعة الأولى هي المسؤولة عن نشر الأمن والحفاظ عليه من خلال تنفيذ ودعم العمليات الأمنية وبما يضمن امتثالها للتشريعات المحلية والدولية، ومن أمثال هذه المجموعة الإدارة العليا، ومدراء الأمن، ومدراء تقانة المعلومات، والمدققون، فكل شخص مشترك في الإطار الأمني يعرف بالضبط ما هو دوره ومسؤولياته، وهذا يعني انه لايوجد تداخل في الأدوار والمسؤوليات.

أما المجموعة الثانية متمثلة بالأشخاص المتأثرين بالأمن على سبيل المثال المستفيدون من نظم المعلومات، والتي ينبغي أن يكونوا على بينة من الأسباب التي تظهر الحاجة إلى الأمن فضلاً عن العواقب إذا ما خرق الأمن، وخير مثال على ذلك هو ما يحدث إذا أعطى المستفيد كلمة المرور الخاصة به إلى مستفيد أخر، فالعواقب قد تكون الاحتيال والسرقة.

فمن المهم أن كلاً من المستفيدين وكذلك الأشخاص المسؤولون عن تنفيذ الأمن فهم تأثير الأمن وأهمية فرضه (Labuschagne & Marnewick, 2006, 3). ووفقاً لـ (Martins) يمكن تقسيم مكون الأفراد إلى تسعة جوانب، كما هو موضح في الشكل (3).

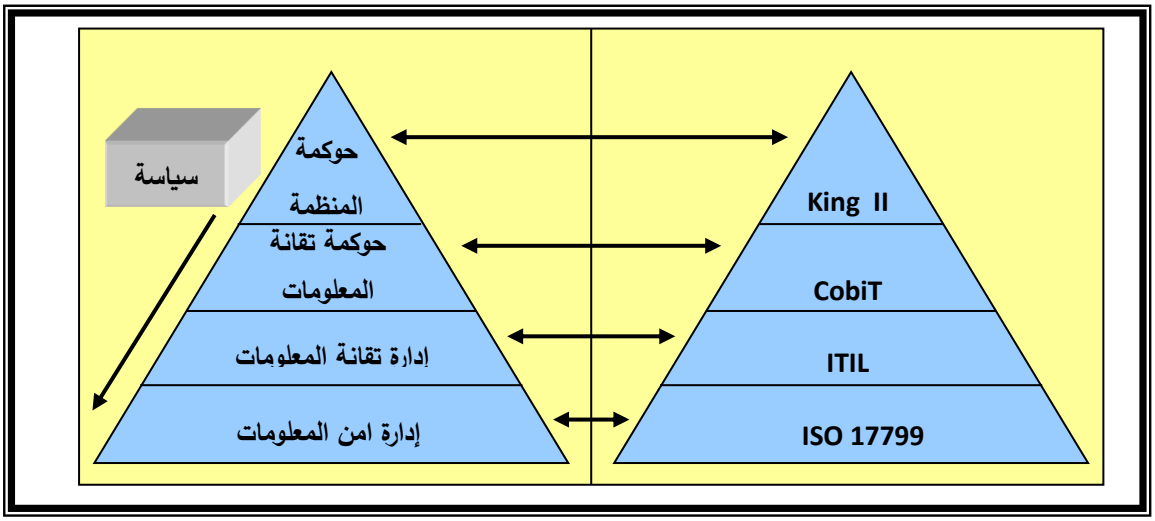


الشكل (3) مكون الأفراد

Source: Martins A., (2001), "Information Security Culture Survey", www.ujdigispace.uj.ac.za/bitstream/handle, 15.

الثاني: مكون السياسة.

توجد العديد من الطرائق المتاحة أمام المنظمة لتحقيق امن المعلومات (Njenga & Brown, 2009, 353)، كما موضحة في الشكل (4).



الشكل (4) مكون السياسة

Source: Labuschagne L. & Marnewick C., (2006), "A Security Framework for An ERP System", Conference proceedings of the ISSA New Knowledge Today Conference. Pretoria: ISSA, 4.

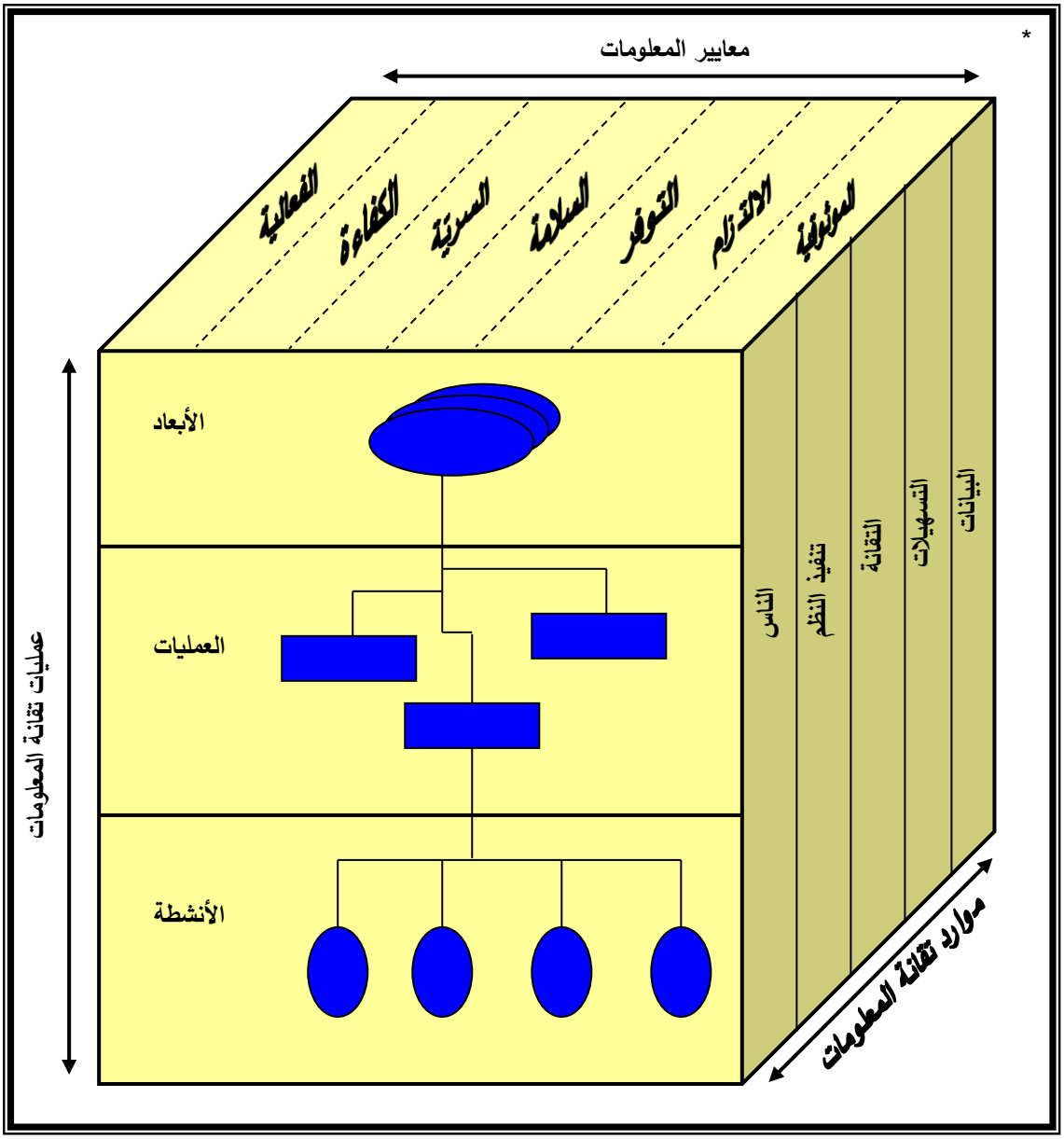
يصور الشكل (4) تفاصيل مكون السياسة والذي يزودنا بنظرة عامة عن السياسات المختلفة وفقاً لمتطلبات حوكمة المنظمة مقسمة إلى ثلاثة مستويات هي حوكمة تقانة المعلومات♣، إدارة تقانة المعلومات، وإدارة أمن المعلومات مدعومة من قبل CobiT، ITIL، وISO17799 على التوالي، وستتم مناقشة ذلك كالآتي:

- King II: تتمثل بمنظمة تعمل في جنوب أفريقيا، أصدرت تقارير بشأن حوكمة المنظمة وتقانة المعلومات (KCCG, 2002, 7-10)، وأشارت إلى أن حوكمة المنظمة تبدأ وتدار في المستوى الاستراتيجي للمنظمة.

- (CobiT: Control Objectives for Business Information Technology): هو إطار للسيطرة على حوكمة تقانة المعلومات (Tuttle & Vandervelde, 2007, 240-241)، والذي يضمن أن موارد تقانة المعلومات متجانسة مع رؤية واستراتيجيات وأهداف المنظمة (Ridley et al., 2004, 1-2). فهي تتضمن التعليمات وممارسات السيطرة (Von Solms, 2005, 100)، وتركز على ماذا يجب على المنظمات أن تعمل؟، ومن ثَمَّ يمكن تناول إطار CobiT من وجهات نظر ثلاثة وصفت بمكعب CobiT كما موضح في الشكل (5).

♣ تعرف حوكمة تقانة المعلومات: (Grembergen, 2004, 5)

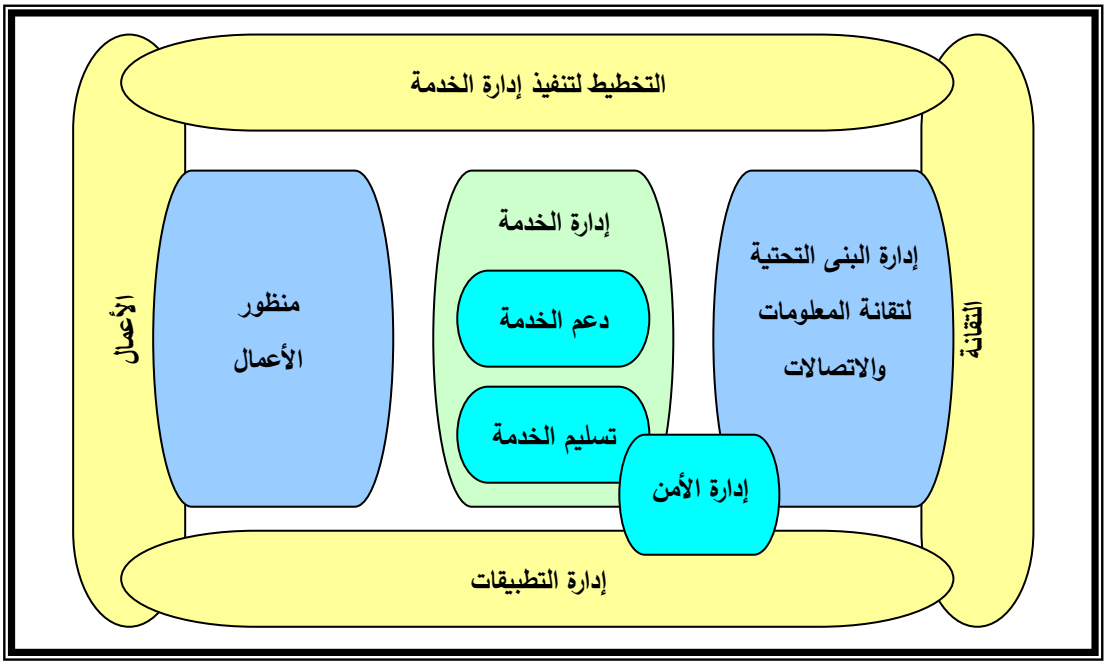
- وزارة الصناعة والتجارة العالمية: القدرة التنظيمية للسيطرة على صياغة وتنفيذ إستراتيجية تقانة المعلومات، ودليل ذو توجيه سليم لغرض تحقيق المزايا التنافسية.
- معهد حوكمة تقانة المعلومات: إنها الهياكل التنظيمية، والإجراءات التنفيذية والقيادية التي تضمن بأن تقانة المعلومات تساند وتوسع إستراتيجية المنظمة وأهدافها.
- (Etzler, 2007, 19): هو القدرة التنظيمية التي يمارسها مجلس الإدارة، الإدارة التنفيذية، وإدارة تقانة المعلومات للسيطرة على صياغة وتنفيذ إستراتيجية تقانة المعلومات والرقابة عليها بما يضمن توافق (مواءمة) تقانة المعلومات مع أعمال المنظمة.



الشكل (5) مكعب CobiT

Source: -Aksoy Nejat, (2005), "CobiT Fundamentals", SF ISACA Fall Conference, September 26th, 17.
- Guldentops et al., (2000), "CobiT Framework", 3rd ed., IT Governance Institute™, USA, 16.

- (ITIL: Information Technology Infrastructure Library): يركز على وصف وتحديد العمليات الرئيسة مثل المشكلة، والتغيير، وإدارة التهيئة ويزودنا أيضاً بإطارٍ (آلية) لإدارة هذه العمليات، ويركز على كيف يجب أن تعمل (Steel & Tan, 2005, 1-5)، وبمعنى أوسع هو إطار لعمليات إدارة خدمات تقانة المعلومات (Coentro, 2007, 23) (Lubambo, 2009, 13)، وكما موضح في الشكل (6).



الشكل (6) إطار ITIL

Source: Zhen W. & Xin-yu Z., (2007), "An ITIL-based IT Service Management Model for Chinese Universitie", www.ieeexplore.ieee.org, 1.

- ISO 17799: معاير عالمية تزودنا بتعليمات وتوصيات لتنفيذ وإدارة أمن المعلومات (Carlson, 2001, 1-3)، فهو مقسّم إلى عشر وحدات يمكن استعمالها لتنفيذ الأمن، وهذه الوحدات هي: (Muda, 2010, 14) (Chetty & Coetze, 2009, 235)

1. سياسة الأمن.
2. تأسيس أمن المعلومات.
3. إدارة الموجودات.
4. امن الموارد البشرية.
5. الأمن المادي (Physical) والبيئي.
6. إدارة التشغيل والاتصالات.
7. التحكم في الوصول للمعلومات.
8. تطوير النظام وصيانته.
9. استمرارية العمل.
10. الالتزام.

بالاعتماد على ما ذكر، فمن المهم لهذه السياسات أن تطبق على نظام ERP، فالالتزام بهذه الإجراءات والمعايير العالمية يجعل من السهل تدقيق نظام ERP، ومن ثم فإن الشعور بالراحة لدى المديرين التنفيذيين لا يتحقق إلا إذا كان نظام ERP يشكّل جزء الصورة الأكبر من ITIL و CobiT في المنظمة (Marnewick, 2008, 78).

الثالث: مكون التقانة.

ينقسم مكون تقانة أمن المعلومات إلى خمسة مرتكزات (أركان) يتم تبنيها عند تصميم نظام ERP، ويمكن مناقشة كل مرتكز من المرتكزات الخمسة كالآتي: (Diakite, 2008, 49-50) (Sookdawoor, 2005, 11-13)

▪ التعريف والتحقّق: إن المسؤولية الأولى لأمن المعلومات ضمن نظام ERP هو ضمان أن يتم الوصول إلى النظام من قبل المستفيدين المخولين، وفقاً لمجموعة من الصفات أو الخصائص التي تحدد بشكل فريد لكل مستفيد، والتي قد تكون مثلاً مجموعة من كلمات المرور (Barnes et al., 2002, 81-84).

▪ التفويض: أحد أكثر السمات الحرجة ضمن أمن نظام ERP هو حماية موارد الحاسوب وذلك بتقييد حقوق الوصول والتصرفات للمستفيدين ضمن النظام (Barnes et al., 2002, 85-87)، وذلك من خلال السماح للمخولين فقط باستخدام موارد الحاسوب، وتشمل موارد الحاسوب الملفات الفردية، عناصر البيانات، وبرامج الحاسوب، وأجهزة الحاسوب، والوظائف التي توفرها تطبيقات الحاسوب.

▪ السريّة: تنطوي سريّة المعلومات في نظام ERP على ضمان أن تكون المعلومات متاحة فقط للمصرح لهم بالوصول، وذلك لخصوصية هذه المعلومات.

▪ السلامة: تعني حفظ المعلومات من تغيير الأشخاص غير المخوّلين (توفير الحماية من تعرض البيانات للتعديل العرضي أو المتعمّد)، وضمان بأن بيانات نظام ERP تعطي تمثيلاً صحيحاً ودقيقاً للمعلومات.

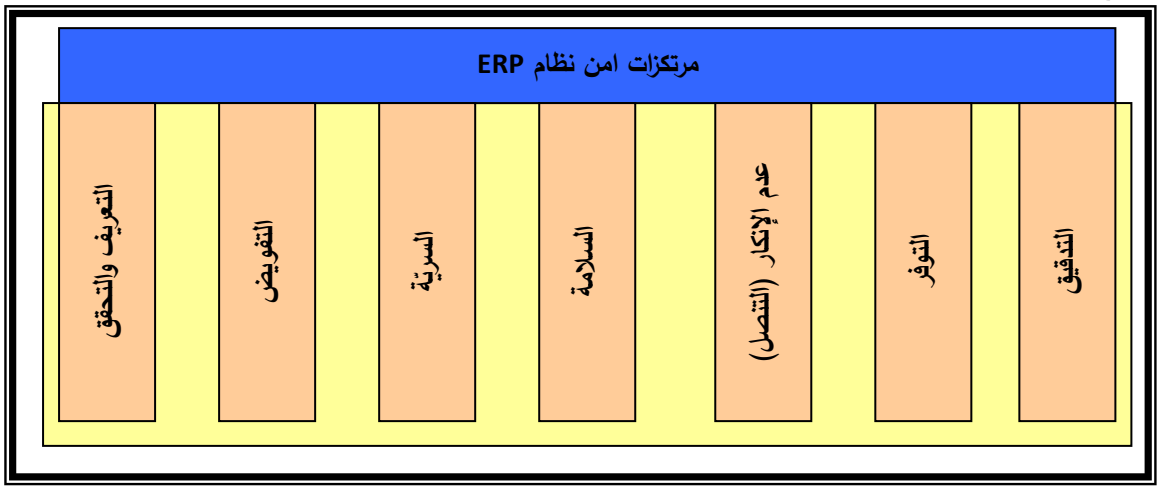
▪ عدم الإنكار (الاعتراف): تنص على أن المرسل أرسل المعلومات مع إثبات استلامها من قبل المستلم، وتأكد المستلم من هوية المرسل (Onieva et al., 2008, 2-3).

فالمرتكزات الخمسة أعلاه لاتخاطب القضيتين الاتيتين ضمن نظام ERP: (Labuschagne & Marnewick, 2006, 5-6).

▪ التوفر: يحتاج نظام ERP إلى بقائه متوفراً 7/24 لاستمرارية العمل، فالمنظمات يجب أن تكون مهيأة لاسترجاع البيانات من النظام وتقليل الحاجة للعطلات، والصيانة، والإدارة. أما المشاكل الخاصة فتتطلب جدولة الوظائف الخلفية، وتوزيع وموازنة أعباء العمل، ومراقبة أداء النظام، وقواعد المعلومات، ونظم التشغيل، والشبكات، فضلاً عن توليد الإنذارات. وتعني أيضاً قدرة النظام على توفير المعلومات التي يحتاجها المستفيدون دون عرقلة وبالشكل المطلوب (Niekerk, 2010, 27).

▪ التدقيق: من الممكن تدقيق تصميم نظام ERP بوقت مبكر في تنفيذ النظام، فعندما تكون الضغوط على الموارد والمواعيد النهائية قصيرة يمكن التغاضي عن قضايا التدقيق، لكن للأسف يمكن أن يؤدي ذلك إلى نظام غير آمن مع ضوابط مصمّمة بشكل سيء، لذلك فهناك حاجة إلى قضايا التدقيق عندما ينشر النظام أو ينفذ، وذلك بهدف التعرف على الأخطار التي تواجه النظام ومن ثم تحسين مستويات الأمن. كما يشمل التدقيق تقييم سلوك الموظفين في الامتثال للسياسات الأمنية، لأن غالبية الحوادث الأمنية تكون من داخل المنظمة (Vroom & Von Solms, 2004, 193-194).

عليه، يمكن تمديد المرتكزات الخمسة إلى سبعة مرتكزات لتشمل التوفر والتدقيق، والشكل (7) يوضح المرتكزات السبعة المتعلقة بنظام ERP.



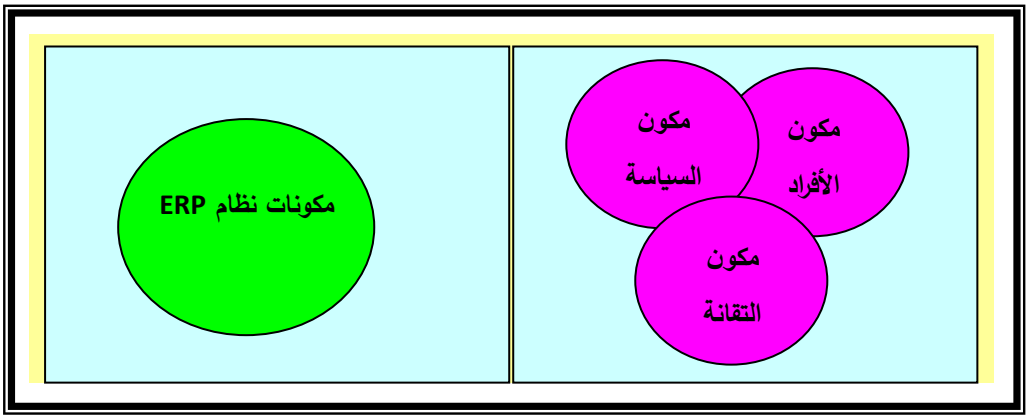
الشكل (7) المرتكزات السبعة لأمن نظام ERP

Source: Labuschagne L. & Marnewick C., (2006), "A Security Framework for An ERP System", Conference proceedings of the ISSA New Knowledge Today Conference. Pretoria: ISSA, 6.

تأسيساً على ما تقدم، يمكن استخدام الإطار الأمني الموضح في الشكل (38) لإدارة القضايا الأمنية المحيطة بنظام ERP.

2. تكامل أمن المعلومات ضمن نظام ERP

تم توضيح نموذج مكوّنات نظام ERP في الفقرة السابقة، والذي يتكون من عنصرين، إذ يتم مقابلة كل عنصر من عناصر نموذج مكونات النظام في كل عنصر من عناصر الإطار الأمني، مع تكييفها بطريقة سليمة وثابتة على نموذج نظام ERP وكما موضح في الشكل (8).



الشكل (8) مقابلة إطار الأمن في نموذج نظام ERP

المصدر: إعداد الباحث بالاعتماد على:

- Marnewick, Carl, (2008), "Ensuring Successful ERP Implementations Using The Vision-To-Project Framework", Thesis of Doctorae, Faculty of Science, University of Johannesburg, 88.

يتضح من الشكل بأن نموذج نظام ERP يشكل الأساس لتنفيذ الإطار الأمني، فهذه المقابلة أو المواءمة بينهما تمكن المنظمة من تنفيذ نظام ERP بما يتوافق مع المعايير العالمية، كما تعني أيضاً بأنه عندما يُنفَّذ الأمن، فإن ذلك سيضمن بأنها عملية مستمرة في نظام ERP ولن تهمل.

ويمكن بيان عملية المقابلة بين نموذج مكوّنات نظام ERP وإطار الأمن من خلال عرض الجدول الاتي

الجدول (2) يوضح مقابلة نموذج مكوّنات نظام ERP في إطار امن المعلومات

إطار الأمن / نموذج	مكون السياسة	مكون الأفراد	مكون التقانة
مكونات نظام ERP	▪ CobiT ▪ ITIL ▪ ISO 17799 • سياسة الأمن • إدارة الموجودات • الأمن المادي والبيئي • إدارة العمليات والاتصالات • السيطرة على الوصول للمعلومات • تطوير النظام وصيانته • استمرارية العمل • الالتزام	▪ الموازنة ▪ الإدارة ▪ التغيير	▪ التعريف والتحقّق ▪ التفويض ▪ السريّة ▪ السلامة ▪ عدم الإنكار (التنصل) ▪ التوفر ▪ التدقيق

المصدر: إعداد الباحثان بالاعتماد على:

- Labuschagne L. & Marnewick C., (2006), "A Security Framework for An ERP System", Conference proceedings of the ISSA New Knowledge Today Conference. Pretoria: ISSA, 11-12.

أما بخصوص مناقشة الجدول أعلاه، فيتم إيضاحه كالأتي:

1. مكوّن السياسة في إطار الأمن.

يركّز مكوّن السياسة على السياسات والإجراءات التي يجب أن تنفذ لإدارة وفرض الأمن، وعلى الرغم من أن مكوّن البرمجيات يتعامل فقط مع وحدات برمجيات نظام ERP، إلا أن CobiT و ITIL يزودنا بتوجيهات لكيفية تنفيذ هذه الوحدات، كما يفرض CobiT على وحدة إدارة علاقات المجهز كيف يمكن للأمن أن يدار مع الزبون.

أما تأثير ISO 17799 على وحدات برمجيات نظام ERP فيمكن بيانها على النحو الأتي:

- ❖ سياسة الأمن: تتطلب سياسة الأمن التعرف على كيفية عمل نظام ERP، وسيحوي على كل المعلومات ذات العلاقة.
- ❖ إدارة الموجودات: ينظر إلى نظام ERP بأنه يتضمن الأجهزة والبنية التحتية للشبكات والتي تتمثل بموجودات النظام التي ينبغي أن تدار، بالإضافة إلى رأس المال الفكري كتعديل النظام (الايصاء).
- ❖ الأمن المادي والبيئي: تحتاج خوادم (مزودات) نظام ERP إلى إقامتها في بيئة أمنة، ومن ثم لابد للمنظمة من السيطرة على عملية الدخول إلى النظام والمباني الخاصة به.
- ❖ إدارة العمليات والاتصالات: يجب أن يكون للإجراءات العملياتية موقع خاص بها، وذلك لتكرار عمليات النسخ الاحتياطي وحماية النظام من الوصول غير المشروع (القانوني).
- ❖ السيطرة على الوصول للمعلومات: ينبغي أن يكون للمنظمة سيطرة على الوصول للنظام، بالإضافة إلى سيطرتها على بعض الوحدات.
- ❖ تطوير النظام وصيانته: هذه الوحدة ستحدد الأمن داخل كل وحدة ضمن مكوّن البرمجيات، وبعدها كيف سيتم تشفير البيانات.
- ❖ استمرارية العمل: لابد للمنظمة من التأكد من أن النظام انحز وبالإمكان توفير المعلومات، فضلاً عن تحديد واختبار خطط استمرارية العمل للتأكد أيضاً من أن النظام يمكن أن يعمل في حال وقوع كارثة.
- ❖ الالتزام: وتعني امتثال نظام ERP بالمعايير والتشريعات.

2. مكوّن الأفراد في إطار الأمن.

وبالرغم من أن الناس سيستخدمون نظام ERP وسيتأثرون بالأمن المحيط بالنظام، إلا أن مكوّن البرمجيات لايتأثر كثيراً بمكوّن الناس. فالقضايا التي تتأثر بمكوّن الناس هي قضايا ناعمة (Soft) كالثقة والسلوك الأخلاقي، وفيما يلي بعض القضايا الصلبة:

- ❖ الموازنة: يجب على المنظمة أن تنفق المال على التدريب لكي يفهم المستفيدين كيف يعمل نظام ERP، تأثير الأمن على عملهم، والقضايا التي تحيط بأمن نظام ERP.
- ❖ الإدارة: لايستطيع المستفيدين من نظام ERP أن يفرضوا الأمن إلا إذا كان مدعوماً من قبل الإدارة.
- ❖ التغيير: إن تنفيذ نظام ERP سيؤثّر على المستفيدين، لأنه سيحدث تغيير في حياتهم، لذلك يتعين على المنظمة أن تعرف كيف تتعامل مع هذا التغيير.

3. مكوّن التقانة في إطار الأمن.

يمكن تطبيق المرتكزات السبعة على مكوّن البرمجيات، فمرتكز التعريف والتحقّق يحدد من له الحق في الوصول إلى مكوّنات البرمجيات، بينما مرتكز التفويض يحدد أي نوع من الوحدات يمكن

الوصول إليها. يجب أن تكون المعلومات المجهزة للمستفيدين متكاملة من كل وحدات النظام بالإضافة إلى سريتها، وهذا يعني أن المعلومات ينبغي أن تتدفق من جانب واحد في نظام ERP، فعلى سبيل المثال – وحدة إدارة علاقات المجهز– فمن حقها طباعة الفاتورة من تدخل أي مستفيد، وهو ما يعني بان هنالك اتفاقات (تعاملات) خاصة مع المجهز لايمكن رؤيتها من قبل الغرباء، أي تبقى سريّة.

أما عدم الإنكار فيلعب دوراً مهماً خصوصاً في وحدة إدارة علاقات المجهز وإدارة سلسلة التجهيز. عليه، لابد لكل وحدات النظام أن تكون متوفرة دائماً، خصوصاً للتفاعل وتدفق المعلومات بين الوحدات المختلفة، بالإضافة إلى ملائمتها للمجهزين والزبائن. علاوة على ذلك، لابد لكل الوحدات أن تتوافق مع معايير التدقيق.

المحور الثالث / الاطار الميداني

أولاً. اهداف نظام ERP في شركة الحكماء

يشهد العالم هذه الأيام تطوراً واسعاً في نظم وتكنولوجيا المعلومات إذ تطورت أنظمة الحاسوب واتسع مجال العمل فيها لما تمتاز به من مرونة وسرعة ودقة وما تتصف به من كفاءة في أداء العمل. لذا فأن التحول من الأسلوب التقليدي (اليدوي) المتبع حالياً إلى أسلوب تقني مبرمج يساعد في تخطي الصعوبات التي تواجهها الإدارة والأفراد العاملين في الشركة ويعزز الأداء المنظمي، فضلاً عن تحقيق الأهداف الآتية:

1. بناء منصة قياس وتعزيز الأداء المنظمي، ولتكون منطلقاً باتجاه ترشيد صنع واتخاذ القرارات في الشركة.
2. زيادة درجة التعاون والتنسيق بين مختلف الأقسام داخل الشركة من جهة، وبينها وبين الإدارة العليا من جهة أخرى.
3. توظيف شبكة الاتصالات التي تمتلكها الشركة في تبادل المعلومات في ما بين أقسام الشركة.
4. تحسين كفاءة الأداء لجميع الأقسام والعاملين في الشركة، وذلك بتوفير احتياجاتهم من المعلومات، وتحقيق التنظيم الأمثل للعلاقة بينهم، من خلال السيطرة المركزية على عمل كافة الأنظمة في الاختصاصات المختلفة بما يضمن المحافظة على سرية العمل والمعلومة المنتقلة.

5. تجنب حالات التكرار في العمل الإداري وإدخال المعلومات وتحليلها، الذي يقوم به أكثر من قسم في الشركة المبحوثة في الوقت ذاته، مما يساعد في التخلص من الأخطاء الإدارية التي يمكن الوقوع فيها.

6. تقليل الحاجة إلى الوثائق الورقية، ومن ثم التخفيف من حدة الزيادة السنوية في الاستهلاك الورقي، فضلاً عن التخلص عن الأخطاء الناجمة عنه.

7. إمكانية الحصول على المعلومات التي تخص الموظفين (مدراء وعاملين) بأقصر وأسهل الطرق بعد تطبيق النظام الجديد.

8. المحافظة على البيانات والمعلومات من الفقدان أو التلف ولأي سبب من خلال إدخالها على الحاسوب.

9. توفير قاعدة معلومات لجميع البيانات والمعلومات من اجل ضمان الحصول على المعلومات المطلوبة بالنوع والكم المطلوب وبشكل منظم.

10. توفير مستودع معلومات للبيانات والمعلومات من اجل ضمان الحصول على المعلومات المطلوبة بالنوع والكم المطلوب وبشكل منظم، وبالأخص ما يخص الأداء المنظمي.

11. العمل على عدم حدوث التكرار في عمليات جمع وإدخال ومعالجة البيانات وتحليلها من خلال وجود قاعدة بيانات واحدة تشمل جميع المعلومات.

12. تقليل عبء العمل الإداري اليومي على الموظف، مما يساعد على توفير خدماته وجهوده لأعمال أخرى أكثر أهمية والشركة بحاجة اكبر إليها.

13. توظيف تقانات المعلومات الحديثة (المعالجة التحليلية الآنية والتنقيب في البيانات) في تعزيز الأداء المنظمي.

14. السيطرة على حركة التعاملات اليومية التي تجري في الشركة.

ويتسم النظام المقترح بسمات أخرى فضلاً عن أهدافه إذ يمتاز بـ:

- سهولة استخدام النظام إذ يستطيع المستفيد العمل عليه وتصفحه.
- إمكانية النظام على التحديث والحفظ والإضافة والاسترجاع.

وعن طريق نظام ERP يمكن تجهيز الإدارة بالتقارير والمعلومات المطلوبة بدقة متناهية وبدون عناء، ومن ثم قياس وتعزيز الأداء المنظمي فضلاً عما سيوفره النظام من اكتساب الخبرة للعاملين من خلال استخدامهم الحاسوب وبأسلوب علمي يوفر المزيد من الوقت لديهم لعمل أفضل.

ثانياً: وصف عينة الدراسة

يشير الجدول (3) إلى نسب أهم الخصائص المميزة لعينة الدراسة، وكما يأتي:

الجدول (3) وصف عينة الدراسة

الجنس			
ذكر		أنثى	
العدد	%	العدد	%
19	95	1	5

العمر (سنة)					
35-25		45-36		55-46	
العدد	%	العدد	%	العدد	%
16	80	2	10	2	10

التحصيل الدراسي			
بكالوريوس		شهادة عليا	
العدد	%	العدد	%
19	95	1	95

مدة الخدمة في المنصب الحالي (سنة)							
اقل من سنة		2-1		4-3		5 فأكثر	
العدد	%	العدد	%	العدد	%	العدد	%
2	10	2	10	10	50	6	30

المصدر: إعداد الباحثان.

يشير الجدول (3) الآتي:

أ. نسبة الذكور هي العالية.

ب. أعلى نسبة للمدراء الذين تقترب أعمارهم من (25-35).

ج. أعلى نسبة للتحصيل الدراسي كانت للحاصلين على شهادة البكالوريوس.

د. بلغت أعلى نسبة للمديرين في المنصب الحالي ممن لديهم خدمة (3-4) سنوات.

ثالثاً: عرض نتائج البحث وتحليلها

يتطلب نجاح نظام ERP وقدرته في الحفاظ على العمليات الإدارية توافر أرضية أمنية تمكن النظام من تقديم معلوماته بدقة وموثوقية ومحمية بأطر امنية عالية، وهذا ما يتطلب تحليله والوقوف على واقعه في الشركة المبحوثة، وذلك من خلال استخدام قائمة الفحص[1] وكما يأتي:

([1]). **المعادلات الخاصة بقائمة الفحص هي:**

- **النتيجة = الاوزان × التكرارات**
- **المعدل = مج النتيجة / مج التكرارات**
- **النسبة المئوية = مج النتيجة / (N * أعلى وزن)**

أن النتائج الخاصة بأمن معلومات نظام ERP الخاصة بالشركة تشير يمكن توضيحها من خلال المعدلات والنسبة المئوية، وكما مبين في الجدول (4).

الجدول (4) نتائج تحليل مجالات أمن المعلومات لنظام ERP

1. مكون الأفراد				
ت	العبارات	متوفر	متوفر لحدٍ ما	غير متوفر
1	تهتم إدارة شركتنا بوضع سياسة (مجموعة من المعايير والأنظمة) أمن المعلومات لنظام ERP.	*		
2	تهتم إدارة شركتنا بتحديد سلوك المستفيد والحالات المتوقعة منه.		*	
3	تحرص شركتنا على إجراء مقارنات مرجعية مع شركات تمتاز بأمنية عالية لنظمها.	*		
4	تحرص شركتنا على تحليل المخاطر والتهديدات التي تواجه التدابير الأمنية لنظام ERP.	*		
5	تهتم إدارة شركتنا بتوفير المبالغ اللازمة لتنفيذ القضايا المتعلقة بشأن ثقافة أمن المعلومات لنظام ERP.		*	
6	تدرك الإدارة العليا لأهمية امن المعلومات لنظام ERP في الحفاظ على موجود المعلومات.		*	
7	تسعى شركتنا إلى غرس الثقة في بيئة تقانة ونظم المعلومات.		*	
8	تحرص شركتنا على توعية المستفيدين بشأن ضوابط امن المعلومات لنظام ERP.			*
9	تهتم شركتنا بنشر السلوك الأخلاقي الخاص بأمن المعلومات لنظام ERP.	*		
10	تشجع إدارة شركتنا التغييرات التي تسهم في تعزيز أمن المعلومات لنظام ERP.		*	
الأوزان		**3**	**2**	**1**
التكرارات		**4**	**5**	**1**
النتيجة		**12**	**10**	**1**
المعدل		**2.3**		
النسبة المئوية		**76.7**		
2. مكون السياسة.				
ت	العبارات	متوفر	متوفر لحدٍ ما	غير متوفر
أ	تحرص إدارة شركتنا على حوكمة تقانة المعلومات من حيث أنها:			
1	تسعى لإشراك مدراء تقانة المعلومات في تحديد إستراتيجية وأهداف الشركة.	*		

2	تقوم بتحديد وتعريف واضح لمسؤوليات وادوار وصلاحيات المستفيدين الذين ينفذون مختلف نشاطات تقانة المعلومات.		*	
3	تقوم بوضع تعليمات مكتوبة تصف وتحدد مختلف السلوكيات الغير جيدة وتوزعها على المستفيدين.	*		
4	تضع معايير عالية جدا لموظفي تقانة المعلومات في المواقع الحساسة من الشركة.			*
5	تؤكد على تنفيذ عمليات النسخ الاحتياطي للمعلومات وإدامتها بشكل دوري.		*	
ب	تهتم إدارة شركتنا بإدارة تقانة المعلومات من حيث أنها:			
6	تهتم بوضع الخطط لإدارة تقانة المعلومات الخاصة بنظام ERP.		*	*
7	تمتاز خطط إدارة تقانة المعلومات بمرونتها وقدرتها العالية على تحقيق الاحتياجات المستقبلية لشركتنا.	*		
8	تحرص على إدارة البنى التحتية لتقانة المعلومات والاتصالات.	*		
9	تشجع على تدريب موظفي إدارة تقانة المعلومات.	*		
ج	تهتم إدارة شركتنا بإدارة أمن المعلومات من حيث أنها:			
10	تحرص إدارة شركتنا على الإشراف على تنفيذ أسس ومعايير امن المعلومات لنظام ERP.	*		
11	تهتم إدارة شركتنا بإجراء الاختبارات لضمان امن المعلومات في نظام ERP.	*		
12	تحرص شركتنا على إجراء التنسيق الأمني للمعلومات (حماية المعلومات تكون مسؤولية الجميع).	*		
13	تهتم شركتنا بتحديد المعلومات التي تتطلب حمايتها ومن المسؤول عن حماية هذه المعلومات.	*		
14	تهتم شركتنا بتحديد الموجودات التي تحتاج إلى حماية ومن المسؤول عن حماية هذه الموجودات.	*		
15	تحرص شركتنا على وضع عقوبات على الموظفين المخالفين لأنظمة الأمن.		*	
16	تهتم إدارة شركتنا بتوفير الأمن المادي والبيئي للحد من التعرض للمخاطر كاحتراق المبنى مثلاً.	*		
17	تحرص شركتنا على وضع خطط تتبعها عند حدوث مشاكل غير متوقعة لضمان استمرارية العمل.		*	
18	تحرص شركتنا على الالتزام لقوانين ولوائح أمن المعلومات الخاصة بنظام ERP.	*		
	الأوزان	**3**	**2**	**1**
	التكرارات	**11**	**5**	**2**
	النتيجة	**33**	**10**	**2**
	المعدل	**2.5**		
	النسبة المئوية	**83.3**		

3. مكون التقانة.				
ت	العبارات	متوفر	متوفر لحدٍ ما	غير متوفر
1	تمتاز شركتنا بعدم السماح للمستفيدين من الوصول إلى معلومات نظام ERP إلا بعد التحقّق من هويته (مثلاً استخدام كلمات المرور).	*		
2	تحرص شركتنا على ممارسة عمليات التفويض للمستفيدين ضمن نظام ERP بشأن حرية التصرف في استخدام موارد الحاسوب.	*		
3	تشجع شركتنا توافر السريّة في المعلومات التي يقدمها نظام ERP.	*		
4	تهتم شركتنا بتحديد الأشخاص المسموح لهم بتعديل البيانات لغرض توفير الحماية من تعرض البيانات للتعديل العرضي أو المتعمّد.			*
5	تحرص شركتنا على عدم إنكار (الاعتراف) المرسل للمعلومات والمستلم لها.		*	
6	تهتم شركتنا بممارسة عملية التدقيق الخاصة بنظام ERP للوصول إلى نظام آمن.	*		
الأوزان		**3**	**2**	**1**
التكرارات		**4**	**1**	**1**
النتيجة		**12**	**2**	**1**
المعدل		**2.5**		
النسبة المئوية		**83.3**		

الجدول (5) نتائج تحليل مجالات أمن المعلومات لنظام ERP ومعدلاتها والنسب المئوية والمعدل الإجمالي للشركة المبحوثة

ت	مجالات تقانة المعلومات	المعدل (الوزن الكلي للفقرات)	النسبة المئوية (%)
1	مكون الأفراد	2.3	%76.7
2	مكون السياسة	2.5	%83.3
3	مكون التقانة	2.5	%83.3
المجموع		**7.3**	**243.3**
المعدل الإجمالي		**2.4**	**%81.1**

يتضح من الجدول حصول المجالات (مكون الأفراد، مكون السياسة، ومكون التقانة) على معدلات تتراوح بين (2.3–2.5) درجة وهو معدل عالٍ، وبنسب (76.7%، 83.3%، 83,3%) على التوالي، وهذا مؤشر ايجابي يشير إلى تمتع نظام ERP بأمن معلومات عالٍ، مما يسهم ذلك في الحفاظ على العمليات الإدارية للشركة.

المحور الرابع / الاستنتاجات والمقترحات

أولاً: الاستنتاجات

اعتمادا على ما سبق يمكن النظر إلى أهم الاستنتاجات على النحو الآتي:

1. يمثل امن المعلومات جزءاً مهماً في نظام ERP، لمسوغات معينة إذ يمكن تصور التنفيذ الناجح للنظام في بيئة المنظمة، لكن هذا التصور غير ذي جدوى إذا كان الأمن المحيط بالنظام ليس في مكانه.
2. ان الحماية الأمنية لنظام ERP تمكنه من تقديم معلومات كفوءة تسهم في الحفاظ على العمليات الإدارية في المنظمة
3. أثبتت نتائج التحليل الاحصائي الى توافر نظام ERP أمنية عالية، وعلى مستوى كل المجالات الخاصة باطار الأمني لنظام ERP.

ثانياً: المقترحات

تتجسد اهم هذه المقترحات فيما مفاده الآتي:

1. العمل على زيادة الاهتمام بنظم وتقانة المعلومات (وخاصة امن المعلومات) بصورة مستمرة في الشركة المبحوثة كون ذلك يعد عاملاً مهماً في استمرارية النجاح في تنفيذ نظم المعلومات ومنها نظام ERP.
2. استخدام تنفيذ القوانين الخاصة بالعقوبات الناتجة عن الاخلال في إيصال المعلومات وتبادل الوثائق بين الشركة والجهات ذات العلاقة بها
3. توسيع الاعتماد على أمن المعلومات للنظم الالكترونية، ومعالجة الضعف في البنية التقنية.
4. ضرورة إيلاء الإدارة مزيداً من الاهتمام بتطوير برامج للتدريب خاصة بأمن المعلومات بالشكل الذي تسهم في تعزيز أمن نظام ERP.
5. يحث الباحثان زملائهم لإيلاء متغير بحثهم المزيد من الاهتمام لما له من اثر بالغ في نجاح أنظمة المعلومات، ونقترح عليهم في هذا المجال على اعادة دراسة هذا الموضوع، لكن في اطار بناء الإدارة الالكترونية، فضلاً عن زيادة الإنتاجية والاستغلال الأمثل للطاقات.

المصادر

A. Reports

1. Barker, William C., (2003), “Information Security”, Guideline for Identifying an Information System as a National Security System, National Institute of Standards and Technology.
2. Force, Joint, (2010), “Information Security”, Guide for Applying the Risk Management Framework to Federal Information Systems A Security Life Cycle Approach, National Institute of Standards and Technology.

B. Dissertations & Thesis

1. Coentro, João Pimentel, (2007), "A Model of Quality Service Management for Information Systems", Master Thesis Unpublished, **University of Porto.**
2. Diakite, Soumailadit, (2008), "WISP: A Wireless Information Security Portal", Master Thesis Unpublished, **University of Johannesburg.**
3. Etzler, Joel, (2007), "IT Governance According to COBIT: How does the IT performance within one of the largest investment banks in the world compare to COBIT?", Master Thesis Unpublished, **Stockholm University.**
4. Lubambo, Nontobeko, (2009), "Investigating The Use of The ITIL Framework Towards IT Service Delivery At The Nmmu", Master Thesis Unpublished, **Nelson Mandela Metropolitan University**.
5. Marnewick, Carl, (2008), "Ensuring Successful ERP Implementations Using The Vision-To-Project Framework", Doctor Thesis Unpublished, **University of Johannesburg**.
6. Martin, Andrew P., (2003), "Key Determinants of Information Availability: A Multiple Case Study", Master Thesis Unpublished, **University of Nebraska**.
7. Muda, Mohd Zuki, (2010), "Awareness and Acceptance Analysis of Information Security Policy", Master Thesis Unpublished, **University of Malaysia**.
8. Niekerk, Johannes, (2010), "Fostering Information Security Culture Therough Integrating Theory and Technology", Doctor Thesis Unpublished, **Nelson Mandela Metropolitan University.**
9. Sookdawoor, Oumeshsingh, (2005), "An Investigation of Information Security Policies and Practices in Mauritius", Master Thesis Unpublished, **University of South Africa.**

C. Journals

1. Onieva, J., Zhou, J. & Lopez J., (2008), "Multi-Party Non-Repudiation: A Survey", **ACM Comput**, Vol. 41, No. 1.
2. Tuttle, Brad & Vandervelde, Scott D., (2007), "An empirical examination of CobiT as an internal control framework for information technology", **International Journal of Accounting Information** Systems, Vol. 8, No. 4.
3. Von Solms, Basie, (2005), "Information Security governance: COBIT or ISO 17799 or both?", **Computers & Security**, Vol. 24, No.
4. Vroom, Cheryl & von Solms, Rossouw, (2004), "Towards information security behavioural compliance", **Computers & Security**, Vol. 23, No. 4.

D. Conferences

1. Aksoy Nejat, (2005), "CobiT Fundamentals", SF ISACA Fall Conference, September 26th.

2. Chetty, Jacqui & Coetzee, Marijke, (2009), "Evaluating Information Security Controls Applied By Service-Oriented Architecture Governance Frameworks", **Proceedings of the ISSA Conference**, School of Tourism & Hospitality, University of Johannesburg.
3. Labuschagne L. & Marnewick C., (2006), "A Security Framework for An ERP System", Conference proceedings of the ISSA New Knowledge Today Conference. Pretoria: ISSA.
4. Njenga, Kennedy N. & Brown, Irwin, (2009), "Inductively Deriving an Organisational Information Security Risk Management Agenda by Exploring Process Improvisation", **Proceedings of the ISSA Conference, School of Tourism & Hospitality**, University of Johannesburg.
5. Ridley, Gail, Young, Judy & Carroll, Peter, (2004), "COBIT and its Utilization: A framework from the literature", **Proceedings of the 37th Hawaii International Conference on System Sciences**.
6. Steel, Cater A. & Tan, Wui-Gee, (2005), "Implementation of IT Infrastructure Library (ITIL) in Australia: **Progress and Success Factors" IT Governance International Conference**, Auckland, NZ.

E. Books

1. Barnes, C., Bautts, T., Lloyd, D., Ouellet, E., Posluns, J., Zendzian, D. & O'Farrell, N., (2002), **Syngress** Publishing, Inc., USA.
2. Grembergen, Wim Van, (2004), **"Strategies for Information Technology Governance",** Idea Group Inc., USA & United Kingdom.
3. Guldentops et al., (2000), "CobiT Framework", 3rd ed., IT Governance Institute™, USA, 16.

F. Internet

1. Carlson, Tom, (2001), "Information Security Management: Understanding ISO 17799", www.netbotz.com/library/ISO_17799.
2. Entrust, (2004), "Information Security Governance (ISG): An Essential Element of Corporate Governance", www.entrust.com.
3. Martins A., (2001), "Information Security Culture Survey", www.ujdigispace.uj.ac.za/bitstream/handle.
4. Pal R. & Thakker D., (2002), "Defining an EnptERPrise-Wide Security Framework", http://www.networkmagazineindia.com.
5. Zhen W. & Xin-yu Z., (2007), "An ITIL-based IT Service Management Model for Chinese Universitie", www.ieeexplore.ieee.org.

ألملحق (1)

جامعة الموصل

كلية الإدارة والاقتصاد

م/قائمة فحص

أولا: البيانات العامة

1. الجنس:
2. العمر:
3. التحصيل الدراسي:
4. مدة الخدمة في المنصب الحالي:

أمن المعلومات لنظام ERP

1. مكون الأفراد				
ت	العبارات	متوفر	متوفر لحدٍ ما	غير متوفر
1	تهتم إدارة شركتنا بوضع سياسة (مجموعة من المعايير والأنظمة) أمن المعلومات لنظام ERP.			
2	تهتم إدارة شركتنا بتحديد سلوك المستفيد والحالات المتوقعة منه.			
3	تحرص شركتنا على إجراء مقارنات مرجعية مع شركات تمتاز بأمنية عالية لنظمها.			
4	تحرص شركتنا على تحليل المخاطر والتهديدات التي تواجه التدابير الأمنية لنظام ERP.			
5	تهتم إدارة شركتنا بتوفير المبالغ اللازمة لتنفيذ القضايا المتعلقة بشأن ثقافة أمن المعلومات لنظام ERP.			
6	تدرك الإدارة العليا لأهمية امن المعلومات لنظام ERP في الحفاظ على موجود المعلومات.			
7	تسعى شركتنا إلى غرس الثقة في بيئة تقانة ونظم المعلومات.			
8	تحرص شركتنا على توعية المستفيدين بشأن ضوابط امن المعلومات لنظام ERP.			
9	تهتم شركتنا بنشر السلوك الأخلاقي الخاص بأمن المعلومات لنظام ERP.			
10	تشجع إدارة شركتنا التغييرات التي تسهم في تعزيز أمن المعلومات لنظام ERP.			
2. مكون السياسة.				
ت	العبارات	متوفر	متوفر لحدٍ ما	غير متوفر
1	تحرص إدارة شركتنا على حوكمة تقانة المعلومات من حيث أنها:			
1	تسعى لإشراك مدراء تقانة المعلومات في تحديد إستراتيجية وأهداف الشركة.			
2	تقوم بتحديد وتعريف واضح لمسؤوليات وادوار وصلاحيات المستفيدين الذين ينفذون مختلف نشاطات تقانة المعلومات.			
3	تقوم بوضع تعليمات مكتوبة تصف وتحدد مختلف السلوكيات الغير جيدة وتوزعها على المستفيدين.			
4	تضع معايير عالية جدا لموظفي تقانة المعلومات في المواقع الحساسة من الشركة.			

5	تؤكد على تنفيذ عمليات النسخ الاحتياطي للمعلومات وإدامتها بشكل دوري.			
2	تهتم إدارة شركتنا بإدارة تقانة المعلومات من حيث أنها:			
1	تهتم بوضع الخطط لإدارة تقانة المعلومات الخاصة بنظام ERP.			
2	تمتاز خطط إدارة تقانة المعلومات بمرونتها وقدرتها العالية على تحقيق الاحتياجات المستقبلية لشركتنا.			
3	تحرص على إدارة البنى التحتية لتقانة المعلومات والاتصالات.			
4	تشجع على تدريب موظفي إدارة تقانة المعلومات.			
3	تهتم إدارة شركتنا بإدارة أمن المعلومات من حيث أنها:			
1	تحرص إدارة شركتنا على الإشراف على تنفيذ أسس ومعايير امن المعلومات لنظام ERP.			
2	تهتم إدارة شركتنا بإجراء الاختبارات لضمان امن المعلومات في نظام ERP.			
3	تحرص شركتنا على إجراء التنسيق الأمني للمعلومات (حماية المعلومات تكون مسؤولية الجميع).			
4	تهتم شركتنا بتحديد المعلومات التي تتطلب حمايتها ومن المسؤول عن حماية هذه المعلومات.			
5	تهتم شركتنا بتحديد الموجودات التي تحتاج إلى حماية ومن المسؤول عن حماية هذه الموجودات.			
6	تحرص شركتنا على وضع عقوبات على الموظفين المخالفين لأنظمة الأمن.			
7	تهتم إدارة شركتنا بتوفير الأمن المادي والبيئي للحد من التعرض للمخاطر كاحتراق المبنى مثلاً.			
8	تحرص شركتنا على وضع خطط تتبعها عند حدوث مشاكل غير متوقعة لضمان استمرارية العمل.			
9	تحرص شركتنا على الالتزام لقوانين ولوائح أمن المعلومات الخاصة بنظام ERP.			
3. مكون التقانة.				
ت	العبارات	**متوفر**	**متوفر لحدٍ ما**	**غير متوفر**
1	تمتاز شركتنا بعدم السماح للمستفيدين من الوصول إلى معلومات نظام ERP إلا بعد التحقّق من هويته (مثلاً استخدام كلمات المرور).			
2	تحرص شركتنا على ممارسة عمليات التفويض للمستفيدين ضمن نظام ERP بشأن حرية التصرف في استخدام موارد الحاسوب.			
3	تشجع شركتنا توافر السريّة في المعلومات التي يقدمها نظام ERP.			
4	تهتم شركتنا بتحديد الأشخاص المسموح لهم بتعديل البيانات لغرض توفير الحماية من تعرض البيانات للتعديل العرضي أو المتعمّد.			
5	تحرص شركتنا على عدم إنكار (الاعتراف) المرسل للمعلومات والمستلم لها.			
6	تهتم شركتنا بممارسة عملية التدقيق الخاصة بنظام ERP للوصول إلى نظام آمن.			