التحديات الأمنية لمشاريع الرقمنة بمؤسسات المعلومات العربية

د. متولى النقيب

مدرس تكنولوجيا المكتبات والوثائق والمعلومات
كلية الآداب – جامعة المنوفية

مقدمة:

تعتبر ظاهرة مشاريع رقمنة مصادر المعلومات في العالم العربي ظاهرة جديدة في عالم تقنيات المعلومات والتي تستخدم فيها تقنية المعلومات والاتصالات وأعمال الحوسبة بصورة مكثفة مبشراً ببزوغ فجر جديد في عالم تقنية المعلومات. وقد جاءت نتيجة لـدمج تقنية الاتصالات وتقنية الحاسب الآلي وما يرتبط به من صناعات متطورة للبرمجيـات[] وينصب اهتمام مثل هذه المشاريع على الإتاحة والخدمة. حيـث أصـبح العـالم أكثـر تواصلا، والأحداث غير المتوقعة أوسع انتشارا، والهجوم على البنى التحتية والـشبكات والأنظمة أكثر تعقيدا مما كانت عليه في الماضي. في نفس الوقت، بـدأت العديـد مـن مؤسسات المعلومات العربية، وبقوة في تنمية وتسهيل توصيل خدماتها الكترونيا من خلال نظم إدارة المحتوي الرقمي. هذا التطوير ضروري للنجاح المستقبلي، وينطـوي عليـه مخاطر للخدمات الرقمية من خلال الوصول المقصود أو غيـر المقـصود لمعلومـات حساسة، وتعريض مشاريع الرقمنة لتهديدات قائمة على التقنية الجديدة، وتعريض البنـى التحتية للمخاطر. ولضبط هذه التهديدات المفروضة، ينبغي تبني نهج لأمـن نظـم إدارة المحتوي الرقمي بمشاريع الرقمنة العربية مبنية على المخاطر المحتملة.

فمع اتساع دائرة التطورات التقنية المتلاحقة، وتنامي حجم مصادر المعلومات الرقمية بمختلف أشكالها، وازدياد حاجة المؤسسات المعلوماتية العربية إلى تحديث معلوماتها وتطوير مقتنياتها وخدماتها، فضلاً عن تنوّع احتياجات الباحثين والدارسين للحصول على معلومات غزيرة ومتنوعة، ظهرت جملة من مشاريع الرقمنة الحديثة لمواكبة عصر المعلومات، حيث دخلت كثيرٌ من مؤسسات المعلومات العربية في السنوات الأخيرة، بعد إكمالها بناء البنية التحتية لتكنولوجيا المعلومات، عصر مشاريع الرقمنة أذكر منها على سبيل المثال دار الكتب المصرية ومركز توثيق التراث الحضاري والطبيعي، شبكة إسلام أون لاين، المستودع الرقمي لمكتبة الإسكندرية، مكتبة الملك فهد الوطنية، مكتبة الوراق ...ألخ فقد قامت هذه المؤسسات بتحويل أرصدتها من مصادر المعلومات التقليدية إلى الصيغة الرقمية وإعتماد مختلف الأنظمة الحديثة التي تمكنها من تحويل هذه المصادر إلى مصادر رقمية يمكن البحث فيها بواسطة معايير مختلفة من خلال شبكات المعلومات.

فقد قامت هذه المؤسسات بتحويل أرصدتها من الشكل المطبوع إلى الصيغة الرقمية وهذا ما نجم عنه إشكالات متعددة تتمثل في الأساس في صعوبة إسترجاع هذه المصادر المطبوعة في حال توزعها في أماكن جغرافية متعددة وبقاء هذه المصادر معرضة للخطر-مثل المخطوطات والبحوث الأكاديمية والتقارير الفنية-، من سوء الاستعمال وسوء التخزين والحوادث المختلفة كالتلف الطبيعي كالتخمر أو التلف المادي كالتعرض للمياه والحرائق وسوء الاستعمال، كما أن الكثير من المؤسسات المعلوماتية العربية تعاني من مشكلة المكان في تخزين مصادرها مما يؤدي بهذه المؤسسات إلى إعتماد الرقمنة ومختلف الأنظمة الحديثة التي تمكنها من تحويل هذه المصادر المطبوعة إلى مصادر رقمية يمكن البحث فيها بواسطة معايير مختلفة، مع الحفاظ على صلاحيات وسرية تلك المصادر.

ويحتم ذلك ضرورة توافر ما يلي:

- طرق ملائمة لزيادة الوعي بالمخاطر المحيطة بنظم وتطبيقات مشاريع الرقمنة بمؤسسات المعلومات العربية.
- توجيهات ومعايير وأساليب مقننة للحفاظ علي مصادر المعلومات ونظماها وتطبيقاتها في البيئة الرقمية.
- إجراءات مناسبة تجرم المساس بسرية وخصوصية وتوافر البيانات والمعلومات لمستخدميها في مشاريع الرقمنة بمؤسسات المعلومات العربية.
- مقاييس وإجراءات تعكس المبادئ التي تخص أمن مصادر المعلومات الرقمية

فيجب علي المسئولين إدراك أن أي نظام مقترح لرقابة وحماية المعلومات لا يجب أن يرتكز فقط علي الجوانب الفنية والتكنولوجية لنظام إدارة المحتوي الرقمي. فقضية ضمان دقة وسلامة المعلومات لا تعتبر قضية تأمين وحماية أنظمة الحاسب فقط. حيث تتضمن عملية إدارة المخاطر وجود أصول تتعرض للمخاطر والتهديدات، وفي عصرنا الحالي، تعتبر المعلومات والحقوق الفكرية أحد أهم أصول وممتلكات المؤسسة، والتي من الصعب تقييمها كما في حالة الأصول المادية.

حيث يقترح الباحث إطار متكامل، يمكن المسئولين بمشاريع الرقمنة العربية من إعادة صياغة قضية حماية المحتوي الرقمي في شكل قضية لإدارة المخاطر التي تتعرض لها مكونات هذه المشاريع، يتوقف علي طبيعة المؤسسة المعلوماتية، ويتكون من أربعة مراحل:

- تحديد طبيعة الإختراقات والمخاطر، التي تتعرض لها نظم إدارة المحتوي الرقمي بمشاريع الرقمنة بمؤسسات المعلومات العربية، والتي تختلف باختلاف طبيعة نشاطها ونوعها.
- تقييم إجراءات الرقابة والحماية المطبقة من قبل إدارة المشروع، للتصدي لتلك المخاطر التي تتعرض لها نظم إدارة المحتوي الرقمي بمشاريع الرقمنة العربية.

- تحديد مدي فعالية إجراءات الرقابة والحماية المطبقة، من إدارة المشروع والمؤسسة المعلوماتية، في التصدي للإختراقات التي تتعرض لها نظم إدارة المحتوي الرقمي بمشاريع الرقمنة العربية، بما فيها الاختراقات غير المرتبطة بالجوانب الفنية للنظام. حيث يتم قياس الفجوة بين إجراءات الرقابة المطبقة وإجراءات الرقابة واجبة التطبيق، في ضوء طبيعة المخاطر التي تتعرض لها نظم إدارة المحتوي الرقمي بمشاريع الرقمنة بمؤسسات المعلومات العربية.
- وضع إستراتيجية لسد الفجوة الرقابية، بين إجراءات الرقابة المطبقة وإجراءات الرقابة واجبة التطبيق، تختلف باختلاف طبيعة نشاط ونوعية المشروع الرقمي.

حيث تعتبر قضية حماية المعلومات قضية شاملة، فلا يجب التركيز فيها علي حماية حماية الجوانب الفنية للنظام، مثل أجهزة ومعدات الحاسب والبرامج، ولكن يجب الإهتمام أيضاً بالجوانب غير الفنية للنظام، مثل العاملين ومستوي تدريبهم وتحديد مسئولياتهم وصلاحيتهم في ما يتعلق بحماية المعلومات، ووجود سياسة معلنة ومطبقة من قبل مؤسسة المعلومات لحماية نظام إدارة المحتوي الرقمي. فإدارة المخاطر المرتبطة بالمعلومات، مثلها مثل عمليات إدارة المخاطر المرتبطة بأصول المؤسسة الآخري، يجب أن تتناول سياسات المؤسسة المطبقة.

١. أهمية الدراسة:

تركز هذه الدراسة علي البعد المرتبط بالتحديات الأمنية لمشاريع الرقمنة بمؤسسات المعلومات العربية ونظمها وتطبيقاتها في البيئة الرقمية المحملة علي شبكات المعلومات وقابليتها للتعرض للضرر والخطر، حيث أن التحول السريع إلي الرقمنة يرافقه عقبات تهدد أمن مشاريع الرقمنة بمؤسسات المعلومات العربية وما يرافقها من أخطار القرصنة سواء لفك رموز التأمين والحماية، أو تلك البرامج التي يتم دسها في جهاز الضحية والذي يؤدي إلي التحكم في جهازه تحكماً كاملاً، بالإضافة لتلك البرامج التي يتم إرسالها عبر البريد الإلكتروني بهدف التدمير والتخريب، إضافة إلي العديد من التهديدات المادية

من تعدي علي أجهزة الحاسب في المؤسسة والعمر الإفتراضي لوسائط التخزين، إضافة إلي الكوارث الطبيعية مثل الحرائق، الفيضانات أو إنقطاع مصدر الطاقة، كل هذا أدي إلي وضع العاملين في مشاريع الرقمنة بمؤسسات المعلومات العربية أمام تحديات أمنية كبيرة. فهذه الدراسة تقدم صورة حقيقية للتحديات الأمنية التي تواجه مشاريع الرقمنة بمؤسسات المعلومات العربية؛ مما قد يساهم في التغلب عليها أو التقليل منها. وقد كسبت الدراسة الحالية أهميتها من كونها تميز بدقة بين العناصر التالية:

- اخترقات ومخاطر نظم إدارة المحتوي الرقمي بمشاريع الرقمنة بمؤسسات المعلومات العربية.
- إجراءات رقابة وحماية نظم إدارة المحتوي الرقمي بمشاريع الرقمنة بمؤسسات المعلومات العربية.
- فعالية الآليات المطبقة لإدارة المخاطر: حيث يتم قياس تلك الفعالية بالفجوة بين مستوي المخاطر التي تتعرض لها نظم إدارة المحتوي الرقمي بمشاريع الرقمنة العربية، ونطاق إجراءات الرقابة والحماية المطبقة.
- مكونات نظم إدارة المحتوي الرقمي، وما يرتبط بها من مخاطر أو إجراءات رقابية ملائمة: حيث تم تصنيف تلك االمكونات إلي مجموعتين، تلك المرتبطة بالجوانب الفنية وتشمل (المخاطر التي تهدد البرامج والتطبيقات ونظم التشغيل، واجهزة ومعدات الحاسب، والبيانات/المعلومات، وشبكات الحاسب)، وتلك المرتبطة بالجوانب غير الفنية وشمل (المخاطر التي تهدد التجهيزات المادية لمحيط عمل النظام، والمشغلين/العاملين، والسياسات واللوائح والقوانين).

٢. مشكلة الدراسة:

بدأت المؤسسات بجميع أنواعها بالاهتمام بشكل كبير بالتهديدات التي يمكن أن تواجه أمن المعلومات الرقمية وإدارتها وأصبحت ذات اهتمام أساسي من قبل أقسام تكنولوجيا المعلومات التابعة لها. حيث تتعرض نظم المعلومات للعديد من المخاطر

والتهديدات، وذلك عندما تكون تلك النظم قابلة للإختراق (Rainer et al.,1991). فقد كشفت نتائج الدراسة التي قام بها معهد حماية نظم الحاسب، والتي تم إجراؤها علي ٥٣٠ مؤسسة أمريكية، أن ٩٠% من المؤسسات محل الدر اسة تعرضت لاختراقات لإجراءات رقابة وحماية نظم المعلومات الآلية، وأن ٧٥% من تلك المؤسسات قد واجهت العديد من المشاكل والصعوبات نتيجة لعمليات الاختراق، والتي قد تسببت في خسائر إجمالية قدرها ٢٠٢ مليون دولار، وذلك في عام ٢٠٠٢ (CSI/FBI, 2003), . إن تطبيق نظم إدارة المحتوي الرقمي من قبل مشاريع انرقمنة بالعالم العربي، يحقق لها العديد من المزايا والمنافع، ولكنه في نفس الوقت يعرض معلوماتها للعديد من المخاطر والتهديات. فقد تم تطوير العديد من آليات وإجراءات الرقابة، والتي تؤمن الحماية لكل جانب من جوانب نظم إدارة المحتوي الرقمي، وذلك في محاولة للتصدي للإختراقات المختملة. وبالرغم من ذلك فإن فعالية الإجراءات المطبقة لرقابة وحماية نظم إدارة المحتوي الرقمي بمشاريع الرقمنة العربية كانت محل شك، وذلك بسبب استمرار تزايد الإختراقات، وما يترتب عنها من حسائر مالية ضخمة. إن لإجراءات وآليات الرقابة دور ضئيل في توفير الحماية لنظم إدارة المحتوي الرقمي، فقضية الحماية تعتبر قضية أفراد، وأيضاً قضية مؤسسية (Hinde, 2003).

تركز النظرة التقليدية لإدارة المخاطر علي توفير الحماية ضد المخاطر التي تتعرض لها نظم إدارة المحتوي الرقمي، بما في ذلك حماية البنية التحتية لأنظمتها الآلية. علي الرغم من ذلك، لا يجب التركيز فقط علي الجوانب الفنية (Posthumus, S. and von Solms, R. ,2004). فقد بينت دراسة (Ernst & Young ,1996)، أن الأخطاء غير المتعمدة، من قبل العاملين أو الأطراف الخارجية، كانت السبب الرئيسي وراء الخسائر المالية الضخمة، التي تعرضت لها ٣٤% من المؤسسات في بريطانيا. لذلك نجد ان اختراقات نظم إدارة المحتوي الرقمي بمشاريع الرقمنة العربية قد يكون بسبب جوانب فنية (مثل وجود خلل بالبرمجيات)، أو بسبب جوانب غير فنية (مثل الفشل في إدارة أنظمة الرقابة أو أخطاء بشرية). لذلك، فحتي تصبح إدارة مشاريع الرقمنة العربية

للمخاطر فعالة، في حماية نظم إدارة المحتوي الرقمي، يجب أن تغطي كلاً من الجوانب الفنية وغير الفنية. فقد كشفت دراسة (Workman, Michael ,2009)، وضع المؤسسات كلاً من فيروسات الحاسب، والأعداد الكبيرة من الرسائل الإلكترونية التي تحتوي علي مواد داعائية Bulk e-mail، من أولويات اهتمامها. حيث يمتلك ١٠٠% من المؤسسات برامج حماية ضد فيروسات الحاسب، ويمتلك ٧١% منها برامج للتصدي للرسائل الإلكترونية الدعائية Anti-Spam Protection، كآليات لحماية شبكات الحاسب. وعلي الرغم من ذلك، تقوض معظم المؤسسات تلك الآليات بتقصيرها في تدريب موظفيها علي عدم فتح مرفقات البريد الإلكتروني المشكوك فيه.

ونجد أن استخدام كلمات السر للتحقق من شخصية المستخدم له عيوب عدة. أحدها عدم وعي المستخدمين بأهمية وتأثير هذه الكلمات على أمن الحاسبات والشبكات والمعلومات في المؤسسة بشكل عام. ففي الغالب يعتقد المستخدم أن عواقب سوء استخدام حسابه الخاص تقع على ملفاته الخاصة فقط، بينما هذه العواقب يمكن أن تشمل جميع المستخدمين وأنظمة الحاسب والشبكات في المنشأة. ففي إحدى مؤسسات المعلومات الكبيرة نسبياً وجد أن اكثر من ٩٠% من كلمات السر ضعيفة وأمكن كسرها خلال فترة وجيزة باستخدام برامج متوفرة في الإنترنت تقوم بالبحث في جميع البدائل Force Search Brute ويتوجب على المؤسسة وضع وتنفيذ سياسة واضحة وآمنة لحسابات التشغيل وكلمات السر (Misra ,Subhas C.,2008) فمن خلالها يتم إجبار المستخدم على تغيير كلمة السر بعد مضي فترة من الزمن، وعدم السماح باستخدام كلمة سراستخدمت في الماضي القريب، وإقفال الحسابات التي لم يستخدمها أصحابها لفترة طويلة وكذلك ذات كلمات السر الضعيفة، وتحديد موعد لبدء وإغلاق الصلاحيات وخاصة للأعمال الموسمية، والاحتفاظ بسجل لمحاولات الدخول المتكررة على النظام وتحليله بشكل دوري، وتحديد عدد محاولات الدخول الفاشلة قبل إغلاق الحساب، وإعلام المستخدم بمحاولات الدخول الفاشلة بالإضافة إلى آخر مرة تم فيها الدخول،

والحرص على إبلاغ كلمة السر بشكل سري وللشخص المعني مباشرة أو من خلال برامج معينة دون تدخل بشري.

وقد تكون التهديدات عرضية أو متعمدة وقد يكون لها علاقة باستخدام أو تطبيق نظم تكنولوجيا المعلومات أو النواحي البيئية والفيزيائية التابعة لكتنولوجيا المعلومات. قد تأخذ هذه المخاطر أي شكل من أشكال سرقة المعلومات أو مخاطر متابعة الأعمال عن طريق الانترنت أو التجسس عن بعد أو سرقة المعدات أو الوثائق من خلال أي ظاهرة مناخية كالزلازل أو الحرائق او الفيضانات أو الحوادث الوبائية. قد ينتج عن هذه المخاطر العديد من الآثار السلبية على العمل مثل الخسارة المالية أو الضرر المادي أو ضياع خدمات الشبكات الرئيسية أو خسارة ثقة المستفيد نتيجة لفقدان إمداد الطاقة أو إخفاق معدات الاتصالات.

وتسئ العديد من مؤسسات الأعمال تخصيص وتوجيه مواردها إلي إجراءات رقابة وحماية غير فعالة، في حين تهمل إجراءات أخري أكثر فعالية. فقد كشفت دراسة (Von Solms, B. and von Solms, R. ,2004) العديد من المشاكل المتعلقة بإدارة أنظمة رقابة وحماية نظم إدارة المحتوي الرقمي، حيث اتضح عدم إدراك معظم المؤسسات لحقيقة كون قضية حماية نظم إدارة المحتوي الرقمي قضية مؤسسية، وليست قضية فنية فقط. لذلك إن عدم تطبيق إجراءات الرقابة والحماية الفعالة قد يزيد من مخاطر اختراق نظم إدارة المحتوي الرقمي بمشاريع الرقمنة بمؤسسات المعلومات العربية، لذلك يجب علي القائمين علي مثل هذه المشروعات تعديل نظرتهم التقليدية لطبيعة المخاطر والإختراقات. فإجراءات الرقابة المادية وإعداد النسخ الإحتياطية، لم تعد إجراءات كافية لتوفير الرقابة والحماية.

٣. أهداف الدراسة:

إن التقدم في صناعة الحاسبات الآلية ووسائط التخزين الآلية وإتساع إستخدام شبكة الإنترنت وما ينجم عنها من خدمات ومنافع متبادلة وما يرافقها من برامج التأمين

علي البيانات المرسلة أو محتويات الحاسب. وعلي الرغم من وجود برامج التأمين المعقدة مازال خطر الإختراق والتحكم في البيانات يأخذ الصادرة في أولويات العاملين في المؤسسات المعلوماتية.

إن التحول السريع إلي الرقمنة يرافقه عقبات تهدد أمن مصادر المعلومات الرقمية الموجودة لدي المؤسسة المعلوماتية أو تلك التي تنقل عبر الشبكات وما يرافقها من أخطار القرصنة سواء لفك رموز التأمين والحماية، أو تلك البرامج التي يتم دسها في جهاز الضحية والذي يؤدي إلي التحكم في جهازه تحكماً كاملاً، بالإضافة لتلك البرامج التي يتم إرسالها عبر البريد الإلكتروني بهدف التدمير والتخريب، إضافة إلي العديد من التهديدات المادية من تعدي علي أجهزة الحاسب في المؤسسة، إضافة إلي الكوارث الطبيعية مثل الحرائق، الفيضانات أو إنقطاع مصدر الطاقة، كل هذا أدي إلي وضع العاملين في مشاريع الرقمنة بمؤسسات المعلومات العربية أمام تحديات أمنية كبيرة.

إن تطبيق مدخل متكامل في إدارة المخاطر، يتناسب مع محيط عمل نظام إدارة محتوي رقمي بعينه، يعتبر مطلب أساسي لتوفير الرقابة الفعالة، لذلك تهدف هذه الدراسة إلي تحليل الفروق في طبيعة الاختراقات والمخاطر التي تتعرض لها نظم إدارة المحتوي الرقمي بمشاريع الرقمنة بمؤسسات المعلومات العربية، وإجراءات الرقابة الملائمة للتصدي لتلك الاختراقات والمخاطر، بين مؤسسات المعلومات العربية المختلفة، حيث تختبر تلك الدراسة مدي ملائمة إجراءات الرقابة المطبقة، من قبل هذه المؤسسات، مع تحديد طبيعة المخاطر المتلازمة التي تتعرض لها نظم إدارة المحتوي الرقمي بهذه بمشاريع الرقمنة بمؤسسات المعلومات العربية. حيث يتمثل الهدف الأول للدراسة في تحديد الفجوة بين مستوي المخاطر، ونطاق إجراءات الرقابة والحماية المطبق. وبناء علي تلك الفجوة، يأتي الهدف الثاني للدراسة، وهو اقتراح آليات لسد الاختراقات، من خلال تطبيق إجراءات لرقابة وحماية نظم إدارة المحتوي الرقمي بمشاريع الرقمنة بمؤسسات المعلومات العربية.

٤. أسئلة الدراسة:

تحاول تلك الدراسة الإجابة علي التساؤلات البحثية التالية:

١. ما هي طبيعة المخاطر المتلازمة التي تتعرض لها نظم إدارة المحتوي الرقمي بمشاريع الرقمنة بمؤسسات المعلومات العربية ؟

٢. ما هي إجراءات الرقابة والحماية، المطبقة من قبل مشاريع الرقمنة بمؤسسات المعلومات محل الدراسة، للتصدي لتلك المخاطر التي تتعرض لها نظم إدارة المحتوي الرقمي؟

٣. ما هو مستوي فعالية إجراءات الرقابة والحماية، المطبقة من قبل مشاريع الرقمنة بمؤسسات المعلومات العربية، في التصدي للمخاطر التي تتعرض لها نظم إدارة المحتوي الرقمي، بما فيها المخاطر غير المرتبطة بالجوانب الفنية للنظام؟

٤. ما هي إستراتيجية التصدي للمخاطر والإختراقات التي تتعرض لها نظم إدارة المحتوي الرقمي بمشاريع الرقمنة بمؤسسات المعلومات العربية في قطاعات مختلفة، وما تتضمنها من إجراءات لرقابة وحماية فعالة تتناسب مع طبيعة كل قطاع؟

٥. مصطلحات الدراسة:

⊙ مشاريع الرقمنة بمؤسسات المعلومات العربية:

هي تلك المشروعات التي تحتوي علي مجموعة من مصادر المعلومات الرقمية وبها العديد من الإمكانات الفنية ذات العلاقة بإنتاج وتوثيق مصادر المعلومات، والبحث عنها واستخدامها وبذلك فإن هذه المشاريع هي امتداد و دعم لنظم خزن المعلومات واسترجاعها التي تدير المعلومات الرقمية بغض النظر عن الوعاء سواء كان نصيًا أو صوتيًا أو في شكل صور بنوعيها الثابت وغير الثابت، وتكون متاحة على شبكة الإنترانت أو الإنترنت. وفيما يلي مشاريع الرقمنة العربية محل الدراسة:

- **مستودع الأصول الرقمية التابع لمكتبة الأسكندرية: (http://dar.bibalex.org)** : عبارة عن مكتبة رقمية عربية تحوي اكثر من ١٠٠ الف كتاب يمكن الاطلاع عليها من خلال شبكة. وترجع اهمية هذا المشروع في حفظ الكتب والمراجع التي تقتنيها مكتبة الاسكندرية من التلف او الضياع، وهو يأتي ايضا ردا للتحدي الثقافي العالمي في ظل فقر المحتوى العربي على شبكة الانترنت وضآلته مقارنة باللغات الاخرى اضافة الى ما يقدمه المشروع من خدمة فائقة لطلاب العلم والباحثين والاكاديميين و للجمهور عامة، وتشمل مجموعات الكتب مجالات وموضوعات كثيرة منها مجال العلوم الانسانية كعلم الاجتماع والنفس والفلسفة والعلوم الطبيعية والتاريخ والجغرافيا وكتب ومراجع في الادب والبلاغة والتكنولوجيا والعلوم التطبيقية والرياضيات. وتتضمن كذلك مجموعات خاصة بالديانات والمعارف العامة والدوريات والخرائط والموضوعات المتعلقة بالسلام والاستخدام السلمي للطاقة النووية والفقر والسكان وحرية الصحافة والاتصالات والحفاظ على التراث والتعليم والملكية الفكرية وحقوق النشر والماركات التجارية والتصميمات وبراءات الاختراع وحقوق الانسان والقانون الدولي والنمو الاقتصادي.
- **الوراق (http://www.alwaraq.net)** : عبارة عن مكتبة رقمية تضم الألاف من أمهات الكتب التراثية في الأدب و الشعر و التاريخ واللغة العربية وتتيح قراءة الكتاب كاملاً مع وجود محرك بحث ذو إمكانيات عالية، فهذا المشروع يهدف إلي نشر التراث العربي والإسلامي بإستخدام تكنولوجيا المعلومات و ما يتضمن ذلك من إعادة تحقيق و توثيق لبعض مصادره و إعادة صياغة بعضها الآخر.
- **ببليواسلام (www.biblioislam.net)** : عبارة عن مكتبة رقمية تهدف إلى خدمة الباحثين الأكاديميين في المجالات الإسلامية، وذلك من خلال التعريف بمصادر المعلومات المختلفة (كتب، ودوريات، وبحوث مؤتمرات، ورسائل جامعية)

من خلال عدة مستويات تشمل: البيانات الببليوجرافية، والمستخلصات، والعروض، والمراجعات، والنصوص الكاملة. ويهتم الموقع بالدراسات التي تنصب على العلوم الشرعية، واللغة العربية، والتاريخ الإسلامي، والعلوم المرتبطة بها؛ كتحقيق التراث، والترجمة، والآثار، إضافة إلى العلوم المعلوماتية والتربوية والاقتصادية والأمنية، والتي يتم التأصيل لها من المنظور الشرعي، وكذلك الدراسات المرتبطة بقضايا الهوية الثقافية والأنثروبولوجيا.

- **مركز توثيق التراث الحضاري والطبيعي (www.cultnat.org)** : هو أحد المراكز البحثية التابعة لمكتبة الإسكندرية بدعم من وزارة الاتصالات والمعلومات وإضافةً إلى ما يضطلع به المركز حاليا من توثيق تراث مصر الحضاري والطبيعي، فإنه حدد لمسيرته صياغة وإنجاز خطة قومية لبرنامج التوثيق الشامل، بتوظيف أحدث التقنيات وأعلى وأكفأ الخبرات العلمية والفنية، إلى جانب الحرص التام على التعاون الوثيق المثمر مع المنظمات القومية والدولية المعنية والمتخصصة.

- **مكتبة المدينة الرقمية (http://elibrary.mediu.edu.my)**: موقع علمي يُعنَى بالرصيد العلمي المكتوب الذي تزخر به المكتبة العربية من المؤلَّفات، سواءً من الكتب أو الموسوعات أو المجلات أو المقالات أو الفتاوى، وغير ذلك من تراثنا المقروء... وعرْضه على شبكة الويب، بأسلوب يحقِّق الفائدة العلمية المرجوّة للدّارسين والباحثين في شتّى بقاع الأرض، بطريقة عرض تتناسب مع ما يَخدم القارئَ ويُوفِر عليه الجهد والوقت؛ وذلك بالاستفادة القصوى ممّا تُتيحه التقنيةُ الحديثة من إمكانات في التصفّح والعرْض والبحث. فهذا المشروع يسّعي لبناء مكتبة عربية رقمية في شتّى فنون المعرفة المفيدة، وذلك عن طريق إسهام المُطَّلعين على هذه المكتبة بجهودهم، وترسيخ مبدإ أن العلْم رحِم بين أهله.

- **دار الكتب المصرية *(www.darelkotob.gov.eg)* وبها أكثر من مشروع**

رقمي: إثراء التراث الحضاري، رقمنة الخرائط، رقمنة البرديات، توثيق التـراث الصحفي والدوريات المصرية وهي مشاريع رقمنة تعاونية بين دار الكتب المصرية ومركز توثيق التراث الحضاري والطبيعي التابع لمكتبة الأسكندرية الهدف منهـا رقمنة الكتب التراثية التى تمتلكها الدار من سنة ١٨٧٠ حتـى ١٩٥٥، و رقمنـة 10000 خريطة ، ورقمنة المخطوطات الإسلامية المدونة على البرديات، وتوثيق الصحف والدوريات المصرية بكافة لغاتها منذ بداية نشرها، وحتى عـام ١٩٥٢م سواء طبعت بمصر أم خارجها، سواء توقفت عن الصدور أم لا تزال مستمرة حتى الآن، ثم إتاحة كل هذا من خلال برنامج اليكترونى على شبكة الإنترنت لعرضـها لجمهور الباحثين.

- **مكتبة الملك فهد الوطنية (http://www.kfnl.gov.sa)** : تهدف المكتبـة إلـى اقتناء الإنتاج الفكري وتنظيمه وضبطه وتوثيقه والتعريف به ونشره فهناك مشروع رقمي وهو الكتاب الإلكتروني والمجلة، حيث أنه يهتم بنشر مطبوعات مكتبة الملك فهد الوطنية وخاصة السلسلة الأولى و الثانية والثالثة بشكل رقمي من خلال موقع المكتبة علي شبكة الإنترنت.

⊙ **نظم إدارة المحتوي الرقمي:** هو برنامج يتيح خدمات حفظ وتنظيم وبث المجموعات الرقمية علي الحاسب من خلال شبكة الإنترنت أو الإنترانت (النقيب، ٢٠٠٦).

⊙ **استراتيجية او سياسة أمن المعلومات:** هي مجموعة القواعد التي يطبقها الأشخاص لدى التعامل مع التقنية ومع المعلومات داخل المنشأة وتتصل بـشؤون الـدخول الـى المعلومات والعمـل علـى نظمهـا وادارتهـا. (Tsohou, Aggeliki, and et al. 2006,). وتنطلق الاستراتيجية الفاعلة من القدرة على ايجاد نظام متواصـل لعمليـة تحليل المخاطر وتحديد احتياجات الحماية ، وعملية تحليل المخاطر هي فـي حقيقتهـا نظام متكامل للتحليل وسلامة التصرف تبدأ من الاعداد الجيد القائم على فهـم وادراك وتحديد عناصر النظام والعمليات والمخاطر، ومن ثم تحديد معـايير التهديـد ونطـاق

الحماية المطلوب منها وتبعا له وسائل الحماية، لتنتهي ببيان معيار الخسارة المقبولة التي يتصور تحققها بغض النظر عن مستوى الحماية ومستوى الاستعداد للمواجهة.

⊙ **التهديد:** مجموعة مؤلفة من عدة متتابعات ناجمة عن وقوع حادث غير مرغوب فيه أو الاحتمال القوي لوقوع حادث ما. (Misra ,Subhas C.,2008)

⊙ **مخاطر نظم إدارة المحتوي الرقمي :** هناك مخاطر عديدة يمكن ان تواجه نظم إدارة المحتوي الرقمي وابرز هذه المخاطر ما يلي : (Wan, XM ,2008; ISO/IEC FCD 27033:2009).

- **اختراق الأنظمة** : ويتحقق ذلك بدخول شخص غير مخول بذلك الى نظام الكمبيوتر والقيام بأنشطة غير مصرح له بها كتعديل البرمجيات التطبيقية وسرقة البيانات السرية او تدمير الملفات او البرمجيات او النظام او لمجرد الاستخدام غير المشروع.
- **الاعتداء على حق التخويل** : ويتم من خلال قيام الشخص المخول له استخدام النظام لغرض ما باستخدامه في غير هذا الغرض دون ان يحصل على التخويل بذلك، وهذا الخطر يعد من الأخطار الداخلية في حقل إساءة استخدام النظام من قبل موظفي المؤسسة، وهو قد يكون أيضا من الأخطار الخارجية، كاستخدام المخترق حساب شخص مخول له باستخدام النظام عن طريق تخمين كلمة السر الخاصة به او استغلال نقطة ضعف بالنظام للدخول اليه بطريق مشروع او من جزء مشروع ومن ثم القيام بانشطة غير مشروعة.
- **زراعة نقاط الضعف** : عادة ينتج هذا الخطر عن اقتحام من قبل شخص غير مصرح له بذلك او من خلال مستخدم مشروع تجاوز حدود التخويل الممنوح له بحيث يقوم الشخص بزرع مدخل ما يحقق له الاختراق فيما بعد. ومن اشهر امثلة زراعة المخاطر حصان طروادة ، وهو عبارة عن برنامج يؤدي غرضا مشروعا في الظاهر لكنه يمكن ان يستخدم في الخفاء للقيام بنشاط غير مشروع، كان يستخدم برنامج معالجة كلمات ظاهريا لتحرير وتنسيق النصوص في حين يكون غرضه

الحقيقي طباعة كافة ملفات النظام ونقلها الى ملف مخفي بحيث يمكن للمختـــرق ان يقوم بطباعة هذا الملف والحصول على محتويات النظام.

- **مراقبة الاتصالات** : بدون اختراق كمبيوتر المجني عليه يتمكن الجاني من الحصول علـــى معلومات سرية غالبا ما تكون من المعلومات التي تسهل له مستقبلا اختراق النظام وذلـــك ببساطة من خلال مراقبة الاتصالات من إحدى نقاط الاتصال او حلقاتها.
- **اعتراض الاتصالات** : وكذلك بدون اختراق النظام يقوم الجاني في هذه الحالـــة بـــاعتراض المعطيات المنقولة خلال عملية النقل ويجري عليها التعديلات التي تتناســـب مـــع غـــرض الاعتداء، ويشمل اعتراض الاتصالات قيام الجاني بخلق نظام وسيط وهمي بحيـــث يكـــون على المستخدم ان يمر من خلاله ويزود النظام بمعلومات حساسة بشكل طوعي.
- **الخدمة** : ويتم ذلك من خلال القيام بأنشطة تمنع المستخدم الشرعي مـــن الوصـــول الـــى المعلومات او الحصول على الخدمة وابرز انماط انكار الخدمة ارسال كميـــة كبيـــرة مـــن رسائل البريد الإلكتروني دفعة واحدة الى موقع معين بهدف اسقاط النظام المـــستقبل لعـــدم قدرته على احتمالها او توجيه عدد كبير من عناوين الإنترنت على نحـــو لا يتـــيح عمليـــة تجزئة حزم المواد المرسلة فتؤدي الى اكتظاظ الخادم وعدم قدرته على التعامل معه.
- **عدم الاقرار بالقيام بالتصرف** : ويتمثل هذا الخطر في عدم اقرار الشخص المرسل اليه او المرسل بالتصرف الذي صدر عنه، كأن ينكر انه ليس هو شخصيا الذي قام بارسال طلـــب الشراء عبر الإنترنت.

٦. الدراسات السابقة:

إن حداثة المادة العلمية التي تناولتها الدراسة أدت إلي ندرة المراجع والدراســـات السابقة وعلي الرغم من هذا فإن الباحث قد توصل إلي عدد من الدراسات المهتمة بشكل عام بأمن نظم المعلومات الآلية في المؤسسات المختلفة وهي:

ISO/IEC FCD 27033:2009. Information technology — Security techniques — Network security. http://www.iso.org/

تقدم هذه المواصـــفة ISO/IEC FCD 27033:2009 ارشـــادات حـــول إدارة مخاطر أمن المعلومات، حيث تتألف من: (تقـــييم المخـــاطر، عـــــلاج المخـــاطر،

قـــبول المخاطر، ترابـــط المخاطر، مراقبة المخاطر). ويقول ادوارد همفـرييس، رئيس فريق العامل الذي وضع المواصفة "اليوم، معظم المؤسـسات تعتـرف بالـدور الحاسم الذي تلعبه تكنولوجيا المعلومات في دعم اعمالها واهدافها مـع ظهـور شـبكة الانترنت واحتمال اداء جميع الاعمال على شبكة الانترنت. لذلك نجـد إن أمـن نظـم المعلومات أصبح في الصدارة، وإن المواصفة المذكورة لها علاقة بالمدراء والموظفين المعنيين بإدارة مخاطر أمن المعلومات في نطاق المؤسسة. وأينما كان ذلك ممكنا". غير ان المواصفة المذكورة لا تقدم أية معلومات محددة منهجيه لادارة المخاطر الأمنيـة. والامر متروك لمؤسسة لتحديد نهج لادارة المخاطر.

Jones, Cynthia M. (2009). Utilizing the technology acceptance model to assess employee adoption of information systems security measures. D.B.A., Nova Southeastern University, 2009 , 182 pages; AAT 3372768

تقدم هذه الدراسة إطار نظري لدعم وحماية نظم المعلومـات فـي المؤسـسات المختلفة، من خلال تقليص أخطاء العاملين والعمل علي تحسين فعالية إجراءات الرقابة والحماية المطبقة، حيث يري الباحث أن آليات وإجراءات رقابة وحماية نظم المعلومات قد تفقد فعاليتها إذا أسئ فهمها واستخدامها او لم يتم توظيفها، أو تطبيقها بـشكل غيـر سليم، من قبل المشغل والمستخدم النهائي.

Wan, XM (2008). "Construction of information System Security Precaution in Digital Library". the 3rd International Conference on Information Systems for Crisis Response and Management/4th International Symposium on Geo-Information for Disaster Management, AUG 04-06, 2008 Harbin Engn Univ Harbin PEOPLES R CHINA, pp 263-268

هذه الدراسة تقدم تحليلا للعوامل التي تؤثر على أمن نظام المعلومات في المكتبة الرقمية بما في ذلك : إعدادات الشبكة، البيئة المحيطة، فيروسـات الحاسـب، هجـوم القراصنة، الخ وهو يعرض سلسلة من التدابير الأمنية التي تتألف من بناء نظام أمنـي وقائي لفيروسات الكمبيوتر، وأمن الخادم، ورصد ومراجعة سلوك المستفيدين على شبكة

الإنترنت، وبناء نظام أمني للطوارئ، و تشريعات أمن المعلومات. فقد كشفت هذه الدراسة أن الإجراءات الوقائية تشمل استخدام آليات ورقابة وحماية متقدمة، مثل استخدام برامج متقدمة لرقابة عمليات الوصول للنظام، وبرامج لكشف محاولات اختراق الشبكات المستخدمة، واستخدام جدران النار Firewalls، وتوفير الحماية المادية لمكونات نظام المكتبة الرقمية، حيث أن تطبيق الجانب غير التقني في إدارة المخاطر، غير المرتبط بالجوانب الفنية للنظام، يساعد في تقليص المخاطر الناجمة عن الأخطاء الداخلية. فوجود سياسة لأمن المعلومات معلنة ومكتوبة، يمكن أن توفر دعم لحماية النظام، كما أن وضع خطط طوارئ، معلنة وموثقة، لاستمرارية الأعمال، توضح الإجراءات التي يجب اتباعها في حالات الكوارث وتعطل النظام، وتحديد المسئولين عن تنفيذ تلك الإجراءات يساعد علي حماية العمليات الحرجة للمكتبة الرقمية من آثار إخفاق النظام. كما يجب وجود إجراءات رقابية تمنع خرق القوانين والتنظيمات واللوائح الداخلية، أما إجراءات الرقابة والحماية المتعلقة بالعاملين فتشمل عقد دورات تدريبية خاصة بإجراءات تشغيل وحماية نظم إدارة المحتوي الرقمي، وذلك من شأنه أن يقلص الأخطاء البشرية، ويساعد في توعية العاملين بمحاولات إختراق نظم إدارة المحتوي الرقمي. كما أن إجراءات عمليات مراجعة دورية وغير دورية، قد تمكن من قليص مخاطر التلاعب أو سوء إستغلال العاملين لموارد النظام.

Lihong Zhou, Ana Vasconcelos, Miguel Nunes (2008), "Supporting decision making in risk management through an evidence-based information systems project risk checklist". *Information Management & Computer Security*, Vol. 16 No. 2, pp. 166 - 186

هذه الورقة تهدف الى تقديم دراسة عن مخاطر نظم المعلومات وإدارة المشاريع الرقمية تهدف إلى تحديد المخاطر والأنطولوجيا المرجعية التي ستمكن عملية صنع القرار والتخطيط لاستراتيجية التخفيف من آثارها في نظام المعلومات، من خلال تحليل لعشر دراسات حالة في المملكة المتحدة والولايات المتحدة ونيوزيلندا ، وقد قسمت إلى خمس فئات رئيسية : مرحلة ما قبل المشروع ، والمستفيدين ، وإدارة المشاريع ،

والقضايا التكنولوجية ، وتطوير المنهجية. وتشير نتائج التحليل أن هناك عددا كبيرا من عوامل الخطر التي تتكبدها المؤسسة قبل بدء المشروع رسميا، ولذلك ينبغي وضع سياسة لأمن المعلومات قبل بداية المشروع بوقت كافي.

Tejay, Gurvirender Pal Singh. (2008). Shaping strategic information systems security initiatives in organizations, Ph.D., Virginia Commonwealth University, 2008 , 360 pages; AAT 3346492

والهدف الرئيسي من هذه الدراسة هو تعزيز فهم استراتيجية أمن نظم المعلومات، لكي تكون ناجحة ، مع إضفاء الطابع المؤسسي على مبادرة الأمن أمر ضروري. من خلال تحليل وتقييم آليات إدارة المخاطر المرتبطة بنظم المعلومات، مع التركيز علي إجراءات مراقبة عمليات الوصول لنظم المعلومات الآلية باعتبارها عنصر هام في تأمين وحماية أنظمة الحاسب. ويعتقد الباحث أن من الأسباب المباشرة لاختراقات نظم المعلومات الآلية: الإفتقار إلي المعرفة والممارسات الملائمة في بعض المجالات كهندسة البرمجيات، وآلياتوبرامج الرقابة والحماية، والتشفير. حيث يتعامل معظم مستخدمي ومشغلي نظم الحاسب مع آليات وبرامج الرقابة والحماية علي أنها إضافات غير ذات أهمية لنظم الحاسب. وقد توصلت الدراسة إلي أن الإستراتيجية الأمنية لنظام المعلومات يجب أن تكون متناغمة مع الاستمرارية الثقافية للمنظمة .

Kuegah, Folly (2006). Security measures and effective corporate information systems management: An examination of issues surrounding computer network security, Ph.D., Capella University, 2006 , 130 pages; AAT 3229905

أهتمت هذه الدراسة بتحليل الآليات التي تستخدمها المؤسسات، التي تتحول إلي العمل من خلال شبكة الإنترنت وتحويل جميع معلوماتيها في شكل رقمي، في تقييم إدارة المخاطر التي تتعرض لها في ظل هذه البيئة الجديدة. حيث كشفت الدراسة علي أن أخطر الإختراقات لإجراءات رقابة وحماية نظم المعلومات الآلية، في هذه الحالة، تتمثل في: التدمير غير المتعمد للبيانات، والإدخال غير المتعمد لبيانات غير سليمة من قبل العاملين، والتدمير المتعمد للبيانات والإدخال المتعمد لبيانات غير سليمة من قبل

العاملين، والمخاطر الناجمة عن البرامج الخبيثة، وعدم الإحتفاظ بنسخ احتياطية كافية لملفات البيانات وملفات لتوثيق عمليات الدخول للنظام، والحوادث الطبيعية مثل الحريق والفيضانات وإنقطاع التيار الكهربائي.

Joint, Nicholas (2006). "Risk assessment and copyright in digital libraries", *Library Review*, Vol. 55 No. 9, pp. 545 – 548

تحاول هذه الورقة تقديم رؤى واضحة إلى الطرق اللازمة لتقييم مخاطر المكتبات الرقمية المتزايدة في بيئة الشبكات الإفتراضية لإكتساب مزيد من الخبرة في قضايا الحقوق الرقمية والمبادئ التي حددت معالمها الممارسين ولهذا تقدم هذه الورقة بعض الأفكار المفيدة في كيفية التعامل مع الجوانب القانونية لحقوق الملكية الفكرية بالمكتبات الرقمية.

Rudasill, Lynne and Moyer, Jessica (2004)."Cyber-security, cyber-attack, and the development of governmental response: the librarian's view", *New Library World*, Vol. 105 No. 7/8, pp. 248 – 255

هذه الدراسة تعرض لمحة عن التطور التاريخي لسياسات أمن المعلومات في الفضاء الإلكتروني الصادرة عن مجموعة متنوعة من الحكومات والوكالات. مثل الاتحاد الأوروبي، وحكومة الولايات المتحدة الأمريكية من خلال تحليل وثائق السياسة التي تظهر بعض أوجه التشابه في الطريقة الوطنية لرد الفعل على التهديدات المحتملة في الفضاء الإلكتروني. فهذه الورقة تساعد المكتبات وتشجعهم لتصبح أكثر نشاطا ومشاركة وعلم بشأن تطوير سياسات الحكومة في هذا المجال. وعلي وضع سياسات واضحة لأمن المعلومات في العالم الرقمي وتقدم بعض المفاهيم العملية من واقع السياسات الوطنية لأمن المعلومات في الفضاء الإلكتروني.

Posthumus, S. and von Solms, R. (2004), "A framework for the governance of information security", *Computer & Security*, Vol. 23, pp. 638-46.

قدمت هذه الدراسة ثلاث مخاطر أساسية لنظم المعلومات الآلية: المخاطر الناتجة عن ظواهر طبيعية، والمخاطر الفنية، والمخاطر المرتبطة بالعاملين.

Wright, S. and Wright, A. (2002), "Information system assurance for enterprise resource planning systems: implementation and unique risk considerations", *Journal of Information Systems*, Supplement, Vol. 16, pp. 99-113.

دراسة إستكشافية للوصول إلي تصور حول المخاطر الإستثنائية المرتبطة بتطبيق نظم تخطيط موارد المشروع ERP ، وذلك من خلال لإجراء مجموعة من المقابلات الشخصية. حيث كشفت الدراسة عن إفتقار أنظمة تخطيط موارد المشروع لإجراءات الرقابة والحماية الكافية، وأن إنجاز عملية تحويل البيانات كانت تتم بشكل ردئ وأن هناك احتمال كبير لوجود أخطاء في القوائم المالية ووجود مخاطر تجارية، نتيجة إفتقار المشغلين للتدريب المناسب، كما بينت نتائج الدراسة اختلاف الاختراقات والمخاطر، التي تتعرض لها أنظمة تخطيط موارد المشروع باختلاف التطبيقات والبرامج المستخدمة، وباختلاف حزم برامج الحماية التي يوردها البائعين المختلفين.

وبفحص الدراسات السابقة، تبين أنه لا توجد سوي دراسة واحدة مرتبطة بشكل مباشر بالتحديات الأمنية بالمكتبات الرقمية (Wan, XM ,2008)، وباقي الدراسات ركزت علي أمن نظم المعلومات الآلية في المؤسسات المختلفة بخلاف المؤسسات المعلوماتية. ويتضح عدم تمييز العديد منها بين مخاطر نظم المعلومات الآلية، وعدم فعالية آليات إدارة المخاطر المطبقة. فقد تعاملت العديد منها مع عدم فعالية آليات المخاطر المطبقة، علي أنها تمثل اختراقات وتهديدات لنظم المعلومات الآلية، فمثلاً تم معالجة عدم كفاية بعض اجراءات الرقابة والحماية، مثل القصور في إجراءات الرقابة علي وسائط تخزين البيانات، وعلي آليات تداول المخلات والمخرجات، وعمليات الوصول للنظام، والفصل غير الدقيق بين مسؤوليات ووظائف نظم المعلومات الآلية، وعدم إجراءات الحماية المادية، علي أنها تمثل مخاطر للنظام. كما لم تهتم بعض تلك الدراسات بالفروق في طبيعة المخاطر المتلازمة والمرتبطة بنظم المعلومات الآلية، وإجراءات الرقابة والحماية الملائمة للتصدي لتلك الإختراقات، بين المؤسسات المختلفة. ولم تصنف العديد من الدراسات السابقة المخاطر التي تتعرض لها نظم المعلومات الآلية

أو إجراءات الرقابة والحماية، بحسب مدي إرتباطها بالجوانب المادية وغير المادية للنظام، أو تصنيفها بحسب طبيعة مكونات نظم المعلومات الآلية وما يرتبط بها من مخاطر أو إجراءات رقابية ملائمة، تلك المرتبطة بالجوانب الفنية والجوانب غير الفنية للنظام.

٧. محددات الدراسة :

- اقتصرت الدراسة علي جميع العاملين بمشاريع الرقمنة بمؤسسات المعلومات العربية مما يعملون بالوظائف الإدارية والفنية المختلفة الآتية: (مدير مشروع، مدير تكنولوجيا المعلومات، رئيس قسم، دعم فني، أخصائي معلومات، محرر/كاتب فني، محلل نظم، مصمم ويب، مصمم جرفكس، مهندس/مشرف شبكات، مهندس/مشرف نظم ، مبرمج/مطور ، مدخل بيانات)
- اقتصرت الدراسة علي مشاريع الرقمنة بالمؤسسات المعلوماتية التالية : مكتبة الإسكندرية ، دار الكتب المصرية، مكتبة الملك فهد الوطنية، مكتبة الوراق، مكتبة بيليواسلام، مركز توثيق التراث الحضاري والطبيعي، مكتبة المدينة الرقمية. ومن ناحية أخرى اقتصرت الدراسة على تضمين هذه المشاريع دون غيرها اعتماداً على ملاحظة الباحث المرتبطة بان هذه المشاريع تمثل مشاريع رقمنة كبيرة وهامة لمؤسسات المعلومات في العالم العربي وقد نتجت هذه الملاحظة من خلال استطلاع مبدئي لمواقع هذه المشاريع علي شبكة الويب وما كتب عنها بمصادر المعلومات المختلفة.
- أجريت الدراسة خلال الفصل الدراسي الأول من العام الجامعي ٢٠٠٩ - ٢٠١٠
- اقتصرت الدراسة علي استبانة من إعداد وتطوير الباحث حيث تم التأكد من صدقها وثباتها بالطرق المعروفة؛ لذا فإن صدق النتائج يعتمد علي صدق أداة الدراسة.
- يتحدد تعميم نتائج الدراسة خارج مجتمعها الإحصائي بمدي مماثلة المجتمع الخارجي لمجتمع الدراسة الحالي.

٨. خطوات تنفيذ الدراسة:

لتحقيق أهداف وتساؤلات الدراسة يتبع الباحث الخطوات التالية:

١. تحديد مشكلة الدراسة وأسئلتها ومتغيراتها.

٢. الاطلاع على بعض الدراسات والبحوث السابقة الخاصة بالتحديات والمخاطر الأمنية لمشاريع الرقمنة وأمن نظم المعلومات.

٣. مراجعة الإطار النظري الخاص بالتحديات والمخاطر الأمنية في البيئة الرقمية، مع الاطلاع على تجارب بعض الدول الغربية في هذا المجال..

٤. بناء أداة الدراسة، مع التأكد من صدقها وثباتها.

٥. تحديد مجتمع الدراسة، وعينتها.

٦. توزيع أداة الدراسة على عينة الدراسة.

٧. جمع الأداة وتحليلها، والتوصل إلى النتائج، ومناقشتها، وتقديم التوصيات.

٩. منهجية الدراسة:

في ضوء طبيعة الدراسة والأهداف التي سعت إلى تحقيقها وبناء على الأسئلة التي سعت الدراسة للإجابة عنها، استخدم الباحث المنهج الوصفي التحليلي بأسلوبه المسحي لتحقيق أهداف الدراسة، ذلك أن المنهج الوصفي لا يقتصر على وصف الظاهرة وجمع المعلومات والبيانات عنها، بل يمتد إلى الوصول إلى استنتاجات تسهم في فهم الواقع المراد دراسته وتطويره والذي لا يقف عند حد جمع المعلومات المتعلقة بالظاهرة من أجل استقصاء مظاهرها وعلاقاتها المختلفة، وإنما يعمد كذلك إلى تحليل الظاهرة وتفسيرها والوصول إلى استنتاجات تسهم في تطوير الواقع وتحسينه.

١/٩ أداة الدراسة:

لتحقيق أهداف وأسئلة الدراسة المتمثلة في معرفة التحديات الأمنية لمشاريع الرقمنة بمؤسسات المعلومات العربية، قام الباحث بالإطلاع علي الإنتاج الفكري المتوفر في هذا

المجال كما تم مسح المقاييس المتعلقة بموضوع الدراسة، وقد اعتمد الباحث على الاستبانة كأداة لتجميع البيانات. وقد اشتملت علي مجموعتين من الأسئلة :

المجموعة الأولي: وتتضمن ٢٣ سؤال، تدور حول معدل تكرار حدوث كل نوع من أنواع اختراقات ومخاطر نظم إدارة المحتوي الرقمي بمشاريع الرقمنة بمؤسسات المعلومات العربية المختلفة، مصنفة حسب مكونات نظام إدارة المحتوي الرقمي كما يلي:-

(أ) اختراقات ومخاطر البرامج والتطبيقات وتتكون من:

١. وجود أخطاء في تصميم البرامج والتطبيقات تؤدي إلي إنتاج معلومات خاطئة لفترات طويلة.

٢. قيام مبرمجو ومطوري أنظمة إدارة المحتوي الرقمي بتضمين أوامر خفية تسمح بدخول غير المصرح به إلي النظام أو بإدخال فيروسات الحاسب إليها.

(ب) اخترقات ومخاطر أجهزة وملحقات الحاسب وتتكون من:

١. الوصول غير المصرح به لغرفة الخادم وما يرتبط به من أجهزة من قبل العاملين.

٢. الخسائر والأضرار الناتجة عن إنقطاع التيار الكهربائي.

(ج) اختراقات ومخاطر البيانات ومصادر المعلومات الرقمية وتتكون من:

١. الإدخال المتعمد لبيانات غير سليمة من قبل العاملين.

٢. التدمير المتعمد للبيانات ومصادرالمعلومات من قبل العاملين.

٣. الوصول غير المصرح به للبيانات ومصادر المعلومات من قبل العاملين.

٤. التعديل والتلاعب بمخرجات المعلومات والبيانات.

٥. سرقة بيانات ومعلومات المؤسسة، وإستغلالها في أغراض شخصية.

(د) اختراقات ومخاطر شبكات المعلومات وتتكون من:

١. الوصول غير المصرح به للبيانات أو للنظام من قبل أطراف خارجية (قراصنة الحاسب).

٢. المخاطر الناتجة عن فيروسات الحاسب مثل محو أو إتلاف ملفات البيانات والبرامج وأنظمة تشغيل الحاسب، وشل حركة النظام، وتمكين قراصنة الحاسب من الوصول غير المصرح به إلي النظام والتحكم به عن بعد.

٣. اعتراض بيانات محولة عبر شبكات الحاسب.

(هـ) اختراقات ومخاطر التجهيزات المادية لمحيط عمل النظام وتتكون من:

١. المخاطر الناجمة عن الكوارث الطبيعية مثل الزلازل، البراكين، الفيضانات، السيول، والحرائق.

٢. الإعطال الناجمة عن عدم كفاية التجهيزات المادية للمحافظة علي طريقة عمل الأجهزة بشكل سليم.

(و) اختراقات ومخاطر العاملين وتتكون من:

١. الإدخال غير المتعمد لبيانات غير سليمة من قبل العاملين.

٢. التدمير غير المتعمد للبيانات والمعلومات من قبل العاملين.

٣. تبادل كلمات السر فيما بين العاملين.

٤. الحوادث البشرية مثل الحرائق وفصل التيار الكهربائي.

٥. إصدار أوامر للحاسب تؤدي إلي تشغيل البيانات بطريقة خاطئة بسبب نقص الخبرة والتدريب.

(ز) اختراقات ومخاطر السياسات واللوائح والقوانين وتتكون من:

١. التطورات التكنولوجية السريعة التي تسبق وضع السياسات وإجراءات الرقابة الملائمة.

٢. الأضرار الناجمة عن الفصل غير المناسب بين المسئوليات ومهام نظم إدارة المحتوي الرقمي (مثلاً البرمجة والتشغيل)

٣. الأضرار الناجمة عن عدم تدوير الواجبات والمسئوليات الوظيفية.

٤. الخسائر التجارية والمالية الناجمة عن حالات التوقف والتعطل المفاجئ للنظام.

حيث طلب من المشاركين الإجابة علي تلك الأسئلة بالإختيار من بين خمس إختيارات، للتعبير عن معدل تكرار الإختراقات والمخاطر السابقة {(١) معدل مرة واحدة في السنة، (٢) أكثر من مرة في السنة أو شهرياً، (٣) معدل أكثر من مرة في الشهر أو إسبوعياً، (٤) معدل اكثر من مرة في الإسبوع او يومياً، (٥) معدل أكثر من مرة في اليوم أوبشكل متكرر}

المجموعة الثانية: وتتضمن ٦٣ سؤال، تدور حول طبيعة ونطاق إجراءات الرقابة والحماية، المطبقة للتصدي لتلك الإختراقات والتهديدات التي تتعرض لها نظم إدارة المحتوي الرقمي بمشاريع الرقمنة بمؤسسات المعلومات العربية. مصنفة حسب مكونات نظام إدارة المحتوي الرقمي كما يلي:-

(أ) اجراءات رقابة وحماية البرامج والتطبيقات وتتكون من:

١. توثيق وتسجيل عمليات دخول مستخدمي النظام.
٢. الإحتفاظ بنسخ احتياطية للبرامج ونظم التشغيل المستخدمة.
٣. مراقبة عمليات الوصول إلي النسخ الأصلية للبرامج.
٤. مراقبة ما يتم إجراؤه من تعديلات علي التطبيقات والبرامج المستخدمة.
٥. إجراءات لمنع الكتابة والتسجيل علي وسائط حفظ النسخ الإحتياطية للبرامج.
٦. الإحتفاظ بالنسخ الأصلية للبرامج والتطبيقات في مكان يقع خارج موقع الخادم.
٧. التقصي والتقرير عن عمليات الدخول غير المرخص بها للنظام.
٨. تحديد صلاحيات تتناسب مع كل مستوي من مستويات الوصول للنظام.
٩. مراقبة عمليات منح وإبطال آليات الوصول للنظام (مثل بطاقات الهوية، أو كلمات المرور)
١٠. التحقق من تغيير كلمات المرور بشكل دوري، وأن يكون من الصعب تخمينها.
١١. التحقق من عدم الكشف عن كلمات المرور والإحتفاظ بها بشكل سري (مثلاً عدم كتابتها أو إظهارها علي شاشة الحاسب).

١٢. التحقق من إبطال آليات الوصول لمن لم يعد يعمل لدي المؤسسة أو تم نقلهم لأقسام وفروع أخري.

١٣. التحقق من خضوع كل الإجراءات السابقة لإشراف ومراقبة من قبل موظف مسئول.

١٤. وضع إجراءات لرقابة عمليات تطوير البرامج والتطبيقات والتحقق من توافر آليات الحماية بالتطبيقات المطورة داخلياً أو الجاهزة المشتراه.

(ب) اجراءات رقابة وحماية أجهزة وملحقات الحاسب وتتكون من:

١. وجود قيود علي الدخول لغرفة الخادم.

٢. تثبيت أجهزة الحاسب، بحيث لا يمكن تحريكها، في أماكن مقفلة تخضع للمراقبة في حالات عدم تشغيلها.

٣. استخدام مصدر للطاقة الإحتياطية، لتوليد الطاقة في حالات إنقطاع التيار الكهربائي.

٤. مراقبة محاولات الوصول إلي الوحدات الطرفية للحاسب، أو غرفة الخادم، أو أجهزة ومعدات الحاسب التي توجد خارج غرفة الخادم.

٥. وجود إجراءات رقابية كافية علي إعداد أو إبطال آليات الوصول المادي مثل المفاتيح.

٦. التحقق من خضوع كل الإجراءات المتعلقة بالوصول المادي لإشراف ومراقبة من قبل موظف مسئول.

(ج) اجراءات رقابة وحماية البيانات ومصادر المعلومات الرقمية وتتكون من:

١. وجود إجراءات رقابة كافية علي تداول مدخلات ومخرجات النظام، بين الأقسام المختلفة.

٢. إعداد النسخ الإحتياطية للبيانات ومصادر المعلومات بصورة روتنية.

٣. حماية النسخ الإحتياطية من إعادة الكتابة أو التسجيل عليها.

٤. الإحتفاظ بالنسخ الإحتياطية في مكان آمن خارج غرفة الخادم.

٥. تشفير النسخ الإحتياطية للبيانات والمعلومات الهامة.
٦. إستخدام أكثر من تقنية لعمل النسخ الإحتياطية.
٧. إبطال أمر تهيئة Format
٨. تشفير البيانات الحساسة مثل بيانات المستفيدين والموظفين.
٩. إغلاق أجهزة الحاسب غير المستخدمة، لمنع الإطلاع عليها، والتعديل في البيانات.
١٠. حصر أنواع مصادر المعلومات وتصنيفها إلي فئات، وفقاً لدرجة أهميتها وحساسيتها، وتحديد مستوي الحماية الواجب توفيره لكل فئة.
١١. تحديد الصلاحيات المرتبطة بكل مستوي من مستويات الوصول للبيانات.
١٢. تسجيل العمليات والمعالجات التي تتم علي البيانات والمعلومات أول بأول.
١٣. رقابة كافية علي إدارة مكتبات وسائط تخزين البيانات ومصادر المعلومات الرقمية القابلة للنقل والتداول مثل الأقراص والأشرطة.
١٤. وجود إجراءات تنظم عملية التخلص من وسائط تخزين البيانات.

(د) اجراءات رقابة وحماية شبكات المعلومات وتتكون من:

١. استخدام برامج الحماية لاكتشاف وإزالة فيروسات الحاسب والبرامج الضارة.
٢. استخدام أنظمة التكويد والتشفير للبيانات التي يتم نقلها وتداولها عبر شبكات النظام.
٣. استخدام برامج حوائط النار Firewalls لصد الوصول غير المشروع إلي الشبكات المتصلة بالإنترنت.
٤. مد وصلات خطوط الإتصال داخل أنابيب أمنة، تمتد خارج غرفة الحاسب الآلي، لمنع النسخ أو التجسس علي البيانات والمعلومات المتداولة عبر شبكات الحاسب.
٥. وجود ضوابط رقابية لمنع الوصول غير المشروع إلي شبكات الحاسب، من قبل الإطراف الخارجية، عن طريق الإتصال هاتفياً Dial-Up.
٦. تطبيق الضوابط الملائمة لتأمين رسائل البريد الإلكتروني والمعلومات المنشورة علي مواقع الويب، وتبادل البيانات إلكترونياً، والإتصالات بكافة أنواعها.

(هـ) اجراءات رقابة وحماية التجهيزات المادية لمحيط عمل النظام وتتكون من:

١. توافر واستخدام طفايات الحريق وتوزيعها بشكل سليم.

٢. وضع أجهزة ومعدات الحاسب في أماكن بعيدة عن مضخات المياه.

٣. استخدام أغطية واقية من الأتربة والماء لتجنب الأضرار الناجمة عنها.

٤. حظر التدخين واستخدام مراوح صغيرة لدفع الأدخنة بعيداً عن أجهزة الحاسب.

٥. وجود أجهزة تكييف في غرفة الخادم. وأماكن تواجد الأجهزة والمعدات.

٦. استخدام أجهزة للوقاية ضد الزلازل زالإهتزازات.

(و) اجراءات رقابة وحماية العاملين وتتكون من:

١. وجود إجراءات لرقابة وحماية سرية المعلومات، مع توعية العاملين بالمسئولية الأخلاقية التي يجب مراعاتها عند التعامل مع المعلومات الخاصة.

٢. وجود إجراءات تنظم عملية التخلص من البيانات غير السليمة.

٣. الإستعانة باستشارات المتخصصين في حماية نظم إدارة المحتوي الرقمي.

٤. تطبيق إجراءات مراجعة دورية وغير دورية لتحقق من مستوي الحماية المتاح للنظام.

٥. تدريب العاملين علي الإجراءات السليمة والأمنة لتشغيل النظام.

٦. عقد برامج لتوعية العاملين بالمخاطر التي تتعرض لها نظم إدارة المحتوي الرقمي، والضوابط والوسائل الملائمة لمواجهتها.

٧. تدريب العاملين علي استخدام قنوات الإتصال المتاحة للتبليغ والتقرير عن الأعطال والإختراقات الأمنية الطارئة.

٨. توعية العاملين بدورهم في حماية كلمات المرور الخاصة بهم.

(ز) اجراءات رقابة وحماية السياسات واللوائح والقوانين وتتكون من:

١. وجود سياسة لأمن البيانات ومصادر المعلومات الرقمية معلنة ومكتوبة، تحدد موقف الإدارة العليا من أمن المعلومات، وكيفية تحقيق الأمن، وتحقيق التكامل بين تلك

السياسة والسياسات الأخري بالمؤسسة.

٢. تحديد مسئوليات كل وظيفة عن عمليات الحماية المرتبطة بها.

٣. وضع خطط طوارئ معلنة وموثقة، لإستمرارية الأعمال، توضح الإجراءات التي يجب إتباعها في حالات الكوارث وتعطل وتوقف النظام.

٤. تدوير الواجبات والمسئوليات الوظيفية، لزيادة فرص اكتشاف الأخطاء والمخالفات.

٥. الأعطال الإجبارية كوسيلة لتقليص احتمال التلاعب بالنظام.

٦. اشتمال سياسات التعيين علي التحقق من سيرة العاملين، لتجنب تعيين أفراد غير أمناء.

٧. مراعاة القوانين التي تحمي حقوق الملكية الفكرية (مثل ترخيص إستخدام البرامج والتطبيقات ومصادر المعلومات)، وحماية خصوصة المعلومات الخاصة بالمستفيدين.

٨. إتباع سياسة التأمين ضد الخسائر الناجمة عن إختراقات النظام.

٩. إستقلالية المسئول عن مراقبة محاولات الوصول المادي عن عمليات البرمجة وبرامج النظام ومسئوليات الرقابة الأخري.

حيث طلب من المشاركين الإجابة علي تلك الأسئلة بالإختيار من بين خمس إختيارات، للتعبير عن مدي توافر إجراءات الرقابة والحماية السابقة {(١) غير مطبق، (٢) مطبق بشكل غير مرضي، (٣) مطبق بشكل مقبول، (٤) مطبق بشكل جيد، (٥) مطبق بطريقة سليمة}

٢/٩ صدق أداة الدراسة:

لقد تم إعداد الإستبانة بمراجعة شاملة لأهم الدراسات والبحوث السابقة، والمراجع ذات العلاقة بموضوع الدراسة والتي من خلالها تم التوصل إلى المسودة الأولى للاستبانة. وتعد مصداقية المحتوى Content validity أحد الأساليب المستخدمة لقياس مصداقية الاستبانة بشكل عام. ويستخدم هذا الأسلوب لقياس لغة وبناء التساؤلات بالإضافة إلى

التأكد من إمكانية قياس الأسئلة لما ينبغي أن يقاس. وفى هذا النطاق استخدمت الدراسة الحالية مصداقية المحتوى بالاعتماد على ما يطلق عليه رأى المحكمين من خلال تحكيم الاستبانة من قبل ثلاثة من أساتذة المكتبات وتكنولوجيا المعلومات للتأكد من جودة، البناء والصياغة اللغوية والتسلسل المنطقي للتساؤلات ومدى ارتباطها بتساؤلات الدراسة. وقد أسفر التحكيم عن إدخال بعض التعديلات الخاصة بصياغة التساؤلات.

٣/٩ ثبات أداة الدراسة:

لقد تم حساب معامل الثبات النهائي لأداة الدراسة باستخدام معامل ألفا كرونباخ Alpha Cronbach ، والجدول التالي رقم (1) يبين معاملات ثبات مجموعات الأسئلة في إداة الدراسة.

جدول رقم (١) معاملات ثبات مجموعات الأسئلة معامل ألفا كرونباخ

المجال	عدد الفقرات	معامل الثبات
الإختراقات والمخاطر		
(أ) اختراقات ومخاطر البرامج والتطبيقات	٢	0.84
(ب) اخترقات ومخاطر أجهزة وملحقات الحاسب	٢	0.85
(ج) اختراقات ومخاطر البيانات ومصادر المعلومات الرقمية	٥	0.94
(د) اختراقات ومخاطر شبكات المعلومات	٣	0.83
(هـ) اختراقات ومخاطر التجهيزات المادية لمحيط عمل النظام	٢	0.81
(و) اختراقات ومخاطر العاملين	٥	0.90
(ز) اختراقات ومخاطر السياسات واللوائح والقوانين	٤	0.93
إجراءات الرقابة والحماية:		
(أ) اجراءات رقابة وحماية البرامج والتطبيقات	١٤	0.81
(ب) اجراءات رقابة وحماية أجهزة وملحقات الحاسب	٦	0.85
(ج) اجراءات رقابة وحماية البيانات ومصادر المعلومات الرقمية	١٤	0.83
(د) اجراءات رقابة وحماية شبكات المعلومات	٦	0.85

(هـ) اجراءات رقابة وحماية التجهيزات المادية لمحيط عمل النظام	٦	0.89
(و) اجراءات رقابة وحماية العاملين	٨	0.92
(ز) اجراءات رقابة وحماية السياسات واللوائح والقوانين	٩	0.82

من هنا يتبين بأن اداة الدراسة تتصف بخصائص جيدة من صدق وثبات مما يعني أن الإستدلالات التي ستخرج بها هذه الدراسة ستكون مرتبطة وبدقة بما تم قياسه من خلال أداة الدراسة.

٤/٩ مجتمع الدراسة:

تألف مجتمع الدراسة من جميع العاملين بمشاريع الرقمنة بمؤسسات المعلومات العربية مما يعملون بالوظائف الإدارية والفنية المختلفة مثل (مدير مشروع، مدير تكنولوجيا المعلومات، رئيس قسم، دعم فني، أخصائي معلومات، محرر/كاتب فني، محلل نظم، مصمم ويب، مصمم جرفكس، مهندس/مشرف شبكات، مهندس/مشرف نظم ، مبرمج أومطور، مدخل بيانات ... ألخ)

و قد فرض التشتت الجغرافي لمجتمع الدراسة استخدام الاستبيان الالكتروني عن طريق الويب لجمع البيانات بالاعتماد على موقع www.surveymonkey.com والجدير بالذكر أن المرونة و سهولة الاستخدام من أبرز مميزات الاستبيانات الالكترونية عن طريق الويب، فهي تساهم بشكل كبير فى التغلب على العديد من المشكلات مثل إدراج الرسومات وتطويع المقاييس المستخدمة كمقياس ليكرت، بالإضافة إلى تفعيل التعامل مع المبحوثين باستخدام الواجهة الرسومية. وقد ساعدت الاستبيانات الالكترونية على تفعيل إدارة الباحث للإجابات والتغلب إلى حد ما على المشاكل التي تكتنف الاستبيانات البريدية مثل الوقت والتكلفة وضعف العائد من الاستبيان. وقد تم مخاطبة المسئولين بمشروعات الرقمنة محل الدراسة وأخذ الموافقة علي ان يتم إرسال بريد إلكتروني من قبل المؤسسة لجميع العاملين Broadcast يحتوي علي الرابط الخاص بالإستبانة. وقد بلغ عدد المستجبين بجميع مشاريع الرقمنة محل الدراسة ١٤٨ مستجيب، ويوضح

الجدول رقم (٢) و (٣) توزيع أفراد عينة الدراسة وفقاً للوظيفة ومشروع الرقمنة التابع له.

جدول رقم (٢) توزيع عينة الدراسة حسب الوظيفة

الوظيفة	العدد	النسبة
مدير مشروع	٣	%٢,٨٠
مدير تكنولوجيا المعلومات	٥	%٤,٦٧
رئيس قسم	١٠	%٩,٣٤
مهندس/مشرف شبكات	٦	%٥,٦٠
مهندس/مشرف نظم	٥	%٤,٦٧
مبرمج أومطور	١٢	%١٢,٢١
أخصائي دعم فني	١٣	%١٢,١٤
أخصائي مكتبات ومعلومات	٢٠	%١٨,٦٩
محرر/كاتب فني	٧	%٦,٥٤
محلل نظم	٤	%٣,٣٧
مصمم ويب	٤	%٣,٣٧
مصمم جرفكس	٣	%٢,٨٠
مدخل بيانات	١٥	%١٤,٠١
المجموع	**107**	%١٠٠

جدول رقم (٣) توزيع عينة الدراسة حسب مشروع الرقمنة

مشروع الرقمنة	العدد	النسبة
المستودع الرقمي لمكتبة الإسكندرية	٢٦	%٢٤,٢٩
دار الكتب المصرية	١٥	%١٤,٠١
مكتبة الملك فهد الوطنية	٩	%٨,٤١
ببليواسلام	١٥	%١٤,٠١
الوراق	١٨	%١٦,٨٢
مكتبة المدينة الرقمية	٧	%٦,٥٤
مركز توثيق التراث الحضاري والطبيعي	١٧	%١٥,٨٨
المجموع	**١٠٧**	%١٠٠

١٠. نتائج الدراسة:

توضح الجدول رقم (٤، ٥، ٦، ٧، ٨، ٩، ١٠) مستوي المخاطر التي تتعرض لها مشاريع الرقمنة بمؤسسات المعلومات العربية، حيث تم تصنيف مستويات المخاطر إلي ثلاث مستويات:

- **مخاطر غير متكررة:** حيث متوسط قياسات الإختراقات المحتملة لمكونات نظم إدارة المحتوي الرقمي ≥٣، بمعني أن متوسط معدل حدوث الإختراقات والمخاطر يعادل أو أقل من مرة في الشهر أو أسبوعياً.
- **مخاطر شبه متكررة:** حيث متوسط الإختراقات والتهديدات المحتملة لمكونات نظم إدارة المحتوي الرقمي >٣، بمعني أن متوسط معدل حدوث الإختراقات والمخاطر اكثر من مرة في الشهر أو أسبوعياً، و≤ ٤، بمعني أن متوسط معدل حدوث الإختراقات والمخاطر يعادل أو أقل من مرة في الإسبوع أو يومياً).
- **مخاطر متكررة:** حيث متوسط قياسات الاختراقات والتهديدات المحتملة لأصول نظم إدارة المحتوي الرقمي >4، بمعني أن متوسط معدل حدوث الإختراقات والمخاطر أكثر من مرة في الأسبوع أو يومياً.

جدول رقم (٤) متوسط الإختراقات والتهديدات المحتملة لمكونات نظام إدارة المحتوي الرقمي بمشروع مكتبة الوراق الرقمية

م	مكونات نظم إدارة المحتوي الرقمي	المتوسط الحسابي	الإنحراف المعياري	مستوي المخاطرة
أ	اختراقات ومخاطر البرامج والتطبيقات	2.76	1.18	غير متكررة
ب	اختراقات ومخاطر أجهزة وملحقات الحاسب	2.22	1.14	غير متكررة
ج	اختراقات ومخاطر البيانات ومصادر المعلومات الرقمية	2.43	1.33	غير متكررة
د	اختراقات ومخاطر شبكات المعلومات	3.59	1.20	**شبه متكررة**
هـ	اختراقات ومخاطر التجهيزات المادية لمحيط عمل النظام	2.54	1.17	غير متكررة
و	اختراقات ومخاطر العاملين	2.88	1.38	غير متكررة
ز	اختراقات ومخاطر السياسات واللوائح والقوانين	2.15	1.08	غير متكررة

يتضح من الجدول السابق أن أكثر مكونات نظم إدارة المحتوي الرقمي بمشروع الوراق، تعرض للإختراقات والمخاطر هو شبكات المعلومات بمستوي مخاطرة شبه متكررة. أما مستوي المخاطر والإختراقات التي تتعرض لها باقي مكونات النظام، فتعتبر غير متكررة.

جدول رقم (٥) متوسط الإختراقات والتهديدات المحتملة لمكونات نظام إدارة المحتوي الرقمي بدار الكتب المصرية

م	مكونات نظم إدارة المحتوي الرقمي	المتوسط الحسابي	الإنحراف المعياري	مستوي المخاطرة
أ	اختراقات ومخاطر البرامج والتطبيقات	3.27	1.22	شبه متكررة
ب	اختراقات ومخاطر أجهزة وملحقات الحاسب	2.70	1.13	غير متكررة
ج	اختراقات ومخاطر البيانات ومصادر المعلومات الرقمية	4.33	1.26	متكررة
د	اختراقات ومخاطر شبكات المعلومات	4.32	1.26	متكررة
هـ	اختراقات ومخاطر التجهيزات المادية لمحيط عمل النظام	2.34	1.20	غير متكررة
و	اختراقات ومخاطر العاملين	3.30	1.25	شبه متكررة
ز	اختراقات ومخاطر السياسات واللوائح والقوانين	2.55	1.27	غير متكررة

يتضح من الجدول السابق أن أكثر أصول نظم إدارة المحتوي الرقمي في مشروع رقمنة دار الكتب المصرية، تعرض للاختراقات والتهديدات هو شبكات المعلومات والبيانات ومصادر المعلومات الرقمية بمستوي مخاطرة متكررة، يليها البرامج والتطبيقات والعاملين بمستوي مخاطرة شبه متكررة. أما مستوي المخاطر والإختراقات التي تتعرض لها باقي مكونات النظام، فتعتبر غير متكررة.

جدول رقم (٦) متوسط الإختراقات والتهديدات المحتملة لمكونات نظام إدارة المحتوي الرقمي بمكتبة الملك فهد الوطنية

م	مكونات نظم إدارة المحتوي الرقمي	المتوسط الحسابي	الإنحراف المعياري	مستوي المخاطرة
أ	اختراقات ومخاطر البرامج والتطبيقات	3.75	0.83	شبه متكررة
ب	اختراقات ومخاطر أجهزة وملحقات الحاسب	2.49	0.85	غير متكررة

ج	اختراقات ومخاطر البيانات ومصادر المعلومات الرقمية	3.60	1.32	شبه متكررة
د	اختراقات ومخاطر شبكات المعلومات	4.22	0.76	متكررة
هـ	اختراقات ومخاطر التجهيزات المادية لمحيط عمل النظام	3.35	0.52	شبه متكررة
و	اختراقات ومخاطر العاملين	3.79	0.99	شبه متكررة
ز	اختراقات ومخاطر السياسات واللوائح والقوانين	4.55	0.53	متكررة

يتضح من الجدول السابق أن أكثر أصول نظم إدارة المحتوي الرقمي في مشروع الرقمنة بمكتبة الملك فهد الوطنية، تعرض للاختراقات والتهديدات هوشبكات المعلومات، السياسات واللوائح والقوانين بمستوي مخاطرة متكررة، يليها العاملين، والبرامج والتطبيقات ثم البيانات ومصادر المعلومات الرقمية، والتجهيزات المادية لمحيط عمل النظام بمستوي مخاطرة شبه متكررة. أما مستوي المخاطر والإختراقات التي تتعرض أجهزة وملحقات الحاسب ، فتعتبر غير متكررة.

جدول رقم (٧) متوسط الإختراقات والتهديدات المحتملة لمكونات نظام إدارة المحتوي الرقمي بمكتبة الأسكندرية

م	مكونات نظم إدارة المحتوي الرقمي	المتوسط الحسابي	الإنحراف المعياري	مستوي المخاطرة
أ	اختراقات ومخاطر البرامج والتطبيقات	3.59	0.88	شبه متكررة
ب	اختراقات ومخاطر أجهزة وملحقات الحاسب	2.18	0.79	غير متكررة
ج	اختراقات ومخاطر البيانات ومصادر المعلومات الرقمية	2.57	1.44	غير متكررة
د	اختراقات ومخاطر شبكات المعلومات	4.30	0.54	متكررة
هـ	اختراقات ومخاطر التجهيزات المادية لمحيط عمل النظام	2.51	1.19	غير متكررة
و	اختراقات ومخاطر العاملين	3.72	0.89	شبه متكررة
ز	اختراقات ومخاطر السياسات واللوائح والقوانين	3.85	0.85	شبه متكررة

جدول رقم (٨) متوسط الإختراقات والتهديدات المحتملة لمكونات نظام إدارة المحتوي الرقمي بمركز توثيق التراث الحضاري والطبيعي

م	مكونات نظم إدارة المحتوي الرقمي	المتوسط الحسابي	الإنحراف المعياري	مستوي المخاطرة
أ	اختراقات ومخاطر البرامج والتطبيقات	3.23	1.35	**شبه متكررة**
ب	اختراقات ومخاطر أجهزة وملحقات الحاسب	2.44	1.03	غير متكررة
ج	اختراقات ومخاطر البيانات ومصادر المعلومات الرقمية	2.54	1.28	غير متكررة
د	اختراقات ومخاطر شبكات المعلومات	4.36	0.65	**متكررة**
هـ	اختراقات ومخاطر التجهيزات المادية لمحيط عمل النظام	2.41	0.89	غير متكررة
و	اختراقات ومخاطر العاملين	3.66	1.25	**شبه متكررة**
ز	اختراقات ومخاطر السياسات واللوائح والقوانين	3.68	1.29	**شبه متكررة**

جدول رقم (9) متوسط الإختراقات والتهديدات المحتملة لمكونات نظام إدارة المحتوي الرقمي بمكتبة بيليو اسلام

م	مكونات نظم إدارة المحتوي الرقمي	المتوسط الحسابي	الإنحراف المعياري	مستوي المخاطرة
أ	اختراقات ومخاطر البرامج والتطبيقات	3.32	1.23	**شبه متكررة**
ب	اختراقات ومخاطر أجهزة وملحقات الحاسب	2.67	1.06	غير متكررة
ج	اختراقات ومخاطر البيانات ومصادر المعلومات الرقمية	2.80	1.05	غير متكررة
د	اختراقات ومخاطر شبكات المعلومات	4.24	0.77	**متكررة**
هـ	اختراقات ومخاطر التجهيزات المادية لمحيط عمل النظام	2.35	1.10	**غير متكررة**
و	اختراقات ومخاطر العاملين	3.39	1.18	**شبه متكررة**
ز	اختراقات ومخاطر السياسات واللوائح والقوانين	3.59	1.29	**شبه متكررة**

جدول رقم (10) متوسط الإختراقات والتهديدات المحتملة لمكونات نظام إدارة المحتوي الرقمي بمكتبة المدينة الرقمية

م	مكونات نظم إدارة المحتوي الرقمي	المتوسط الحسابي	الإنحراف المعياري	مستوي المخاطرة
أ	اختراقات ومخاطر البرامج والتطبيقات	3.27	1.18	**شبه متكررة**
ب	اختراقات ومخاطر أجهزة وملحقات الحاسب	2.54	1.13	غير متكررة

ج	اختراقات ومخاطر البيانات ومصادر المعلومات الرقمية	2.85	1.35	غير متكررة
د	اختراقات ومخاطر شبكات المعلومات	4.33	0.75	متكررة
هـ	اختراقات ومخاطر التجهيزات المادية لمحيط عمل النظام	2.62	1.22	غير متكررة
و	اختراقات ومخاطر العاملين	3.57	0.85	شبه متكررة
ز	اختراقات ومخاطر السياسات واللوائح والقوانين	3.88	0.94	شبه متكررة

يتضح من الجدول رقم (٧، ٨، ٩، ١٠) أن أكثر أصول نظم إدارة المحتوي الرقمي في مشروع الرقمنة بمكتبة الأسكندرية، مركز توثيق التراث الحضاري والطبيعي، ببليواسلام، ومكتبة المدينة الرقمية، تعرض للاختراقات والتهديدات هو شبكات المعلومات بمستوي مخاطرة متكررة، يليها البرامج والتطبيقات والعاملين والسياسات والوائح والقوانين بمستوي مخاطرة شبه متكررة. أما مستوي المخاطر والإختراقات التي تتعرض لها باقي أصول النظام في االمشاريع الأربعة، فتعتبر غير متكررة.

يتضح مما سبق أن أكثر مشروع رقمنة عرضه للمخاطر والإختراقات هو بدار الكتب المصرية ومكتبة الملك فهد الوطنية، يليه بمكتبة الأسكندرية، ومركز توثيق التراث الحضاري والطبيعي، ببليواسلام، ومكتبة المدينة الرقمية، حيث تعتبر المخاطر التي تتعرض لها شبكات المعلومات بمكتبة الوراق شبه متكررة، في حين أنها تعتبر متكررة في المؤسسات الأخري.

وفي حالة تصنيف المخاطر إلي مخاطر داخلية وخارجية، يتضح أن الإدخال غير المتعمد لبيانات غير سليمة، والتدمير المتعمد للبيانات من قبل العاملين، وإدخال الفيروسات إلي أنظمة الحاسب، وسوء توجيه عمليات الطباعة ووصول المعلومات إلي أفراد غير مرخص لهم استلامها، من أكثر المخاطر التي تواجه نظم إدارة المحتوي الرقمي بمشاريع الرقمنة بمؤسسات المعلومات العربية. حيث توضح الدراسة إن أخطر التهديدات وعمليات الإختراق تأتي من داخل المؤسسة وليس من خارجها، حيث يشكل

العاملون ممن لديهم صلاحيات الوصول للنظام، تهديد خطير للنظام، فقد يرتكب بعض العاملون ممن يتصفوا بالأمانة، بعض التصرفات غير المتعمدة، نتيجة الإرهاق أو نقص التدريب الكافي والملائم، مما يترتب عنه محو أو تدمير كميات كبيرة من البيانات والمعلومات الهامة. كما قد يسئ البعض الأخر استخدام الصلاحيات الممنوحة لهم في عمليات تلاعب بقصد تحقيق مكاسب خاصة أو التسبب في ضرر المؤسسة.

جدول رقم (١١) مستوي إجراءات الرقابة والحماية الواجبة

م	مكونات نظم إدارة المحتوي الرقمي	الوراق	دار الكتب المصرية	مكتبة الملك فهد الوطنية	مكتبة الأسكندرية الرقمية	مركز توثيق التراث الحضاري	ببليواسلام	مكتبة المدينة الرقمية
أ	البرامج والتطبيقات	3	3.25	3.75	3.25	3.25	3.25	3.50
ب	أجهزة وملحقات الحاسب	٣	3	٣	٣	٣	٣	٣
ج	البيانات ومصادر المعلومات الرقمية	٣	4.25	3.50	٣	٣	٣	٣
د	شبكات المعلومات	3.5	4.25	4.25	4.25	4.50	4.25	4.50
هـ	التجهيزات المادية لمحيط عمل النظام	3	3	3	3	3	3	3
و	العاملين	٣	3.25	4	3.75	3.50	3.50	3.75
ز	السياسات واللوائح والقوانين	٣	3	4.5	4	3.75	3.75	4
	مستوي الرقابة الواجبة	منخفضة	مرتفعة	مرتفعة	متوسطة	متوسطة	متوسطة	متوسطة

يوضح الجدول رقم (١١) مستوي إجراءات الرقابة والتأمين الواجب تطبيقها لتوفير الحماية الازمة لمكونات نظام إدارة المحتوي الرقمي بمشاريع الرقمنة في مؤسسات المعلومات العربية محل الدراسة. حيث تم تحديد مستوي الحماية الواجب تطبيقه علي أساس مستوي المخاطر والتهديدات التي تتعرض لها، والموضحة في الجزء السابق. وقد تم تحديد مستويات الرقابة وفقاً للقواعد التالية حيث تبدأ مستويات القياس لإجراءات الرقابة والحماية الواجب تطبيقها من ٦٠% وكلما زاد مستوي المخاطر والتهديدات

الأمنية المحتملة، كلما زاد مستوي الرقابة والحماية الواجب تطبيقه. فإذا كان مستوي المخاطر المحتملة ≥٣ غير متكررة، فإن مستوي الرقابة الواجب تطبيقه يعادل ٦٠% من إجراءات الرقابة والحماية المتاحة، وإذا كان مستوي المخاطر المحتملة <٣ و ≥٤ شبه متكررة، فان مستوي الرقابة والحماية الواجب تطبيقه يقع في المدي من ٦٥% إلي ٨٠% من إجراءات الرقابة والحماية المتاحة، وإذا كان مستوي المخاطر المحتملة <٤ متكررة، فان مستوي الرقابة الواجب تطبيقه يقع في المدي من ٨٥% إلي ٩٠% من إجراءات الرقابة المتاحة.

وتوضح الجداول رقم (١٢، ١٣، ١٤، ١٥، ١٦، ١٧، ١٨)، متوسط قياسات الإجراءات المطبقة لرقابة وحماية مكونات نظم إدارة المحتوي الرقمي بمشاريع الرقمنة بمؤسسات المعلومات العربية، حيث تم تصنيف مستويات الرقابة والحماية إلي ثلاث مستويات:

- **مستوي الرقابة الكافية:** والذي يشير إلي كفاية إجراءات الرقابة المطبقة لحماية مكونات نظم إدارة المحتوي الرقمي، وذلك عندما يكون مستوي الرقابة المطبقة ≤ ٩٠% من مستوي الرقابة والحماية الواجبة.
- **مستوي الرقابة غير كافية:** والذي يشير إلي عدم كفاية إجراءات الرقابة المطبقة لحماية مكونات نظم إدارة المحتوي الرقمي، وذلك عندما يكون مستوي الرقابة المطبقة <٩٠% و ≤ ٦٥% من مستوي الرقابة والحماية الواجبة.
- **مستوي الرقابة الضعيفة:** والذي يشير إلي قصور وضعف إجراءات الرقابة المطبقة لحماية مكونات نظم إدارة المحتوي الرقمي، وذلك عندما يكون مستوي الرقابة المطبقة <٦٥% من مستوي الرقابة الواجبة.

جدول رقم (١٢) متوسط قياسات الإجراءات المطبقة لرقابة وحماية مكونات نظام إدارة المحتوي الرقمي بمشروع مكتبة الوراق الرقمية

م	المحاور	المتوسط الحسابي	الإنحراف المعياري	مستوي الرقابة
أ	اجراءات رقابة وحماية البرامج والتطبيقات	3.29	1.39	كافية (١٠٨%)
ب	اجراءات رقابة وحماية أجهزة وملحقات الحاسب	3.37	1.37	كافية (١١٢%)
ج	اجراءات رقابة وحماية البيانات ومصادر المعلومات الرقمية	3.37	1.37	كافية (١١٢%)
د	اجراءات رقابة وحماية شبكات المعلومات	2.17	1.12	**ضعيفة** (٦١%)
هـ	اجراءات رقابة وحماية التجهيزات المادية لمحيط عمل النظام	3.37	1.37	كافية (١١٢%)
و	اجراءات رقابة وحماية العاملين	2.29	1.55	**غير كافية**
ز	اجراءات رقابة وحماية السياسات واللوائح والقوانين	1.85	1.08	**ضعيفة** (٦٠%)

يتضح من الجدول السابق أن شبكات المعلومات (والتي تتعرض لمخاطر شبه متكررة) والسياسات واللوائح والقوانين (والتي تتعرض لمخاطر شبه متكررة)، تتمتع بمستوي حماية ضعيفة. وأن العاملين (والتي تتعرض لمخاطر غير متكررة) تتمتع بمستوي حماية غير كافية. أما باقي مكونات نظام إدارة المحتوي الرقمي فتتمتع بمستوي حماية كافية.

جدول رقم (١٣) متوسط قياسات الإجراءات المطبقة لرقابة وحماية مكونات نظام إدارة المحتوي الرقمي بدار الكتب المصرية

م	المحاور	المتوسط الحسابي	الإنحراف المعياري	مستوي الرقابة
أ	اجراءات رقابة وحماية البرامج والتطبيقات	3.12	1.33	كافية (٩٥%)
ب	اجراءات رقابة وحماية أجهزة وملحقات الحاسب	2.95	1.56	كافية (٩٨%)

ج	اجراءات رقابة وحماية البيانات ومصادر المعلومات الرقمية	3.09	1.56	غير كافية
د	اجراءات رقابة وحماية شبكات المعلومات	2.55	1.34	ضعيفة (٥٨%)
هـ	اجراءات رقابة وحماية التجهيزات المادية لمحيط عمل النظام	2.75	1.47	كافية (٩٢%)
و	اجراءات رقابة وحماية العاملين	2.19	1.27	غير كافية
ز	اجراءات رقابة وحماية السياسات واللوائح والقوانين	2.15	1.29	غير كافية

يتضح من الجدول السابق أن شبكات المعلومات (والتي تتعرض لمخاطر متكررة)، تتمتع بمستوي حماية ضعيفة. وأن البيانات والمعلومات (والتي تتعرض لمخاطر غير متكررة) تتمتع بمستوي حماية غير كافية. أما باقي مكونات نظام إدارة المحتوي الرقمي فتتمتع بمستوي حماية كافية.

جدول رقم (١٤) متوسط قياسات الإجراءات المطبقة لرقابة وحماية مكونات نظام إدارة المحتوي الرقمي بمكتبة الملك فهد الوطنية

م	المحاور	المتوسط الحسابي	الإنحراف المعياري	مستوي الرقابة
أ	اجراءات رقابة وحماية البرامج والتطبيقات	3.56	0.83	كافية (٩٦%)
ب	اجراءات رقابة وحماية أجهزة وملحقات الحاسب	3.45	0.83	كافية (١١١%)
ج	اجراءات رقابة وحماية البيانات ومصادر المعلومات الرقمية	3.87	0.99	كافية (١٠٧%)
د	اجراءات رقابة وحماية شبكات المعلومات	3.18	1.18	غير كافية
هـ	اجراءات رقابة وحماية التجهيزات المادية لمحيط عمل النظام	3.88	0.99	كافية (١١٠%)
و	اجراءات رقابة وحماية العاملين	3.76	1.23	كافية (٩١%)
ز	اجراءات رقابة وحماية السياسات واللوائح والقوانين	2.86	1.1.49	ضعيفة (٦٢%)

يتضح من الجدول السابق أن السياسات واللوائح والقوانين (والتي تتعرض لمخاطر متكررة)، تتمتع بمستوي حماية ضعيفة. وأن شبكات المعلومات (والتي تتعرض لمخاطر متكررة) تتمتع بمستوي حماية غير كافية. أما باقي مكونات نظام إدارة المحتوي الرقمي فتتمتع بمستوي حماية كافية

جدول رقم (١٥) متوسط قياسات الإجراءات المطبقة لرقابة وحماية مكونات نظام إدارة المحتوي الرقمي بمكتبة الأسكندرية

م	المحاور	المتوسط الحسابي	الإنحراف المعياري	مستوي الرقابة
أ	اجراءات رقابة وحماية البرامج والتطبيقات	3.51	0.55	كافية (٩٢%)
ب	اجراءات رقابة وحماية أجهزة وملحقات الحاسب	3.22	0.85	كافية (١٠٥%)
ج	اجراءات رقابة وحماية البيانات ومصادر المعلومات الرقمية	3.13	1.32	كافية (١٠٠%)
د	اجراءات رقابة وحماية شبكات المعلومات	2.71	0.88	ضعيفة (٦٠%)
هـ	اجراءات رقابة وحماية التجهيزات المادية لمحيط عمل النظام	2.97	0.85	كافية (٩٢%)
و	اجراءات رقابة وحماية العاملين	3.10	1.23	غير كافية
ز	اجراءات رقابة وحماية السياسات واللوائح والقوانين	2.51	0.55	ضعيفة (٦٠%)

جدول رقم (١٦) متوسط قياسات الإجراءات المطبقة لرقابة وحماية مكونات نظام إدارة المحتوي الرقمي بمركز توثيق التراث الحضاري والطبيعي

م	المحاور	المتوسط الحسابي	الإنحراف المعياري	مستوي الرقابة
أ	اجراءات رقابة وحماية البرامج والتطبيقات	3.10	1.33	كافية (٩٤%)
ب	اجراءات رقابة وحماية أجهزة وملحقات الحاسب	3.19	1.39	كافية (١٠٢%)
ج	اجراءات رقابة وحماية البيانات ومصادر المعلومات الرقمية	3.08	1.35	كافية (١٠٠%)

د	اجراءات رقابة وحماية شبكات المعلومات	2.44	0.71	ضعيفة (٥٢%)
هـ	اجراءات رقابة وحماية التجهيزات المادية لمحيط عمل النظام	2.77	1.54	كافية ٩٥%)
و	اجراءات رقابة وحماية العاملين	2.45	1.35	غير كافية
ز	اجراءات رقابة وحماية السياسات واللوائح والقوانين	2.07	1.05	ضعيفة (٥٥%)

جدول رقم (١٧) متوسط الإختراقات والتهديدات المحتملة لأصول نظام إدارة المحتوي الرقمي بمكتبة بيليو اسلام

م	المحاور	المتوسط الحسابي	الإنحراف المعياري	مستوي الرقابة
أ	اجراءات رقابة وحماية البرامج والتطبيقات	3.33	1.46	كافية (٩٨%)
ب	اجراءات رقابة وحماية أجهزة وملحقات الحاسب	3.21	1.37	كافية (١٠٦%)
ج	اجراءات رقابة وحماية البيانات ومصادر المعلومات الرقمية	3.10	1.35	كافية (١٠١%)
د	اجراءات رقابة وحماية شبكات المعلومات	2.67	0.97	ضعيفة (٦٠%)
هـ	اجراءات رقابة وحماية التجهيزات المادية لمحيط عمل النظام	2.78	1.51	كافية (٩٥%)
و	اجراءات رقابة وحماية العاملين	2.36	1.32	غير كافية
ز	اجراءات رقابة وحماية السياسات واللوائح والقوانين	2.04	1.15	ضعيفة (٥١%)

جدول رقم (١٨) متوسط قياسات الإجراءات المطبقة لرقابة وحماية مكونات نظام إدارة المحتوي الرقمي بمكتبة المدينة الرقمية

م	المحاور	المتوسط الحسابي	الإنحراف المعياري	مستوي الرقابة
أ	اجراءات رقابة وحماية البرامج والتطبيقات	3.19	1.27	كافية (٩٣%)

ب	اجراءات رقابة وحماية أجهزة وملحقات الحاسب	3.32	1.38	كافية (١٠٢%)
ج	اجراءات رقابة وحماية البيانات ومصادر المعلومات الرقمية	3.02	1.42	كافية (١٠٠%)
د	اجراءات رقابة وحماية شبكات المعلومات	2.66	1.05	**ضعيفة (٦٢%)**
هـ	اجراءات رقابة وحماية التجهيزات المادية لمحيط عمل النظام	2.66	1.58	كافية (٩٣%)
و	اجراءات رقابة وحماية العاملين	2.88	1.08	**غير كافية**
ز	اجراءات رقابة وحماية السياسات واللوائح والقوانين	2.41	1.40	**ضعيفة (٦٠%)**

يتضح من الجدول رقم (١٥، ١٦، ١٧، ١٨)، أن شبكات المعلومات، (والتي تتعرض لمخاطر متكررة) والسياسات والوائح والقوانين (والتي تتعرض لمخاطر شبه متكررة)، بمكتبة الأسكندرية، ومركز توثيق التراث الحضاري والطبيعي، وببليواسلام، ومكتبة المدينة الرقمية، تتمتع بمستوي حماية ضعيفة. وان العاملين (والتي تتعرض لمخاطر غير متكررة)، تتمتع بمستوي حماية غير كافية. أما باقي مكونات نظم إدارة المحتوي الرقمي فتتمتع بمستوي حماية كافية

وأخيراً يتضح عدم كفاية إجراءات الرقابة المطبقة لمواجهة المخاطر التي تتعرض لها ثلاث عناصر من مكونات نظام إدارة المحتوي الرقميبمشاريع الرقمنة بمؤسسات المعلومات العربية، وهي شبكات المعلومات، السياسات واللوائح والقوانين، والعاملين، وذلك بصرف النظر عن ماهية مشروع الرقمنة، حيث تواجه معظم المشروعات نفس المخاطر التي تهدد مكونات نظام إدارة المحتوي الرقمي، نتيجة التركيز علي الجوانب الفنية فقط، دون الإهتمام بالجوانب غير الفنية لنظم إدارة المحتوي الرقمي.

الخلاصة والتوصيات

حيث أن نظم إدارة المحتوي الرقمي أصبحت متاحة لكل أنواع وأحجام المؤسسات المعلوماتية المختلفة، فقد أصبح تطبيق إجراءات الرقابة الملائمة لحماية مكونات هذه النظم في المؤسسات المعلوماتية المختلفة، أمر ضروري من الصعب تجاهله من قبل مشاريع الرقمنة بمؤسسات المعلومات العربية. حيث يحتاج اختيار وتطبيق النظام المناسب، إلي مجهود مستمر غير منتهي. فبمجرد تصميم نظام رقابة محكم، تظهر مخاطر وتهديدات جديدة.

فيجب أن ترتبط إجراءات الرقابة والحماية المطبقة، لحماية مكونات نظام إدارة المحتوي الرقمي، بشكل إيجابي مع الإختراقات والمخاطر المحتملة. حيث أن العلاقة غير الإيجابية بين إجراءات الرقابة المطبقة والمخاطر المحتملة قد يؤدي إلي توفير حماية غير فعالة للنظام.

ويجب علي القائمين علي مشاريع الرقمنة بالعالم العربي تعديل نظرتهم التقليدية لآليات إدارة المخاطر، فإجراءات الرقابة المادية وإعداد النسخ الإحتياطية، لم تعد إجراءات كافية لتوفير الرقابة والحماية.

ونجد إن تطبيق إجراءات للرقابة والحماية، تتناسب مع محيط عمل نظام إدارة محتوي رقمي بعينه، تعتبر مطلب أساسي لتوفير الرقابة الفعالة.

ويمكن تجنب الأخطاء البشرية بسهولة أو حتي تقليصها بشكل جوهري من خلال التدريب والدعم المهني الملائم. حيث نجد أن هناك خمسة أنواع اساسية لخدمات أمن نظم إدارة المحتوي الرقمي وهي كما يلي:

خدمات و وسائل حماية التعريف Identification and Authentication هذه الخدمات تهدف الى التثبت من الهوية وتحديدا عندما يقوم شخص ما بالتعريف عن نفسه فان هذه الخدمات تهدف الى التثبت من انه هو الشخص نفسه ولهذا فان التعريف يعد الوسائل التي تحمي من انشطة التخفي والتنكر ومن هنا فان هناك نوعين من خدمات

التعريف الاول تعريف الشخصية واشهر وسائلها كلمات السر وثانيها التعريف بأصل المعلومات كالتثبت من أصل الرسالة. (ISO/IEC FCD 27033:2009)

■خدمات و وسائل السيطرة على الدخول Access Control : وهذه الخدمات تستخدم للحماية ضد الدخول غير المشروع الى مصادر الأنظمة والاتصالات والمعلومات ويشمل مفهوم الدخول غير المصرح به لأغراض خدمات الأمن الاستخدام غير المصرح به والافشاء غير المصرح به ، والتعديل غير المصرح به ، والاتلاف غير المصرح به ، واصدار المعلومات والاوامر غير المصرح بها ولهذا فان خدمات التحكم بالدخول تعد الوسائل الاولية لتحقيق التخويل والتثبت منه . (ISO/IEC FCD 27033:2009)

■خدمات و وسائل السرية Data and message Confidentiality: هذه الخدمات تحمي المعلومات من الافشاء للجهات غير المصرح لها بالحصول عليها، والسرية تعني بشكل عام اخفاء المعلومات من خلال تشفيرها على سبيل المثال او من خلال وسائل أخرى كمنع التعرف على حجمها او مقدارها او الجهة المرسلة اليها.

■خدمات و وسائل حماية التكاملية وسلامة المحتوى Data and message Integrity: هذه الخدمات تهدف الى حماية مخاطر تغيير البيانات خلال عمليات ادخالها او معالجتها او نقلها وعملية التغيير تعني بمفهوم الأمن هنا الالغاء او التحوير او إعادة تسجيل جزء منها او غير ذلك وتهدف هذه الوسائل أيضا الى الحماية من انشطة تدمير المعطيات بشكل كامل او إلغائها دون تخويل .

■خدمات و وسائل منع الانكار Non-repudiation: وهذه الخدمات تهدف الى منع الجهة التي قامت بالتصرف من انكار حصول نقل البيانات او النشاط من قبلها.

ونجد أن هناك العديد من قوائم التدقيق والمراجعة حول مسائل أمن نظم إدارة المحتوي الرقمي واستراتيجيات أمن المعلومات والاتصالات، تقوم بالاساس على توفير نوع من دليل المراجعة الذي يساعد المؤسسات او الافراد في بناء إستراتيجية الأمن والحماية وتحديد اطار عام لواجبات الموظفين والمستشارين والمعنيين بشؤون ادارة

نظم إدار المحتوي الرقمي وتطبيقاتها وبنفس الوقت تقدم هذه القوائم او ادلة المراجعة للمؤسساتّ والافراد اطار عاما لفهم عناصر ومتطلبات بناء نظم الأمن الخاصة بالكمبيوتر والشبكات ومصادر المعلومات الرقمية. ومن بين المسائل التي تعالجها عادة هذه القوائم ما يلي :-

■مسائل واجبات جهات الادارة للتحقق من وجود سياسة أمن للمعلومات موثقة ومكتوبة والتحقق من وجود عمليات تحليل المخاطر وخطة الأمن وبناء الأمن التقني وسياسة ادارة الاتصالات الخارجية ، ومدى معرفة واطلاع الموظفين على السياسة الأمنية ومعرفتهم بواجباتهم، ومدى توفر تدريب على مسائل الأمن وما اذا كان يخضع الموظفون الجدد لتدريب وتعريف حول محتوى الخطة .

■مسائل تنظيم شؤون ادارة الأمن، والتي تتعلق بوجود جهة مختصة بذلك في المؤسسة وما اذا كان هنالك دليل مكتوب، وخطط ومسؤولية التعامل مع إجراءات التنفيذ والتعريف والتعامل مع الحوادث ومع خطط الطوارئ وغيرها. (Kuegah, Folly ,2006).

■مسائل الموظفين أنفسهم من حيث مدى فحص التأهيل والكفاءة ومدى التزام الموظفين بتحقيق معايير الأمن على المستوى الشخصي او فيما يتعلق بواجباتهم، وأغراضها المتصلة بالامن لدى تعيين الموظفين وخلال عملهم ولدى انتهاء خدمتهم لأي سبب، وتتصل أيضا بمدى توفر نصوص عقدية خاصة في عقود الموظفين ومدى توفر وصف دقيق بوجباتهم الوظيفية المتصلة باستخدام المعلومات.

■مسائل جهات تزويد الخدمة او المشورة كالمستشارين والمدققين وغيرهم من حيث تغطية عقود التعامل معهم لمسائل الأمن المختلفة.

■مسائل تصنيف المعلومات من حيث توفرها ومعاييرها .

■مسائل البرمجيات من حيث سياسات شرائها واستخدامها وتنزيلها ومسائل الرخص المتصلة بها وآليات التعامل مع البرمجيات المطورة داخليا وحقوق الوصول اليها واستخدامها، ومسائل حماية البرمجيات التقنية والقانونية .

■مسائل الاجهزة والمعدات من حيث توفر تصور للاحتياجات وتوفير المتطلبات ومعايير توظيف الاجهزة في العمل، واسخداماتها والغاء استخدامها ومسائل الصيانة .

■مسائل التوثيق، وهي الذي تتعلق مدى توفر استراتيجية توثيق لكافة عناصر النظام ولكافة مرتكزات وعمليات خطط الأمن وسياساتها.

■المسائل المتصلة بوسائط التخزين خارج النظام من حيث تحديد وسائط التخزين المستخدمة وتبويبها وحفظها والوصول اليها وتبادلها واتلافها .

■مسائل التعريف والتوثق من شخصية المستخدم وحدود صلاحيات والتفويض، وتتعلق بالتحقق من توفر سياسة التحكم بهذه العناصر والوسائل المستخدمة في تحديد الهوية والتوثق من المستخدم، واستراتيجيات حماية وسائل التعريف تقنيا واداريا، ومدى صلاحية المستخدمين من الخارج او من داخل المؤسسة بشأن الوصول للمعلومات او قطاعات منها، ومسائل التحقق من تصرفات المستخدم، مسائل أمن النظام من حيث توفر وسائل التثبت من حيث وقت الاستخدام و المستخدمين . (Misra ,Subhas C.,2008)

■مسائل الاتصالات من حيث السيطرة على وسائل وتطبيقات الاتصالات الداخلية والخارجية وتوثيق حركات الاتصال وحماية عمليات الاتصال والمعايير التقنية المستخدمة في ذلك واستراتيجيات سرية ورقابة وتتبع واستخدام البريد الإلكتروني.

■مسائل ادارة الملفات وسجلات الأداء واستخدام النظام من حيث توفر وسائل توثيقها وارشفتها والتثبت من جهات الانشاء والتعديل والتعامل مع الملفات وقواعد البيانات والبرامج التطبيقية .

■مسائل النسخ الاحتياطية من البيانات من حيث وقت عمل النسخ الاحتياطية وتخزينها واستخداماتها وتبويبها وتوثيقها وتشفيرها اذا كانت مما يتطلب ذلك .

■مسائل الحماية المادية من حيث التوثق من توفير وسائل وإجراءات الحماية للاجهزة الكمبيوتر والشبكات والبنى التحتية من وسائل الطاقة والتوصيلات ومدى توفر وسائل الوقاية من الحوادث الطبيعة او المتعمدة اضافة الى وسائل حماية مكان وجود

الاجهزة والوسائط وادلة الأمن المكتوبة، والوسائل المادية للوصول الى الاجهزة واستخدامها من المخولين بذلك. ".(Rudasill, Lynne ,2004)

■مسائل التعامل مع الحوادث والاعتداءات، من حيث توفر فريق لذلك وأغراضها التي يقوم بها الفريق لهذه الغاية اضافة الى وجود ارتباط مع جهات التحقيق الرسمية وجهات تطبيق القانون وجهات الخبرة المتخصصة بالمسائل المعقدة او التي لا تتوفر كفاءات للتعامل معها داخل المؤسسة.

■مسائل خطط الطوارئ وخطط التعافي لتخفيف الاضرار والعودة للوضع الطبيعي .

■مسائل الاعلام المتعلقة بالمعلومات المتعين وصولها للكافة او لقطاعات محددة والتحقق من وضوح استراتيجية التعامل الاعلامي مع الحوادث والاعتداءات المتحققة.

ومع ان قوائم المراجعة هذه تتباين من مؤسسة الى أخرى، ومن شخص الى اخر، تبعا للواقع والاحتياجات وطبيعة النظام والمعلومات والتطبيقات العملية الا ان الكثير منها يصلح كإطار عام ومرجعية لدى وضع هذه القوائم والأدلة.

وأخيراً إن توفير بيئة عمل آمنة لنظام إدارة المحتوي الرقمي بمشاريع الرقمنة بمؤسسات المعلومات العربية يتطلب ضرورة تعاون جميع العاملين بالمؤسسة في دعم توفير الرقابة اللازمة لمكونات النظام، وذلك لضمان فعالية إجراءات الرقابة المطبقة.

المصادر والإستشهادات المرجعية:

النقيب، متولي (٢٠٠٦). "آلية عمل نظم إدارة المحتوي الرقمي : دراسة تقييمية" . *الاتجاهات الحديثة في المكتبات والمعلومات* . مج ١٣، ع ٢٦. ص ص ٧١-١٤٧

Chang, S.E. and Bruce Ho, C. (2006), "Organizational factors to the effectiveness of implementing information security management", *Industrial Management & Data Systems*, Vol. 106 No.3, pp. 345-61.

CSI/FBI (2003), *CSI/FBI 2003 Computer Crime and Security Survey*, Computer Security Institute, San Francisco, CA, available at: www.gocsi.com/

Ernst & Young (1996), "The Ernst & Young international information security survey 1995", *Information Management & Computer Security*, Vol. 4 No. 4, pp. 26-33.

Hinde, S. (2003), "The law, cyber crime, risk assessment and cyber protection", *Computers and Security*, Vol. 22 No. 2, pp. 90-5.

ISO/IEC FCD 27033:2009. Information technology — Security techniques — Network security. http://www.iso.org/

Joint, Nicholas (2006). "Risk assessment and copyright in digital libraries", *Library Review*, Vol. 55 No. 9, pp. 545 – 548

Joint, Nicholas (2008). "Addled by authentication: recent changes to password systems in British academic libraries: ANTAEUS", *Library Review*, Vol. 57 No. 7, pp. 491 - 498

Jones, Cynthia M. (2009). Utilizing the technology acceptance model to assess employee adoption of information systems security measures. D.B.A., Nova Southeastern University, 2009 , 182 pages; AAT 3372768

Kuegah, Folly (2006). Security measures and effective corporate information systems management: An examination of issues surrounding computer network security, Ph.D., Capella University, 2006 , 130 pages; AAT 3229905

Lihong Zhou, Ana Vasconcelos, Miguel Nunes (2008), "Supporting decision making in risk management through an evidence-based information systems project risk checklist". *Information Management & Computer Security*, Vol. 16 No. 2, pp. 166 - 186

Misra ,Subhas C.(2008). "Modelling strategic actor relationships for risk management in organizations undergoing business process reengineering due to information systems adoption", *Business Process Management Journal*, Vol. 14 No. 1, pp. 65 – 84

Pieters W., L. and Consoli (2009). "Vulnerabilities and responsibilities: dealing with monsters in computer security", *Journal of Information, Communication and Ethics in Society*, Vol. 7 No. 4, pp. 243 – 257

Posthumus, S. and von Solms, R. (2004), "A framework for the governance of information security", *Computer & Security*, Vol. 23, pp. 638-46.

Rainer, R.K. Jr, Snyderr, C.A. and Carr, H.H. (1991), "Risk analysis for information technology", *Journal of Management Information Systems*, Summer, pp. 192-7.

Rudasill, Lynne and Moyer, Jessica (2004)."Cyber-security, cyber-attack, and the development of governmental response: the librarian's view", *New Library World*, Vol. 105 No. 7/8, pp. 248 – 255

Schepman, Tessie (2008). "Anonymity of library users in The Netherlands and Croatia", *New Library World*, Vol. 109 No. 9/10, pp. 407 - 418

Tejay, Gurvirender Pal Singh. (2008). Shaping strategic information systems security initiatives in organizations, Ph.D., Virginia Commonwealth University, 2008 , 360 pages; AAT 3346492

Tsohou, Aggeliki, and et al. (2006). "Formulating information systems risk management strategies through cultural theory", *Information Management & Computer Security*, Vol. 14 No. 3, pp. 198 - 217

Von Solms, B. and von Solms, R. (2004), "The 10 deadly sins of information security management", *Computers & Security*, Vol. 23 No. 5, pp. 371-6.

Wan, XM (2008). "Construction of Information System Security Precaution in Digital Library". the 3rd International Conference on Information Systems for Crisis Response and Management/4th International Symposium on Geo-Information for Disaster Management, AUG 04-06, 2008 Harbin Engn Univ Harbin PEOPLES R CHINA, pp. 263-268

Workman, Michael (2009). "How perceptions of justice affect security attitudes: suggestions for practitioners and researchers", *Information Management & Computer Security*, Vol. 17 No. 4, pp. 341 – 353