مدى استعداد شركات الانترنت لحوكمة أمن معلوماتها باعتماد المواصفة الدولية ISO 17799- (دراسة مقارنة بين شركة اللقاء نت وشركة Speed Way لخدمات الانترنت/كركوك)

م.د. محمد مصطفى حسين حسن
جامعة الموصل/كلية الإدارة والاقتصاد
Asha.mustafa@yahoo.com

م.م. شعيب محمد شريف
كلية القلم الجامعة/كركوك
Shuaebs@yahoo.com

المقدمة

كانت المنظمات تعتمد في السابق على المال والأرض والعمل كعناصر أساسية لاستمرارها ونجاحها، ومع التطور المتسارع في العالم ودخولها في عصر العولمة والاقتصادي الرقمي دخلت المعلومات بقوة لتكون العنصر الحاسم في ديمومة نشاط المنظمات، وأصبحت المنافسة تعتمد على ما تمتلكها المنظمة من المعلومات كمادة أولية أساسية تضمن بقائها في دائرة المنافسة، من هنا فإن هذه المعلومات والمنظومة التي تحويها أصبحت عرضة لبعض المخاطر والتهديدات كالسرقة، والتلاعب، والتخريب، وغيرها من المخاطر المتعمدة والغير المتعمدة، خاصة وان المعلومات تتميز بعدم ملموسيتها، وإمكانية تسريبها بسرعة فائقة، إضافة إلى صعوبة تتبع وكشف مرتكبي جرائم المعلومات، من هنا بدأت المنظمات تتخذ إجراءات وتعتمد سياسات ونظم لحماية معلوماتها قدر المستطاع، ويمكن القول إن هذه الإجراءات والممارسات هي: توجه نحو حوكمة امن المعلومات، وقد قدمت نماذج عديدة في هذا المجال والتي من أبرزها المواصفة ISO17799

الموجهة نحو امن نظم المعلومات، وتقنية المعلومات في المنظمة، وامن المعلومات، وتوفير الحماية لها من خلال الالتزام ببعض المتطلبات التي تدخل في جميع تفاصيل حماية وسلامة المعلومات، وتحديدا المعلومات الحساسة والسرية في المنظمة، لاسيما في بعض المنظمات الخدمية التي تعتبر المعلومات أساسا المنتجات التي تنتجها وتقدمها للزبائن، كشركات الاتصالات والمصارف والصحف وغيرها.

المحور الأول: منهجية البحث

أولا: مشكلة البحث

تطورت المنظمات العاملة في قطاع الاتصالات في العراق مع بداية القرن الحالي، وازدهرت نشاطها مع توسع شبكات الاتصالات وخاصة شبكة الاتصالات الدولية (الانترنت)، مع زيادة حجم المعلومات، وتوسع نطاق تبادل المعلومات، ودخول إطراف عديدة في الاتصال، فإن هذه المعلومات قد تكون عرضة للعديد من المخاطر، لاسيما مع ظهور العديد من الشركات العاملة في هذا القطاع، واشتداد المنافسة بينها، لذلك تحتاج المنظمة إلى حوكمتها للسيطرة وإحكام الرقابة عليها، من هنا يمكن الإشارة إلى مشكلة البحث من خلال التساؤلات البحثية الآتية:

١. هل تمتلك إدارة الشركات قيد البحث فكرة عن المخاطر التي يمكن أن تواجه معلوماتها؟
٢. ما مدى تطبيق الشركات المبحوثة لمتطلبات المواصفة الدولية ISO17799؟
٣. هل هناك اختلاف بين الشركات قيد البحث في حوكمة امن المعلومات من خلال التطبيق والالتزام بمتطلبات المواصفة الدولية ISO17799؟

ثانيا: أهمية البحث

أكاديميا فإن للبحث أهمية في طرح موضوع جوهري لم تتطرق إليها دراسات كثيرة رغم أهمية مضمونها، حيث يناقش الجانب النظري للبحث تفاصيل الأدبيات المطروحة من قبل الباحثين فيما يخص موضوع حوكمة امن المعلومات، أما ميدانيا فتظهر أهمية البحث من خلال توجيه أنظار الشركات العاملة في مجال المعلومات والاتصالات الى حساسية منتجها، وإمكانية تعرضها إلى مخاطر كبيرة تهدد بقائها، وحثهم على الاهتمام بتفاصيل امن المعلومات وسلامتها.

ثالثاً: أهداف البحث

يستهدف البحث نحو تحقيق جملة أهداف من أبرزها:

١. تقديم إطار نظري عن إحدى المواضيع المعاصرة, والتي تولي المنظمات العالمية اهتماما خاصا بها وهو امن المعلومات، وحوكمتها.
٢. التعرف على تفاصيل المواصفة الدولية ISO17799، من خلال استعراض مجالات استخدامها، والمتطلبات الرئيسية والثانوية لهذه المواصفة.
٣. تشخيص نسبة تطبيق المواصفة الدولية ISO17799 من قبل الشركات قيد البحث.
٤. المقارنة بين الشركات قيد البحث من حيث حوكمة أمن المعلومات، والالتزام بمتطلبات المواصفة الدولية ISO17799 المستخدمة في الحوكمة.

رابعا: فرضيات البحث

بناءا على مشكلة البحث المطروحة يمكن صياغة الفرضيات الآتية:

١. لا تمتلك الشركات قيد البحث تصور وفكرة عن المخاطر التي يمكن ان تتعرض لها معلوماتها.

٢. إن متطلبات المواصفة ISO17799 غير مطبقة في الشركات قيد البحث.

٣. هناك اختلاف في حوكمة امن المعلومات وتطبيق متطلبات المواصفة ISO17799 بين الشركات قيد البحث.

خامسا: أداة البحث

بداية فقد وقع الاختيار لميدان البحث على الشركات العاملة في مجال المعلومات والاتصالات، وهما شركة اللقاء نت، وشركة Speed Way لخدمات الانترنت، وهما من اكبر الشركات العاملة في هذا المجال خدمات الانترنت في مدينة كركوك.

واعتمد البحث على استمارة استبانه مصممة لغرض إكمال الجانب الميداني للبحث واختبار الفرضيات، وتضمنت الاستمارة (٤٣) فقرة تتمحور حول متطلبات المواصفة الدولية ISO17799 للتعرف على مدى تطبيق الشركات قيد البحث للمواصفة من خلال متطلباتها، وقد تم توزيع (١٢) استمارة في كل شركة، ومن ثم استرجاع استمارة واحدة فقط من كل شركة، والسبب في ذلك إن هذه المتطلبات هي قياسية, ويتم الاتفاق على الإجابات من قبل المبحوثين لتكون الإجابة موحدة في كل شركة على حدا، وقد تم قياس مدى توافر هذه المتطلبات من خلال استخدام المقياس الثلاثي (درجة عالية، درجة متوسطة، درجة منخفضة)، مع إعطاء الوزن (٣) لفقرة متوفر بدرجة عالية، والوزن (٢) لفقرة متوفر بدرجة متوسطة، والوزن (١) لفقرة متوفر بدرجة منخفضة، أما احتساب معدل الإجابات في الاستمارة فقد تم من خلال المعادلة الآتية:

المعدل = مجموع النتيجة / التكرارات

أما النسبة المئوية للإجابات في القائمة فقد تم احتسابها من خلال المعادلة الآتية:

النسبة المئوية = مجموع النتيجة / ن × أعلى وزن

حيث يشير **(ن)** إلى عدد الأسئلة

المحور الثاني: الإطار النظري

أولا : مفهوم امن المعلومات

إن اعتماد المنظمات على تقنية المعلومات قد زادت بشكل كبير، وقد أصبحت المعلومات خلال السنوات الأخيرة رصيدا استراتيجيا، في حين أصبحت نظم المعلومات المحسوبة الأدوات الإستراتيجية النهائية لكل من الحكومة والمنظمات (Koskosas&et. al,2011,192)، وان هذا التطور التقني في مجال المعلومات قد زال الكثير من الصعوبات والعوائق التي كانت تعيق عمل منظمات الأعمال المختلفة، وذلك لما تتميز به هذه التقنية من مزايا السرعة والدقة والكلفة في تبادل ونقل المعلومات، ألا إن الوجه الآخر لهذه التقنية تحمل في طياتها بعض المخاطر التي يمكن أن تهددها وتهدد معلوماتها، وبسبب العولمة والتنافس ازدادت أهمية إدارة المعلومات من اجل انجاز الأنشطة وصنع القرارات، وفي الواقع غيرت الكثير من المنظمات هياكلها التنظيمية, والإدارية وكذلك أنماط العمل فيها من أجل تعزيز تقنية المعلومات فيها، وان الظواهر الاقتصادية والتكنولوجية، كالتعهيد (الاستعانة بمصادر خارجية)، واستخدام تقنية الخادم / الزبون،والخدمات المصرفية الإلكترونية، كلها تهدف إلى جعل منظمات أصغر حجما وأكثر كفاءة (Debar & Viinikka,2006,417).

من هنا أصبح موضوع امن المعلومات من المواضيع التي تتوجه إليها الأنظار، ويحاول المختصون البحث عن كافة الوسائل لضمان امن وسلامة هذه المعلومات، إن امن المعلومات يهدف إلى حماية المعلومات من التهديدات، أو أية إضرار يمكن أن تصيب هذه المعلومات, وتؤثر على استمرارية العمل في المنظمة،

ويتحقق امن المعلومات من خلال تطبيق وتنفيذ سلسلة من الإجراءات والضوابط والسياسات لحماية هذه المعلومات (Poole,2006,2)، ويوضح (Grippo&Siegel) إن امن المعلومات يتضمن التوجه نحو تحقيق سرية المعلومات، وسلامتها وتكاملها، إضافة إلى استمرارية توافرها وجاهزيتها (Grippo&Siegel, 2001,16)، وعلى هذا الأساس فإن تعزيز الثقة والأمن في استعمال تقنية المعلومات والاتصالات سوف يعزز إطار الطمأنينة الذي يشمل أمن المعلومات, وأمن الشبكات, وضمان الخصوصية والسرية, وحماية الفرد المستخدم، ويعتبر شرطا مسبقا لإنشاء مشاريع الحكومة الإلكترونية لتنمية مجتمع المعلومات, وبناء الثقة بين مستخدمي تقنية المعلومات والاتصالات، ويمثل أمن المعلومات مقاييس الرقابة الإدارية الجيدة، وعند وجود أي قصور في أحد المستويات يمكن أن يهدد كل المستويات الأخرى، على سبيل المثال، إذا كانت سياسات أمن الأفراد غير متضمنة وبالتالي غير منفذة يصبح أمن المعلومات باهظ التكلفة, أو على الأقل غير ممكن مساندته، ومن جهة أخرى يجب أن تؤكد المقاييس المخططة لكل المستويات حدا أدنى من حماية المعلومات على أن تكون مخاطر الأمن محسوبة ومقبولة من قبل الإدارة المعنية(Conner & et. al 2004,4).

ثانيا: مخاطر امن المعلومات

تتعرض المعلومات في المنظمة وخاصة المنظمات التي تتطلب طبيعة عملها استخدام شبكات الاتصالات لنقل وتبادل المعلومات الداخلية والخارجية، ويمكن إيجاز المخاطر التي يمكن أن تتعرض لها المعلومات بالاتي:(Debar & Viinikka,2006,418) (Poole,2006,4)

١. الفيروسات:

الفيروس هو برنامج صغير مكتوب بأحد لغات الحاسب ويقوم بإحداث أضرار في الحاسب والمعلومات الموجودة على الحاسب بمعنى انه يتركز علي ثلاث

خواص وهي التخفي، التضاعف، وإلحاق الأذى، وتتعدد مصادر الفيروسات فقد تأتي من خلال الرسائل الإلكترونية المجهولة، أو صفحات الإنترنت المشبوهة، أو نسخ البرامج المقلدة، أو استخدام برامج غير موثقة، كذلك تبادل وسائل التخزين دون عمل فحص مسبق مثل الأقراص والذاكرة المتنقلة, وإرسال الملفات داخل الشبكة المحلية.

٢. مهاجمة المعلومات المتناقلة:

وهو اعتراض المعلومات عند إرسالها من جهة إلى أخرى، ويحدث هذا التعامل غالباً أثناء تبادل الرسائل خلال شبكات الاتصال كشبكة الإنترنت والانترانت، وشبكة الاكسترانت، لاسيما معلومات البريد الالكتروني فقد تتعرض لخروقات جسيمة من سرقة أو تغيير أو تشويش.

٣. الدخول إلى المواقع المحجوبة:

يحاول بعض المخترقين الوصول الى المواقع المحجوبة بواسطة شبكة الانترنت باستخدام بعض البرامج، والتي عادة ما تكون مواقع مهمة تعرض المنظمة لخسائر

جسيمة نتيجة الوصول إلى هذه المواقع وتسريب المعلومات التي فيها.

٤. خطر التجسس:

التجسس أو التنصت وكشف سرية المعلومات الحساسة، وتعد من اخطر

التهديدات التي يمكن أن تتعرض لها المعلومات في المنظمة، حيث تحاول المنظمات المتنافسة الوصول إلى معلومات المنافسين بشتى الوسائل، بالإضافة إلى الأهداف الأخرى للتجسس، لاسيما في ظل عصر تقنيات المعلومات التي تستبيح الحدود بالاعتماد على الأقمار الصناعية.

٥. الاحتيال الالكتروني:

وتشمل الغش والتزوير وجرائم الصفقات التجارية الكاذبة وسرقة واختلاس الأموال، وكل ما يزعزع الكيان المالي للمنظمة، حيث ينتحل مرتكب هذه الجرائم صفة شركة معينة، أو جهة تجارية وهمية والقيام بمشاريع غير موجودة في الواقع من اجل جمع الأموال من جهات مختلفة عن طريق الاتصال الغير المباشر بين أطراف الصفقة.

ثالثا: حوكمة امن المعلومات

قبل الدخول في تفاصيل حوكمة امن المعلومات لابد من التعرف على مفهوم الحوكمة، ودواعي ظهورها والتي شملت مختلف المجالات في المنظمة منها امن المعلومات، إذ يمكن القول أن مصطلح حوكمة المنظمات ظهرت نتيجة الكثير من الإخفاقات التي لحقت بها على مستوى العالم، كمشاكل الصراع بين الإدارة والمالكين، إذ كان الباحثان Means &Berls أول من تحدثا عن مشاكل فصل الملكية عن الإدارة جراء بعض الممارسات السلبية التي من الممكن أن تحدث من قبل الطرفين؛ لأن كل طرف يسعى إلى تعظيم مصالحه وأحياناً على حساب الآخر بعيداً عن قواعد الأخلاقيات المهنية، علماً أن أساس المشكلة يتعلق بنقص المعلومات والتلاعب بها، عليه ظهرت نظرية الوكالة التي يمكن وصف المنظمة من خلالها على أنها مجموعة من العلاقات بين الأطراف ذوي المصالح المشتركة فيها التي ترتكز على فرضيتين أساسيتين هما: (Wolk, et. al., 2001,101) :

١. إن الموكل (حملة الأسهم) والوكيل (الإدارة) هم أشخاص يتميزون بالوعي، بمعنى أن كل طرف يعرف مصلحته، لذا يسعى إلى تعظيم منافعه المتوقعة، وهذه المنافع هي التي ستحدد تصرفات وقرارات كل طرف.

٢. تأسيساً على ما سبق ستسعى الإدارة إلى تعظيم منفعته حتى ولو كان ذلك على حساب مصلحة حملة الأسهم، ومن هنا سينشأ نوع من تضارب المصالح بين الأطراف.

وعلى ذلك تهدف قواعد وضوابط الحوكمة إلى تحقيق الشفافية والعدالة، ومنح حق مساءلة إدارة المنظمة، ومن ثم تحقيق الحماية للمساهمين وأصحاب المصالح جميعاً، مع مراعاة مصالح العمل والعمال، والحد من استغلال السلطة في غير المصلحة العامة، بما يؤدى إلى تنمية الاستثمار وتشجيع تدفقه، وتنمية المدخرات، وتعظيم الربحية، وإتاحة فرص عمل جديدة، (Fawzy,2003,7)، ويمكن القول إن حوكمة المنظمة تشير إلى "سلسلة من الأفعال والوظائف والتغيرات التي يمكن أن تؤدي إلى نتائج إيجابية، لذلك فإن الحوكمة هي: عملية تأسيس تشمل المسؤوليات والسلطات والاتصالات والمعايير والقياس والسياسات وآليات الرقابة؛ لتمكين الأفراد من تنفيذ الأنشطة في المنظمة" (Mueller, et.al.,2008,3)، إن حوكمة المنظمة يمكن عكسها أو تطبيقها على امن المعلومات ليتم حوكمتها، حيث إن التطبيق والالتزام بالسياسات والإجراءات الأمنية الخاصة بحماية المعلومات ما هي إلا طريق نحو حوكمة هذه المعلومات، إذا يشير كل من (Eslami,et.al.,2008,75) إلى أن الجوانب الأمنية الخاصة بالأفراد العاملين تعد مهمة حالها حال بقية الموارد في المنظمة، ويتم ذلك من خلال الدورات التدريبية لرفع مستوى الوعي لدى الأفراد حول أنظمة الأمن في المنظمة، وان الهدف الرئيس من تنظيم المعلومات هو أولاً لإدارة أمن المعلومات في المنظمة بالتنسيق الأمني للمعلومات، وتوزيع مسؤولية أمن المعلومات، أما الهدف الآخر فهو المحافظة على أمن المعلومات والوصول إليها، وان حماية الأبنية والأجهزة التي يمكن أن تتعرض لهجمات مختلفة لتخريبها أو سرقتها، أو من مخاطر الحريق

والفيضانات، عبر اتخاذ بعض الإجراءات الأمنية كوضع الأقفال على الأبواب، وأجهزة الإنذار وغيرها من الإجراءات ما هي إلا طريقة لحوكمة امن المعلومات.

كما إن حوكمة امن المعلومات يمكن أن تتحقق من خلال التوجه حوكمة تقنية المعلومات؛ لان معظم المعلومات يتم نقلها وخزنها واسترجاعها بالاعتماد على هذه التقنيات، إذا لابد من توفير البيئة الآمنة لتقنية المعلومات بحيث تكون خاضعة للسيطرة والرقابة؛ لأنه وعلى الرغم من المزايا والفوائد التي تحققها المنظمة نتيجة لاستخدام تلك التقنية فإن هناك العديد من المخاطر المتعلقة بها والتي تتسبب بآثار سلبية للمنظمة من خلال تعرض المعلومات للمخاطر المختلفة (Abu Khadra, et.al.,2009)، مما استدعى الحقل الجديد من التفكير ضرورة حوكمة تقنية المعلومات كما هي الحال في حوكمة الأعمال بوساطة الممارسات التي تضمن الاستخدام الأمثل لموارد تقنية المعلومات في المنظمة، ويتم إدارة المخاطر التي يمكن أن تتعرض لها بشكل جيد، فضلاً عن دعم التقنية لأهداف الأعمال (Schwarz & Hirschheim,2003,130).

أخيرا يمكن أن نقول إن حوكمة امن المعلومات هي: تطبيق مجموعة من المتطلبات والإجراءات والقواعد والالتزام بها من اجل ضمان امن وسلامة المعلومات في المنظمة، وحمايتها من التهديدات الداخلية والخارجية سوءا كانت متعمدة أو غير متعمدة.

رابعاً: المواصفة العالمية لحوكمة امن المعلومات ISO17799

هذه المواصفة هي نظيرة للمواصفة البريطانية BS7799، والمستمدة من المبادرة الصناعية في عام ١٩٩٣، وتعرف هذه المواصفة أيضاً بالمواصفة ISO27002، و، وتحدد هذه المواصفة حوالي ١٣٤ من الضوابط أو المتطلبات الأمنية (Kritzinger&et. al,2003, 127)، إن التغيرات البيئية المستمرة تتطلب ضرورة المراقبة المستمرة للأعمال من قبل المنظمات، إذ تركز هذه

المواصفة على إدارة المخاطر وتقديرها(Poole,2006,2)، حيث تعد هذه المواصفة دليلاً لتطبيق مجموعة من السياسات والأساليب والإجراءات والممارسات لدعم إدارة أمن المعلومات في المنظمة (Eslami&et. al,2008,75)، وتم إصدار هذه المواصفة من قبل المنظمة الدولية للتقييس ISO (International Standards For Organization) في العام ٢٠٠٠ تحت تسمية ISO17799، وتعد وثيقة توجيهية للمنظمات نحو هيكلية لإدارة أمن المعلومات (Solms& Solms,2009,43). وهناك ثلاثة متطلبات أساسية للمواصفة ISO17799، وكما يأتي :

١- فحص مخاطر امن معلومات بشكل منظم, ويتم هذا الفحص من خلال حساب التهديدات ونقاط الضعف.

٢- التصاميم والأدوات متماسكة وشاملة للسيطرة على امن المعلومات والأشكال الأخرى من معالجة المخاطر (مثل تجنب الخطر او نقل الخطر) لتوجيه تلك المخاطر التي يعتقد بأنها غير مقبولة.

٣- تبنى عملية إدارة الانحرافات لضمان استمرارية السيطرة على امن المعلومات لمقابلة احتياجات امن معلومات المنظمة بشكل متقدم.

وتتضمن المواصفة العالمية لأمن المعلومات ISO17799 أفضل الممارسات في المراقبة وفي السياسات والضوابط التي تُتبع في إدارة امن المعلومات،وقد حدد (Gheorghe,2010,34) (Eslami&et. al,2008,75) المتطلبات أو الممارسات الرئيسة لهذه المواصفة بالآتي:

١- تقييم المخاطر:

يتم تقييم المخاطر التي من الممكن أن تتعرض لها المنظمة، كالمخاطر التي

قد تؤثر على بعض المعلومات المهمة في المنظمة، أو على الأفراد العاملين، أو ممتلكاتها ويكون هذا التقييم بناء على اعتبارين رئيسين وهما:

- ✓ تحديد مدى تأثير هذه المخاطر على المنظمة: إذ إن هذه المخاطر من المؤكد أن يكون لها تأثير سلبي، ولكن مدى تأثير هذه المخاطر يظهر من خلال الخسائر التي تتحملها المنظمة.
- ✓ احتمالية حدوث هذه المخاطر في المنظمة: فإذا كانت نسبة حدوثه قليلة جداً يتم تجاهل هذا الخطر، إذ تستفيد المنظمة من هذه النتائج في تحديد الإجراءات المناسبة التي تتبعها في إدارة امن المعلومات وعمل لوائح وقوانين تساعدها في حماية نفسها من هذه المخاطر, مثلا إذا كانت المخاطر التي ممكن أن تتعرض لها المنظمة هي سرقة معلومات عن رواتب الموظفين فالمنظمة تتخذ إجراء يناسب هذا الخطر.

٢ – السياسات الأمنية:

هي مجموعه من المعايير والأنظمة التي تقوم بتطبيقها المنظمة لحماية معلوماتها ومرافقها من خلال فرض قوانين وقواعد تلزم المنظمة من خلالها الأفراد العاملين على إتباعها, ومن خلال السياسات الأمنية يمكن التوصية بما يلي:

- ✓ إنشاء منتدى لأمن المعلومات على مستوي الإدارة العليا في المنظمة.
- ✓ تقديم حملات وبرامج للتوعية والتدريب على أمن المعلومات.
- ✓ إدارة المخاطرة كمدخل من مداخل العملية الإدارية في المنظمة.
- ✓ التوافق مع القوانين والتشريعات الملائمة.

وعلى هذا الأساس، فإن أية وثيقة أو تقرير لسياسة أمن المعلومات يجب أن تتضمن التالي:

- ✓ حاجة المنظمة لخطة طوارئ.
- ✓ الحاجة لمساندة حفظ البيانات والمعلومات بفعالية وكفاءة.
- ✓ تجنب البرمجيات المصابة.
- ✓ توفير إجراءات رقابة للوصول للمعلومات.
- ✓ تقرير بالأحداث التي تتعرض لها المنظمة فيما يخص أمن معلوماتها.
- ✓ تحديد الإجراءات المطلوب اتخاذها عند حدوث عدم التوافق مع السياسة من حيث النشاط المصاب، أو الاستخدام غير المناسب.

٣- تنظيم امن المعلومات:

إن الهدف الرئيسي من تنظيم امن المعلومات في المنظمة يعود لأمرين أساسيين:

١- إدارة امن المعلومات داخل المنظمة ويكون من خلال عدة أمور:

- ✓ التنسيق الأمني للمعلومات حيث إن حماية المعلومات تكون مسؤولية مشتركة بين الأفراد العاملين في المنظمة الذين يتعاملون مع هذه المعلومات مثل المعلومات الخاصة برواتب الأفراد تكون مسؤولية حمايتها مشتركة بين جميع الأفراد العاملين في قسم المحاسبة.
- ✓ توزيع مسؤولية امن المعلومات وذلك عن طريق تحديد المعلومات التي تتطلب حمايتها، كذلك تحديد الأفراد المسؤولين عن حماية هذه المعلومات.

٢- المحافظة على امن المعلومات ومرافق المعلومات التي يتم الوصول إليها من قبل أطراف خارج المنظمة كالمتعهدين مع المنظمة لإنجاز مشروع معين لفترة زمنية محددة، وذلك من خلال:

- ✓ تحديد المخاطر التي من الممكن ان تتعرض لها المنظمة من الأطراف الخارجية.
- ✓ معالجة الأمن عند التعامل مع العملاء من خلال تحديد المتطلبات الأمنية التي ينبغي معالجتها قبل السماح للعملاء من الوصول إلى معلومات المنظمة.

٤ – إدارة الموجودات:

يهدف هذا المتطلب تعريف مجال إدارة أمن المعلومات والتأكيد أن موجودات المعلومات قد أعطيت مستوى ملائم من الحماية، إذ إن الموجودات هي كل شيء لها قيمة في المنظمة سواء كانت هذه الموجودات مادية (مثل قاعدة بيانات المنظمة أو الوسائط القابلة للإزالة)، أو الموجودات غير المادية مثل سمعة المنظمة، وان إدارة الموجودات تكون من خلال حصرها، وتحديد مَن المسؤول عن حمايتها، وما أهمية هذه الموجودات بالنسبة للمنظمة، وهل حماية هذه الموجودات كافية مقابل أهميتها بالنسبة للمنظمة.

والمنظمة التي تطبق معيار ISO 17799 تقرر أي من موجودات المعلومات يكون لها تأثير على تشغيل وإتاحة أنشطة المنظمة أو العمل، ويتطلب ذلك تحليل احتمالية تقرير المخاطرة.

٥ – امن الموارد البشرية:

إن الجوانب الأمنية والمسؤوليات المتعلقة بالأفراد العاملين والمتعاقدين والمستخدمين يجب أن تكون محددة وموثقة تبعا للسياسات الأمنية وخصوصية المعلومات بالنسبة للمنظمة, كالتأكد من إن الموجودات أو المعلومات المهمة محمية من خلال المحافظة عليها من السرقة أو إساءة الاستعمال أو الكشف والتعديل غير المصرح به من قبل الغير المخولين، كذلك امن الموارد البشرية يكون

من خلال إقامة المنظمة دورات تدريبية لزيادة وعي الأفراد تجاه الأمن في المنظمة، ووضع عقوبات بحق المخالفين لأنظمة الأمن في المنظمة، وتقليل الأعطال والأضرار التي تسبب القصور في أداء الأمن بالإضافة إلى التعلم من هذه الأحداث، ويمكن تحديد المهام المطلوب اتخاذها لتلبية هذا المتطلب بالاتي:

١. تضمين اعتبارات ومسئوليات الأمن في توصيف الوظائف وإعداد عقودهم.

٢. تدريب المستخدمين النهائيين.

٣. تحديد تهديدات ومزاولات الاستجابة في حالات العجز عن الأداء وأحداث الأمن.

٦- الأمن المادي والبيئي:

فالمقصود فيه أن يقوم بحماية المعلومات المهمة عن طريق منع المهاجمين من الوصول إليها أو سرقتها أو تخريبها, وكذلك حماية مرافق, وموارد المنظمة مثل المباني والأنظمة، وقاعدة بيانات المنظمة، والوسائط المادية التي تخزن عليها معلومات المنظمة المهمة من التعرض للمخاطر مثل الحرائق، ويمكن تطبيقه عن طريق وضع أقفال على الأبواب أو حراس امن لمنع الوصول إلى موجودات المنظمة لسرقتها أو تخريبها أو وضع أجهزة إنذار ضد الحريق للحماية من خطر احتراق المبنى

٧- إدارة استمرارية الأعمال:

من خلال وضع خطط تتبعها المنظمة عند حدوث مشاكل غير متوقعه او لم تتمكن المنظمة من التصدي لها لضمان استمرارية العمل أو تقليل تأثير هذه المشاكل قدر الإمكان، ويهدف هذا البعد أيضا إلى التخلص من تعارض العمليات وتوقفها، وحماية العمليات الحرجة من الأعطال والفشل والكوارث المختلفة، وفي هذا الإطار يمكن تمييز ثلاث أنشطة أساسية هي:

- ✓ استعادة سيناريوهات المخاطر التي يمر بها النظام وسبل التغلب عليها، ويمثل ذلك مسؤولية الأطراف المختلفة التي يتعامل معها أمن النظام وتقدم الاتصالات وإدارة العمليات الفنية الأساسية التي يعتمد عليها استخدامات الآخرين عن بعد.
- ✓ استمرارية الأعمال يمثل المستوي الثاني الخاص باستمرار أداء الأنشطة الأساسية والمفسرة جيدا من موقع لآخر، ويحدد ذلك مسؤولية الإدارة العليا وعدد الإفراد العاملين المطلوب الوصول إليهم على أن يكونوا مستعدين للقيام بهذه المسئوليات عندما يطلب منهم ذلك.
- ✓ إدارة الأزمات التي تعتبر من مسؤوليات الإدارة العليا، وتتضمن الاتصال مع كل الأطراف الخاصة والمهتمة بأعمال الأمن عند حدوث الأزمات المختلفة.

٨- التحكم في الوصول:

إن الهدف من التحكم في الوصول هو تقييد وصول الأفراد الغير المخولين في المنظمة إلى الشبكات والأنظمة والتطبيقات والمعلومات السرية للمنظمة, واكتشاف الأنشطة الضارة المتعمدة، والتحكم في الوصول يكون من خلال تحديد المنظمة صلاحيات الوصول لكل شخص إلى معلوماتها مثلا حسابات وأرصدة العملاء لا يمكن الاطلاع عليها إلا من قبل أفراد محدودين في المصرف، ويمكن تحديد الأنشطة العادية المصاحبة للرقابة والتحكم على الوصول بالتالي:

- ✓ تفسير متطلبات الرقابة علي الوصول (التركيز علي السرية والخصوصية).
- ✓ إدارة حقوق وصول المستخدمين الفردية.
- ✓ تفسير مسئوليات المستخدمين الفردية.
- ✓ تفسير الآليات الملائمة للوصول لشبكة المعلومات.

- ✓ تحديد السياسات والإجراءات المختلفة لمراجعة الوصول إلى النظام واستخدامه.

٩- تطوير نظم المعلومات وصيانتها:

من خلال إدخال تحسينات جديدة على موجودات المنظمة، خاصة في ظل التطور المتسارع في مجال تقنية المعلومات والشبكات، كذلك إجراء الصيانة اللازمة عند حدوث العطلات أو الخروقات الأمنية.

١٠- التوافق:

وهو ضمان التوافق مع سياسات وقوانين ولوائح امن المعلومات، وبذلك تعد حوكمة تقنية المعلومات رمزا لأفضل الممارسات التي تقوم عليها إدارة تقنية المعلومات، حيث تمثل دليلا لتطبيق مجموعة من السياسات, والإجراءات لكي تدعم امن المعلومات التي تدار من لدن المنظمة, وان تطبيق هذا المعيار يمثل ميزة تنافسية؛ لأية منظمة تضمن من خلالها امن معلوماتها.

المحور الثالث: الإطار الميداني للبحث

يتضمن الإطار الميداني للبحث اختبار فرضيات البحث بالاعتماد على البيانات التي تم جمعها من الشركات المبحوثة، حيث سيتم مقارنة مدى تطبيق, واعتماد حوكمة امن المعلومات من قبل الشركتين بالاعتماد على كل متطلب من متطلبات المواصفة ISO 17799، وستتم مقارنة كل متطلب من هذه المتطلبات في الشريكتين على حدا بالتفصيل، وكما يلي:

١- تقييم المخاطر:

يعد تقييم المخاطر متطلبا ضرورياً لابد للشركة أخذها بالاعتبار، وذلك من اجل تحديد نوعية هذه المخاطر، وإمكانية تجنبها، ومدى تأثيرها على معلومات الشركة فيما إذا وقعت فعلا، من هنا فقد أظهرت النتائج إن شركة اللقاء نت تطبق

هذا المتطلب بصورة جيدة، حيث بلغ معدل تطبيق أو الالتزام بهذا المتطلب (٢,٥) درجة، وكانت نسبة تطبيقها في هذه الشركة (٨٣%) وهي نسبة عالية، وكما موضح في الجدول(١).

الجدول (١) المعدلات والنسب المئوية لمتطلب تقييم المخاطر في شركة اللقاء نت

ت	الفقرات	بدرجة منخفضة	بدرجة متوسطة	بدرجة عالية
١	المتابعة والدراسة المستمرة للمخاطر التي يمكن ان تتعرض لها معلومات الشركة			*
٢	الآليات المستخدمة في تحديد المخاطر التي تهدد امن المعلومات الخاصة بالشركة		*	
٣	تقييم درجة أهمية المخاطر التي يمكن أن تتعرض لها المعلومات		*	
٤	تصنيف المخاطر التي يمكن أن تتعرض لها المعلومات حسب أهميتها			*
	الأوزان	١	٢	٣
	التكرارات	٠	٢	٢
	النتيجة	٠	٤	٦
	المعدل	٢,٥		
	النسبة المئوية	%٨٣		

المصدر: الجدول من إعداد الباحثان بالاعتماد على نتائج تحليل البيانات

أما شركة Speed Way فأنها تولي اهتماما خاصا لهذا المتطلب وكما يظهره الجدول (٢)، حيث بلغ معدل الالتزام بتقييم المخاطر ومتابعتها (٣) درجات، وما يدعم هذا المعدل نسبة التطبيق البالغة (١٠٠%)، حيث يتم دراسة ومتابعة المخاطر بصورة مستمرة، فضلا عن تقييم درجة أهمية المخاطر التي يمكن أن تتعرض لها المعلومات، وتصنيفها حسب أهميتها في الشركة، إذا ومن خلال

ملاحظة النتائج يتضح ان شركة Speed Way هي الأفضل من حيث تطبيق هذا المتطلب إذا ما قورنت مع شركة اللقاء نت.

الجدول (٢) المعدلات والنسب المئوية لمتطلب تقييم المخاطر في شركة Speed Way

ت	الفقرات	بدرجة منخفضة	بدرجة متوسطة	بدرجة عالية
١	المتابعة والدراسة المستمرة للمخاطر التي يمكن أن تتعرض لها معلومات الشركة			*
٢	الآليات المستخدمة في تحديد المخاطر التي تهدد امن المعلومات الخاصة بالشركة			*
٣	تقييم درجة أهمية المخاطر التي يمكن أن تتعرض لها المعلومات			*
٤	تصنيف المخاطر التي يمكن أن تتعرض لها المعلومات حسب أهميتها			*
	الأوزان	١	٢	٣
	التكرارات	٠	٠	٤
	النتيجة	٠	٠	١٢
	المعدل	٣		
	النسبة المئوية	%١٠٠		

المصدر: الجدول من إعداد الباحثان بالاعتماد على نتائج تحليل البيانات

٢- السياسات الأمنية:

لابد من وضع معايير وأنظمة تقوم بتطبيقها الشركة لحماية معلوماتها ومرافقها من خلال فرض قوانين وقواعد تلزم إدارة الشركة من خلالها الموظفين على إتباعها، ومن خلال متابعة النتائج تبين أن معدل الالتزام بالسياسات والإجراءات الأمنية من

قبل شركة اللقاء نت كان بالمستوى المطلوب، حيث بلغ المعدل (٢,٧) درجة، وكانت نسبة تطبيق هذا المتطلب من قبل الشركة المذكورة (٩٠%)، ويتضح من خلال الجدول أيضا إن ما يدعم النسبة السابقة هو تأكيد إدارة الشركة على منع استخدام البرامج الغير أمنة والتي قد تعرض المعلومات إلى بعض المخاطر، وكما موضح في الجدول (٣).

الجدول (٣) المعدلات والنسب المئوية لمتطلب السياسات الأمنية في شركة اللقاء نت

ت	الفقرات	بدرجة منخفضة	بدرجة متوسطة	بدرجة عالية
٥	القواعد والقوانين اللازمة إتباعها من قبل الموظفين لحماية امن المعلومات (كعدد حروف الرقم السري)			*
٦	خطة طوارئ لمعالجة الحالات الطارئة التي تواجه المعلومات في الشركة			*
٧	القيود اللازمة لمنع وصول الموظفين الغير المخولين إلى المعلومات الحساسة			*
٨	حفظ المعلومات باستخدام طرق متطورة وآمنة			*
٩	إجراءات منع استخدام بعض البرامج الغير الآمنة في الشركة		*	
١٠	التوافق مع القوانين والتشريعات الخاصة ببعض المعلومات الخاصة		*	
١١	تقرير بالأحداث التي تتعرض لها المعلومات في الشركة			*
	الأوزان	١	٢	٣
	التكرارات	٠	٢	٥
	النتيجة	٠	٤	١٥
	المعدل	٢,٧		
	النسبة المئوية	%٩٠		

المصدر: الجدول من إعداد الباحثان بالاعتماد على نتائج تحليل البيانات

أما تطبيق هذا المتطلب من قبل شركة Speed Way فقد كان مقاربا لشركة اللقاء نت، حيث بلغ معدله (٢,٨) درجة، وما يدعم هذا المعدل نسبة تطبيقه البالغة (٩٣%)، وكما موضح في الجدول (٤)، حيث تركز إدارة الشركة على وضع بعض القوانين والقواعد الواجب إتباعها من قبل الموظفين فيها، ووجود خطة للحالات الطارئة في المعلومات، إضافة إلى تحديد الوصول إلى بعض المعلومات السرية، ورفع التقارير للحوادث التي تحصل في الشركة والخاصة بالمعلومات وأمنها، أي: إن الشركتان لهما نفس التوجه نحو الالتزام بالسياسات, والإجراءات الأمنية التي تدعم امن وسلامة معلوماتها، خصوصا إن طبيعة عمل هذه الشركات تعتمد على المعلومات في الأساس.

الجدول (٤) المعدلات والنسب المئوية لمتطلب السياسات الأمنية في شركة Speed Way

ت	الفقرات	بدرجة منخفضة	بدرجة متوسطة	بدرجة عالية
٥	القواعد والقوانين اللازمة إتباعها من قبل الموظفين لحماية امن المعلومات (كعدد حروف الرقم السري)			*
٦	خطة طوارئ لمعالجة الحالات الطارئة التي تواجه المعلومات في الشركة			*
٧	القيود اللازمة لمنع وصول الموظفين الغير المخولين إلى المعلومات الحساسة			*
٨	حفظ المعلومات باستخدام طرق متطورة وآمنة			*
٩	إجراءات منع استخدام بعض البرامج الغير الآمنة في الشركة			*

١٠	التوافق مع القوانين والتشريعات الخاصة ببعض المعلومات الخاصة		*	
١١	تقرير بالأحداث التي تتعرض لها المعلومات في الشركة			*
	الأوزان	١	٢	٣
	التكرارات	٠	١	٦
	النتيجة	٠	٢	١٨
	المعدل	٢,٨		
	النسبة المئوية	%٩٣		

المصدر: الجدول من إعداد الباحثان بالاعتماد على نتائج تحليل البيانات

٣- تنظيم امن المعلومات:

إن تنظيم امن المعلومات يتطلب إدارتها من خلال توزيع الواجبات والمسؤوليات بين الجميع لحماية هذه المعلومات، ويتضح من الجدول (٥) و(٦) إن معدل تطبيق متطلب تنظيم امن المعلومات من كلا الشركتين هو نفس المعدل والذي بلغ (٢,٥) درجة على التوالي، وكانت نسبة التطبيق في كلا الشركتين أيضا (٨٣%)، حيث يتم التأكيد على تحديد مسؤولية حماية المعلومات، ووضع إجراءات حماية المعلومات.

الجدول (٥) المعدلات والنسب المئوية لمتطلب تنظيم امن المعلومات في شركة اللقاء نت

ت	الفقرات	بدرجة منخفضة	بدرجة متوسطة	بدرجة عالية
١٢	التنسيق الأمني بين الفروع لحماية امن المعلومات المختلفة			*

١٣	تحديد مسؤولية حماية المعلومات حسب نوعها في فروع الشركة		*	
١٤	الإجراءات المتخذة لحماية المعلومات من الجهات الخارجية عند التعامل معها كالمتعهدين			*
١٥	إجراءات حماية معلومات الشركة من خطر بعض عملاء الشركة		*	
الأوزان		١	٢	٣
التكرارات		٠	٢	٢
النتيجة		٠	٤	٦
المعدل		٢,٥		
النسبة المئوية		%٨٣		

المصدر: الجدول من إعداد الباحثان بالاعتماد على نتائج تحليل البيانات

الجدول (٦) المعدلات والنسب المئوية لمتطلب تنظيم امن المعلومات في شركةSpeed Way

ت	الفقرات	بدرجة منخفضة	بدرجة متوسطة	بدرجة عالية
١٢	التنسيق الأمني بين الفروع لحماية امن المعلومات المختلفة			*
١٣	تحديد مسؤولية حماية المعلومات حسب نوعها في فروع الشركة			*
١٤	الإجراءات المتخذة لحماية المعلومات من الجهات الخارجية عند التعامل معها كالمتعهدين		*	
١٥	إجراءات حماية معلومات الشركة من خطر بعض عملاء الشركة		*	
الأوزان		١	٢	٣

التكرارات	٠	٢	٢
النتيجة	٠	٤	٦
المعدل	٢,٥		
النسبة المئوية	%٨٣		

المصدر: الجدول من إعداد الباحثان بالاعتماد على نتائج تحليل البيانات

٤-إدارة الموجودات:

يعد هذا المتطلب من المتطلبات المهمة في المواصفة ISO 17799 ، حيث تشير نتائج تحليل البيانات وكما موضح في الجدول (٧) إلى إن شركة اللقاء نت تتجه نحو تطبيق هذا المتطلب من خلال تحديد الموجودات, والمسؤولين عنها، إضافة إلى تحديد مسؤولية حمايتها، إذ بلغ معدل تطبيق هذا المتطلب (٢) درجة، وجاءت بنسبة (٦٧%).

الجدول (٧) المعدلات والنسب المئوية لمتطلب إدارة الموجودات في شركة اللقاء نت

ت	الفقرات	بدرجة منخفضة	بدرجة متوسطة	بدرجة عالية
١٦	تحديد الموجودات المعلوماتية المادية والغير المادية بدقة في الشركة		*	
١٧	تحديد المسؤول عن كل موجود في فروع الشركة		*	
١٨	تحديد مسؤولية حماية كل موجود معلوماتي (كقاعدة البيانات) في الشركة			*
١٩	تشخيص وتحليل المخاطر الأمنية التي يمكن ان تتعرض لها هذه الموجودات	*		
الأوزان		١	٢	٣
التكرارات		١	٢	١
النتيجة		١	٤	٣
المعدل		٢		

النسبة المئوية	%٦٧

المصدر: الجدول من إعداد الباحثان بالاعتماد على نتائج تحليل البيانات

أما شركة Speed Way وكما يظهر الجدول (٨) فإنها تطبق هذا المتطلب بالتفصيل، حيث بلغ معدله (٣) درجات، اي بنسبة تطبيق قدره (١٠٠%)، وهذا يدل إن هذه الشركة تهتم بهذا المتطلب أكثر من شركة اللقاء نت.

الجدول (٨) المعدلات والنسب المئوية لمتطلب إدارة الموجودات في شركة Speed Way

ت	الفقرات	بدرجة منخفضة	بدرجة متوسطة	بدرجة عالية
١٦	تحديد الموجودات المعلوماتية المادية والغير المادية بدقة في الشركة			*
١٧	تحديد المسؤول عن كل موجود في فروع الشركة			*
١٨	تحديد مسؤولية حماية كل موجود معلوماتي (كقاعدة البيانات) في الشركة			*
١٩	تشخيص وتحليل المخاطر الأمنية التي يمكن ان تتعرض لها هذه الموجودات			*
	الأوزان	١	٢	٣
	التكرارات	٠	٠	٤
	النتيجة	٠	٠	١٢
	المعدل	٣		
	النسبة المئوية	%١٠٠		

المصدر: الجدول من إعداد الباحثان بالاعتماد على نتائج تحليل البيانات

٥- امن الموارد البشرية:

تعتبر الموارد البشرية من أهم موارد الشركة لذلك لابد من الاهتمام بهذا المورد وضمان أمنها، وقد أظهرت نتائج التحليل إن شركة اللقاء نت توفر كافة

المستلزمات والاحتياجات الخاصة بحماية الموارد البشرية لديها، حيث بلغ معدل تطبيق هذا المتطلب (٢,٨) درجة، وكانت نسبة تطبيقها عالية حيث بلغت (٩٣%)، وكما موضح في الجدول (٩).

الجدول (٩) المعدلات والنسب المئوية لمتطلب امن الموارد البشرية في شركة اللقاء نت

ت	الفقرات	بدرجة منخفضة	بدرجة متوسطة	بدرجة عالية
٢٠	الإجراءات اللازمة لتوفير الأمن للموظفين في الشركة			*
٢١	الإجراءات الأمنية اللازمة لحماية الجهات الخارجية المتعاقدة مع الشركة			*
٢٢	إدخال الموظفين في دورات تدريبية لتوعيتهم ونشر ثقافة امن المعلومات بينهم		*	
٢٣	محاسبة المخالفين للأنظمة والقوانين الخاصة بأمن المعلومات			*
٢٤	توجيه الموظفين نحو السياسات الأمنية لحماية خصوصية المعلومات من التخريب			*
	الأوزان	١	٢	٣
	التكرارات	٠	١	٤
	النتيجة	٠	٢	١٢
	المعدل	٢,٨		
	النسبة المئوية	%٩٣		

المصدر: الجدول من إعداد الباحثان بالاعتماد على نتائج تحليل البيانات

يتضح من الجدول (١٠) إن شركة Speed Way تهتم بأمن الموارد البشرية التي لديها أيضا كمتطلب جوهري من متطلبات المواصفة ISO 17799، إذ بلغ

معدل تطبيق (٢,٢) درجة، وكانت نسبة تطبيقها (٧٣%)، إلَّا إن هذه النسبة تعد قليلة نسبيا إذا ما قورنت مع نسبة تطبيق هذا المتطلب من قبل شركة اللقاء.

الجدول (١٠) المعدلات والنسب المئوية لمتطلب امن الموارد البشرية في شركة Speed Way

ت	الفقرات	بدرجة منخفضة	بدرجة متوسطة	بدرجة عالية
٢٠	الإجراءات اللازمة لتوفير الأمن للموظفين في الشركة		*	
٢١	الإجراءات الأمنية اللازمة لحماية الجهات الخارجية المتعاقدة مع الشركة		*	
٢٢	إدخال الموظفين في دورات تدريبية لتوعيتهم ونشر ثقافة امن المعلومات بينهم		*	
٢٣	محاسبة المخالفين للأنظمة والقوانين الخاصة بأمن المعلومات		*	
٢٤	توجيه الموظفين نحو السياسات الأمنية لحماية خصوصية المعلومات من التخريب			*
الأوزان		١	٢	٣
التكرارات		٠	٤	١
النتيجة		٠	٨	٣
المعدل		٢,٢		
النسبة المئوية		٧٣%		

المصدر: الجدول من إعداد الباحثان بالاعتماد على نتائج تحليل البيانات

٦- الأمن المادي والبيئي:

أن توفير الأمن للبنية التحتية للشركة الهدف منها حماية المعلومات السرية والحساسة، لذلك لابد من اتخاذ جميع التدابير اللازمة لحمايتها من المخاطر، ويتضح من خلال نتائج التحليل إن كلا الشركتين قيد البحث تطبقان هذا المتطلب

بالمستوى نفسه، حيث بلغ معدل التطبيق في كلا الشركتين (٢,٨) درجة على التوالي، وبنسبة (٩٣%)، اي: لا يوجد فارق بينهما من حيث تطبيق وتنفيذ هذا المطلب في المواصفة، وكما موضح في الجدولين (١١) (١٢) على التوالي.

الجدول (١١) المعدلات والنسب المئوية لمتطلب الأمن المادي والبيئي في شركة اللقاء نت

ت	الفقرات	بدرجة منخفضة	بدرجة متوسطة	بدرجة عالية
٢٥	الإجراءات الأمنية اللازمة لحماية المباني والغرف الخاصة في الشركة من تهديدات التخريب والسرقة			*
٢٦	الإجراءات الخاصة لحماية الأنظمة والوسائط المادية التي تخزن فيها المعلومات (كقاعدة البيانات)		*	
٢٧	الإجراءات الأمنية لحماية شبكات الاتصال الخاصة بعمل الشركة			*
٢٨	إجراءات الصيانة الدورية للبنية التحتية، والشبكات، وأجهزة حفظ المعلومات			*
٢٩	التجهيزات والأجهزة اللازمة للحماية وتقليل المخاطر التي تهدد الأجهزة والمباني (كأجهزة الإنذار ضد الحريق أو الإقفال أو الكاميرات)			*
الأوزان		١	٢	٣
التكرارات		٠	١	٤
النتيجة		٠	٢	١٢
المعدل		٢,٨		
النسبة المئوية		%٩٣		

المصدر: الجدول من إعداد الباحثان بالاعتماد على نتائج تحليل البيانات

الجدول(١٢) المعدلات والنسب المئوية لمتطلب الأمن المادي والبيئي في شركة Speed Way

ت	الفقرات	بدرجة	بدرجة	بدرجة

		منخفضة	متوسطة	عالية
٢٥	الإجراءات الأمنية اللازمة لحماية المباني والغرف الخاصة في الشركة من تهديدات التخريب والسرقة			*
٢٦	الإجراءات الخاصة لحماية الأنظمة والوسائط المادية التي تخزن فيها المعلومات (كقاعدة البيانات)			*
٢٧	الإجراءات الأمنية لحماية شبكات الاتصال الخاصة بعمل الشركة			*
٢٨	إجراءات الصيانة الدورية للبنية التحتية، والشبكات، وأجهزة حفظ المعلومات			*
٢٩	التجهيزات والأجهزة اللازمة للحماية وتقليل المخاطر التي تهدد الأجهزة والمباني (كأجهزة الإنذار ضد الحريق أو الإقفال أو الكاميرات)		*	
الأوزان		١	٢	٣
التكرارات		٠	١	٤
النتيجة		٠	٢	١٢
المعدل		٢,٨		
النسبة المئوية		%٩٣		

المصدر: الجدول من إعداد الباحثان بالاعتماد على نتائج تحليل البيانات

٧- إدارة استمرارية الإعمال:

لابد من وجود متابعة مستمرة لاستمرارية الإعمال، وضمان عدم توقفها بسبب العطلات والمشاكل المتوقعة والغير المتوقعة، وتشير نتائج الجدول (١٣) إلى إن شركة اللقاء نت لديها الاهتمام الكافي لتطبيق هذا المتطلب، حيث بلغ معدل تطبيقها (٢,٦) درجة، وجاءت بنسبة عالية قدرها (٨٣%)، وما عزز هذه النسبة توفر الخطط اللازمة لمواجهة المخاطر، إضافة إلى وجود الاتصالات بين مختلف الإدارات لحل الأزمات في هذا المجال.

الجدول (١٣) المعدلات والنسب المئوية لمتطلب إدارة استمرارية الأعمال في شركة اللقاء نت

ت	الفقرات	بدرجة منخفضة	بدرجة متوسطة	بدرجة عالية
٣٠	الخطط الموضوعة لمواجهة المخاطر الغير المتوقعة في الشركة			*
٣١	متابعة عدم حدوث تعارض أو تضارب في وظائف عمل الشركة		*	
٣٢	الاتصالات اللازمة بين إدارات الفروع لمواجهة الأزمات في الشركة			*
	الأوزان	١	٢	٣
	التكرارات	٠	١	٢
	النتيجة	٠	٢	٦
	المعدل	٢,٦		
	النسبة المئوية	%٨٧		

المصدر: الجدول من إعداد الباحثان بالاعتماد على نتائج تحليل البيانات

أما تطبيق هذا المتطلب من المواصفة ISO 17799 من قبل شركة Speed Wayفكان بمعدل عالي، حيث بلغ (٣) درجة، وبنسبة تطبيق قدرها (١٠٠%)، اي إن الاهتمام بتطبيق هذا المتطلب من قبل هذه الشركة هي أفضل من شركة اللقاء نت رغم إن الأخيرة حققت نسبة جيدة أيضا، وكما في الجدول.

الجدول(١٤) المعدلات والنسب المئوية لمتطلب إدارة الاستمرارية في شركةSpeed Way

ت	الفقرات	بدرجة منخفضة	بدرجة متوسطة	بدرجة عالية
٣٠	الخطط الموضوعة لمواجهة المخاطر الغير المتوقعة في الشركة			*
٣١	متابعة عدم حدوث تعارض أو تضارب في وظائف عمل الشركة			*

٣٢	الاتصالات اللازمة بين إدارات الفروع لمواجهة الأزمات في الشركة			*
	الأوزان	١	٢	٣
	التكرارات	٠	٠	٣
	النتيجة	٠	٠	٩
	المعدل	٣		
	النسبة المئوية	%١٠٠		

المصدر: الجدول من إعداد الباحثان بالاعتماد على نتائج تحليل البيانات

٨- التحكم في الوصول:

أظهرت النتائج إن شركة اللقاء نت تولي اهتماما لتطبيق هذا المتطلب لكونه من المتطلبات المهمة في المواصفة ISO 17799، من خلال وضع إجراءات خاصة لمنع وصول الغير المخولين إلى بعض المعلومات السرية، إضافة إلى تحديد صلاحيات المخولين، حيث بلغ معدل تطبيق هذا المتطلب (٢,٦) درجة، وكانت نسبة تطبيقها (٨٧%)، وهي نسبة جيدة من التطبيق في شركة اللقاء نت.

الجدول (١٥) المعدلات والنسب المئوية لمتطلب التحكم في الوصول في شركة اللقاء نت

ت	الفقرات	بدرجة منخفضة	بدرجة متوسطة	بدرجة عالية
٣٣	إجراءات وصول الغير المخولين للوصول إلى بعض المعلومات			*
٣٤	تحديد الصلاحيات الخاصة للمخولين للوصول إلى بعض المعلومات			*
٣٥	الآليات والإجراءات المتخذة للوصول إلى شبكة معلومات الشركة		*	
	الأوزان	١	٢	٣
	التكرارات	٠	١	٢

النتيجة	٠	٢	٦
المعدل	٢,٦		
النسبة المئوية	%٨٧		

المصدر: الجدول من إعداد الباحثان بالاعتماد على نتائج تحليل البيانات

أما شركةSpeed Way فقد كانت سباقة في تطبيق وتنفيذ هذا المتطلب من المواصفة من خلال جميع تفاصيلها، إذ حققت درجة تطبيق كاملة وبالغة (٣) درجات، وبنسبة (١٠٠%)، وكما موضح في الجدول.

الجدول (١٦) المعدلات والنسب المئوية لمتطلب التحكم في الوصول لشركة Speed Way

ت	الفقرات	بدرجة منخفضة	بدرجة متوسطة	بدرجة عالية
٣٣	إجراءات وصول الغير المخولين للوصول إلى بعض المعلومات			*
٣٤	تحديد الصلاحيات الخاصة للمخولين للوصول إلى بعض المعلومات			*
٣٥	الآليات والإجراءات المتخذة للوصول إلى شبكة معلومات الشركة			*
	الأوزان	١	٢	٣
	التكرارات	٠	٠	٣
	النتيجة	٠	٠	٩
	المعدل	٣		
	النسبة المئوية	%١٠٠		

المصدر: الجدول من إعداد الباحثان بالاعتماد على نتائج تحليل البيانات

٩- تطوير نظم المعلومات وصيانتها:

لابد من إدخال تحسينات مستمرة في نظم معلومات الشركة من استخدام احدث التقنيات في هذا المجال، ويلاحظ من الجدول (١٧) إن شركة اللقاء نت

تهتم في متابعة التوقفات والعطلات وصيانتها، إضافة إلى تطوير الأجهزة والمعدات الخاصة بعملها، وهذا ما يدعم معدل تطبيقها البالغ (٢,٥) درجة، فضلا عن نسبة تطبيقها البالغة (٨٣%).

الجدول (١٧) المعدلات والنسب المئوية لمتطلب تطوير وصيانة نظم المعلومات لشركة اللقاء نت

ت	الفقرات	بدرجة منخفضة	بدرجة متوسطة	بدرجة عالية
٣٦	الخطط الخاصة لتطوير الأجهزة التقنية للمعلومات		*	
٣٧	الخطط الخاصة للأجراء الصيانة الوقائية لتقنية المعلومات		*	
٣٨	الإجراءات اللازمة لمعالجة التوقفات أو العطلات المفاجئة في تقنيات المعلومات			*
٣٩	الرقابة المستمرة لعمل تقنيات المعلومات والاتصالات في الشركة			*
	الأوزان	١	٢	٣
	التكرارات	٠	٢	٢
	النتيجة	٠	٤	٦
	المعدل	٢,٥		
	النسبة المئوية	%٨٣		

المصدر: الجدول من إعداد الباحثان بالاعتماد على نتائج تحليل البيانات

أما شركة Speed Way وحسب معطيات الجدول (١٨) فأنها تطبق هذا المتطلب بكافة تفاصيلها من حيث التخطيط لتطوير التقنيات والأجهزة، وإجراء الصيانة الوقائية والعلاجية للمعدات وأجهزة الاتصال، حيث بلغ معدل تطبيق هذا المتطلب (٣) درجات، وبنسبة تطبيق قدرها (١٠٠%)، اي إنها أفضل من حيث التطبيق لهذا المتطلب من شركة اللقاء نت.

الجدول (١٨) المعدلات والنسب المئوية لمتطلب تطوير نظم المعلومات لشركةSpeed Way

ت	الفقرات	بدرجة منخفضة	بدرجة متوسطة	بدرجة عالية
٣٦	الخطط الخاصة لتطوير الأجهزة التقنية للمعلومات			*
٣٧	الخطط الخاصة للأجراء الصيانة الوقائية لتقنية المعلومات			*
٣٨	الإجراءات اللازمة لمعالجة التوقفات أو العطلات المفاجئة في تقنيات المعلومات			*
٣٩	الرقابة المستمرة لعمل تقنيات المعلومات والاتصالات في الشركة			*
	الأوزان	١	٢	٣
	التكرارات	٠	٠	٤
	النتيجة	٠	٠	١٢
	المعدل	٣		
	النسبة المئوية	%١٠٠		

المصدر: الجدول من إعداد الباحثان بالاعتماد على نتائج تحليل البيانات

١٠- التوافق:

إن تحقيق متطلب التوافق والتطابق مع قواعد الأمن المعتمدة في الشركة بشكل عام تعتبر ضرورية، ويتضح من خلال الجدول (١٩) إن شركة اللقاء نت توكد على الحصول لدعم الإدارة العليا لضمان امن المعلومات، وهذا ما دعم معدل تطبيق هذا المتطلب والبالغ (٢) درجة، وقد بلغت نسبة تطبيق المتطلب في المواصفة ISO17799 (٦٧%) .

الجدول (١٩) المعدلات والنسب المئوية لمتطلب التوافق في شركة اللقاء نت

ت	الفقرات	بدرجة منخفضة	بدرجة متوسطة	بدرجة عالية
٤٠	التأكيد على التوافق مع سياسات وقواعد امن		*	

	المعلومات من قبل إدارة الشركة			
٤١	دعم الإدارة العليا للإجراءات الخاصة لأمن المعلومات في الشركة			*
٤٢	التوافق مع اتفاقيات دعم امن المعلومات مع الأطراف الخارجية	*		
٤٣	توافق المصرف مع قوانين وتشريعات الدولة الخاصة بأمن المعلومات		*	
الأوزان		١	٢	٣
التكرارات		١	٢	١
النتيجة		١	٤	٣
المعدل		٢		
النسبة المئوية		%٦٧		

المصدر: الجدول من إعداد الباحثان بالاعتماد على نتائج تحليل البيانات

يشير الجدول (٢٠) إلى إن شركة Speed Way تؤكد على التوافق مع سياسات وقواعد امن المعلومات، والحصول على دعم الإدارة العليا في مجال امن المعلومات، فضلا عن التوافق مع الأطراف الخارجية المتعاقدة مع الشركة في بعض المجالات، حيث بلغ معدل تطبيق هذا المتطلب (٢,٢) درجة، وكانت نسبة تطبيقها (٧٣%)، ويتضح إن نسبة تطبيق هذا المتطلب في شركة Speed Way أعلى من تطبيقها في شركة اللقاء نت.

الجدول (٢٠) المعدلات والنسب المئوية لمتطلب التوافق في شركة Speed Way

ت	الفقرات	بدرجة منخفضة	بدرجة متوسطة	بدرجة عالية
٤٠	التأكيد على التوافق مع سياسات وقواعد امن المعلومات من قبل إدارة الشركة			*
٤١	دعم الإدارة العليا للإجراءات الخاصة لأمن المعلومات			*

	في الشركة			
٤٢	التوافق مع اتفاقيات دعم امن المعلومات مع الأطراف الخارجية		*	
٤٣	توافق المصرف مع قوانين وتشريعات الدولة الخاصة بأمن المعلومات	*		
الأوزان		١	٢	٣
التكرارات		١	١	٢
النتيجة		١	٢	٦
المعدل		٢,٢		
النسبة المئوية		%٧٣		

المصدر: الجدول من إعداد الباحثان بالاعتماد على نتائج تحليل البيانات

بعد الاطلاع على نتائج تحليل البيانات, وتفسيرها يمكن القول إن إدارة الشركتين، والأفراد العاملين فيهما ليست لديهم فكرة واضحة عن المواصفة الدولية ISO 17799 وهذا يعني إن الفرضية الأولى: لبحث قد تحققت، أما الفرضية الثانية: للبحث فلم تتحقق؛ لأن النتائج أعلاه أشارت إلى إن الشركتان قيد البحث تطبقان معظم متطلبات وتفاصيل المواصفة ISO17799، ولكن ليس بهدف تطبيق المواصفة تحديدا وإنما كإجراءات وسياسات يلتزمون بها لحماية امن معلوماتهم، وأخيرا يمكن القول إن الفرضية الثالثة: تحققت لوجود اختلاف بين الشركتان قيد البحث في تطبيق متطلبات المواصفة ISO17799، حيث أظهرت النتائج إن شركة Speed Way هي الأفضل من حيث التطبيق.

الخاتمة

أولا: الاستنتاجات

يمكن استعراض أهم الاستنتاجات النظرية والميدانية التي توصل إليها البحث بالاتي:

١- أن تبني حوكمة امن المعلومات أصبحت حاجة ملحة للمنظمات في الوقت الحاضر، وخاصة المنظمات التي تعتمد في عملها على تقنيات المعلومات وشبكات الاتصالات التي تشهد تطوراً مستمراً.

٢- تعد حوكمة امن المعلومات وتقنياتها كمنهجية يمكن اعتمادها من قبل المنظمة لضمان حماية معلوماتها من خلال مرقبتها والسيطرة عليها، خصوصا ان المعلومات باتت المادة الأولية لإنجاز أنشطة المنظمة ونجاحها.

٣- بشكل عام يتضح من خلال النتائج إن شركة Speed Way تطبيق المتطلبات الأساسية للمواصفة ISO17799 بنسبة اكبر من شركة اللقاء نت، رغم أنهما يطبقان بعض المتطلبات بنفس النسبة (تنظيم امن المعلومات، الأمن المادي والبيئي).

٤- إن الفرق الأكبر بين الشركتين قيد البحث ظهر في متطلب إدارة الموجودات، والسبب قد يكون عدم اهتمام شركة اللقاء نت بموجوداتها بالصورة المطلوبة.

٥- إن المتطلب الوحيد الذي تفوق فيه شركة اللقاء نت على شركة Speed Way من حيث التطبيق هو متطلب امن الموارد البشرية، ويعتبرا متطلبا مهما لابد من الاهتمام به من قبل إدارة الشركة.

ثانيا: المقترحات

استنادا على الاستنتاجات السابقة يمكن تقديم بعض المقترحات التي يمكن الاستفادة منها من قبل الشركتين قيد البحث، والبحوث المستقبلية في هذا المجال، وكالاتي:

١- يقترح الباحثان أهمية وجود وحدة أو شعبة في الشركتين قيد البحث تتولى مهمة متابعة المعلومات وتوفير كل ما هو لازم لضمان امن المعلومات وخاصة السرية منها.

٢- توعية الموظفين العاملين في الشركة على أهمية المعلومات وأمنها، باعتبارها المادة الأساسية في الشركة، وخاصة الشركات العاملة في مجال الاتصالات والمعلومات.

٣- إقامة الندوات والمؤتمرات التي تشجع ثقافة الأمن المعلوماتي لدى الإدارات في الشركات، وضرورة الاهتمام بالرقابة على المعلومات وأمنها.

٤- أهمية الاعتماد على المواصفات والمعايير الدولية التي توفر الأمن والحماية للمعلومات من الشركات، من اجل حوكمة امن المنظومة المعلوماتية فيها، واتخاذها هدف تسعى إلى تحقيقها.

المصادر

1- Abu Khadra, Husam, Zuriekat, Majdy&Alrmahi, Nidal, (2009), "An Empirical Examination of Maturity Model As Measurement of Information Technology Governance Implementation", The International Arab Journal of Information Technology, Vol. (6), No. (3).

2- Eslami, Fatemeh&Fasanghari, Mahdi and Abdollahi, Ali, (2008), "Classification of IT Governance Tools for Selecting the Suitable One in an Enterprise", Iran Telecommunication Research Center (ITRC), Iran.

3- Conner, Bill & Noonan, Tom and Hollyman, Robert, (2004), " Information Security Governance: Toward a Framework for Action", McConnell International, www.bsa.org.

4- Debar, H. and Viinikka, J. (2006)," Security Information Management as an Outsourced Service", Computer Security Journal, Vol. 14, No.5.

5- Fawzy, M., (2003), "Assessment of corporate Governance in Egypt", Working Paper, The Egyption Center for Economic Studies, Egypt.

6- Gheorghe, Mirela, (2010), "Audit Methodology for IT Governance", Information Economic Journal, Vol. (14), No. (1).

7- Grippo F.J. & Siegel J.G.(2001), "Security Issues on the Internet", The CPA Journal ,October.

8-Kritzinger, E&Solms, Von &Strous, L.A,(2003), "Information Security: A Corporate Governance Issue ",Integrity and Internal Control in Information Systems, Springer Science+Business Media New York.

9-Koskosas, Ioannis&Kakoulidis, Konstantinos&Siomos, Christos,(2011), "Information Security: Corporate Culture and Organizational Commitment", International Journal of Humanities and Social Science, Vol. 1, No. 3.

10- Mueller, Lynn, et.al., (2008)," IBM IT Governance Approach: Business Performance Through IT Execution, International Business Machines Corporation", IBM.com/Red Books, USA.

11- Poole, Vernon, (2006), "Why Information Security Governance is Critical to Wider Corporate Governance Demands-A European Perspective", Journal Online, www.isaca.org.

12- Schwarz, A. &Hirschheim, R., (2003), An Extended Platform Logic Perspective of IT Governance: Managing Perceptions and Activities of IT, The Journal of Strategic Information Systems, Vol. (12), No. (2).

13-Solms, S. H. &Solms, R. Von, (2009), "Information Security Governance", Springer ScienceBusiness Media, New York, USA.

14-Wolk, et.al., (2001), "Accounting Theory A Caseptual and Institutional Approach", South-Weston Publishing Company, USA.

الملخص:

أضحت المعلومات المادة الأولية التي تتسابق المنظمات للحصول عليها، ولا سيما في ظل عصر الاقتصاد الرقمي الذي يعتمد على المعلومات بالدرجة الأساس لتضمن بقائها واستمرارها في الأسواق التنافسية، وفي ذات الوقت فإن هذه المعلومات يمكن أن تتعرض للكثير من المخاطر التي تهدد أمنها وسلامتها، وبالتالي تهدد نجاح المنظمة، ومن هنا أصبح من الضروري حماية هذه المعلومات بالاعتماد على وسائل وأدوات مختلفة، ومن بينها الاعتماد على حوكمة امن المعلومات وتحديدا محاولة تطبيق والالتزام بمتطلبات المواصفة الدولية ISO17799.

بناء على ما سبق يستهدف البحث قياس مدى استعداد شركات خدمة الانترنت لحوكمة امن معلوماتها، ومحاولة المقارنة بين اثنين من اكبر الشركات العاملة في هذا المجال من حيث تطبيقها لمتطلبات المواصفة الدولية ISO 17799 وهما شركة اللقاء نت، وSpeed Way في كركوك. وخلص البحث إلى مجموعة من الاستنتاجات والتي على أساسها تم تقديم بعض المقترحات.

الكلمات المفتاحية: امن المعلومات ، الحوكم ، حوكمة امن المعلومات.

Abstract:

Information has become the raw material that organizations are racing to obtain, especially in the era of the digital economy, which relies on information to the degree necessary to ensure its survival and continuity in competitive markets. At the same time, this information can be exposed to many risks that threaten its security and safety, and thus threaten the success of the organization. Hence, it has become necessary to protect this information by relying on various means and tools, including relying on information security governance, specifically trying to implement and comply with the requirements of the international standard ISO17799. Based on the foregoing, the research aims to measure the readiness of Internet service companies to govern the security of their information and to try to compare two of the largest companies working in this field in terms of their application of the requirements of the international standard ISO 17799, namely Al-Liqaa Net Company, and Speed Way in Kirkuk. The research concluded with a set of conclusions, on the basis of which some suggestions were made.

Keywords: information security, governance, information security governance. .