جامعة دمشق

كلية الهندسة الميكانيكية و الكهربائية

قسم هندسة الحواسيب و الأتمتة

"مقاربة جديدة لتصميم و تنفيذ نظام أمن للشبكات و المعلومات اعتماداً على منهجية الطبقات"

أطروحة أعدت لنيل درجة الدكتوراه في هندسة الحواسيب الالكترونية و الأتمتة

الأستاذ المشرف: الأستاذ الدكتور غسان فلوح

المشرف المساعد: الأستاذ الدكتور نور بك باشا بن ادريس

إعداد: المهندس وسيم أحمد

21/12/2011

شكر و تقدير

أتقدم بالشكر الجزيل و التقدير للأستاذ الدكتور غسان فلوح للمساهمة الكبيرة التي قدمها لهذا البحث و نصائحه العلمية و خبرته الواسعة في البحث العلمي و علوم الحاسوب.

كما أشكر الأستاذ الدكتور نور بك باشا بن ادريس المشرف المساعد، و السادة أعضاء الهيئة التدريسية في قسم هندسة الحواسيب و الأتمتة بكلية الهندسة الميكانيكية و الكهربائية بجامعة دمشق.

مقاربة جديدة لتصميم و تنفيذ نظام أمن للشبكات و المعلومات اعتماداً على منهجية الطبقات

مقدمة

يعتبر أمن المعلومات و الشبكات من أهم المواضيع التي تولي لها جميع المؤسسات و الهيئات العلمية في جميع أنحاء العالم اهتماماً خاصاً و موارد مالية كبيرة و ذلك للحفاظ على سوية عالية من السرية و الحماية للمعلومات و التي تعتبر لدى بعض المؤسسات – و خاصة الحكومات و الشركات الكبرى والمصارف و المؤسسات المالية – الأصول الأغلى Assets و الأكثر خطورة، و التي يسعى الجميع للحفاظ عليها من التسرب أو الضياع أو التغيير.

و مع تعاظم دور الانترنت والاستخدام الكبير و المتزايد للتجهيزات الالكترونية كأجهزة الخليوي و الحواسب الشخصية و الخدمات الالكترونية، و خاصة المالية منها. و الذي أدى إلى التزايد المخيف للبرامج الضارة و الاختراقات للمواقع و الحسابات المصرفية. ازدادت الحاجة لأبحاث و دراسات في مجال أمن الشبكات و المعلومات.

وعليه فقد دأبت الجهات العلمية المختصة على وضع معايير دولية لأمن المعلومات بحيث تسهل على المعنيين بالموضوع في كافة المؤسسات –على اختلاف طبيعة عملها– تطبيق سياسات أمنية محكمة و مراجعتها للوصول لحالة أمنية مستقرة و في مستوى مقبول لتقديم الخدمات و التسهيلات للزبائن أو للحفاظ على سرية المعلومات و التحكم بالوصول إليها، نذكر منها: ISO 27K,COBIT,NIST، و غيرها.

من هنا أتت فكرة و أهمية هذا البحث لتقديم دراسة و نموذج جديد قابل للتطبيق و التطوير في مجال أمن المعلومات و الشبكات.

يهدف هذا البحث إلى:

1) تصميم نموذج ذي بنية طبقية قادر على مايلي:
   - تضمين كافة النواحي المتعلقة بأمن المعلومات و الشبكات و طرق الحماية و ضمان استمرارية العمل في المؤسسات التي تستخدم أنظمة معلوماتية.
   - توزيع المعايير العالمية في مجال أمن المعلومات و الشبكات على كل طبقة بحسب نوعها و أهميتها.
2) تطوير معادلة جديدة لاحتساب المستوى الأمني للمؤسسة المدروسة تعطي كنتيجة قيمة عددية (كمية) لمستوى المؤسسة أمنياً و تحدد الطبقة الأمنية التي تعكس واقع المؤسسة.
3) تحديد المتطلبات اللازمة لسد الثغرات الأمنية المكتشفة مع توضيح آليات للوصول للمعايير العالمية. وذلك عن طريق توليد تقارير واضحة وسهلة التنفيذ باللغتين العربية و الانكليزية.

4) جعل النموذج المطور قابل للتعديل بحيث يحقق التالي:
- إضافة أو تعديل أي طبقة (مجال) معرف.
- تعديل المتحكمات.
- تعديل آلية الاحتساب.
- تعديل الخرج.

بما يعكس التطور الطبيعي و المتوقع للمعايير العالمية أو لمتطلبات الجهات المعنية بأمن المعلومات، التي تتبع لها المؤسسة المطبقة للنموذج.

5) تطوير نظام مؤتمت يسهل إدخال البيانات و يخزنها في قاعدة بيانات و يقوم بالاحتساب بشكل آلي –وفقاً للمعادلة– و إعطاء النتائج.

يتضمن البحث الفصول التالية:

الفصل الأول: ويتضمن الدراسات المرجعية (أمن المعلومات و الشبكات، نظم التشفير والتعمية، المعايير العالمية المنشورة في أمن المعلومات و الشبكات، القياس الكمي لأمن المعلومات، الهندسة الاجتماعية)، إضافة إلى الأوراق والبحوث المنشورة حول موضوع البحث.
الفصل الثاني: يتضمن النموذج الطبقي المقترح وتوزيع الأدوات والتقنيات المتاحة على كل طبقة. و تحليل النموذج.
الفصل الثالث:تطبيق النموذج المقترح وتطوير معادلة جديدة للقياس الكمي لأمن المعلومات و الشبكات.
الفصل الرابع: ويتضمن تحليل النتائج التي توصل إليها البحث والحلول التي يقدمها النموذج المطور، بالإضافة إلى الاستنتاجات و مقترحات التطوير المستقبلي.
الفصل الخامس:الملاحق.
مسرد المصطلحاتGlossary
المراجع العلمية.
أوراق البحث المنشورة.
موجز عن البحث باللغة الإنكليزية.
الجداول و الأشكال.

الفصل الأول (الدراسات المرجعية)

1.1 أمن المعلومات و الشبكات

1.1.1 مقدمة

مع التزايد الكبير في استخدام الأنظمة المؤتمتة و شبكات الحاسوب و بخاصة الانترنت و الخدمات المرتبطة بها خصوصاً في العشرين سنة الأخيرة؛ تغيرت متطلبات أمن المعلومات و الشبكات من الاكتفاء بناحية الحماية الفيزيائية للحواسيب و الأجهزة الشبكية و بعض الإجراءات الإدارية للتحكم بالعاملين، إلى ضرورة حماية البيانات المتبادلة عبر الشبكات و حماية الملفات و البيانات الشخصية من التسرب و التغيير [Stallings W. C., 2005] .

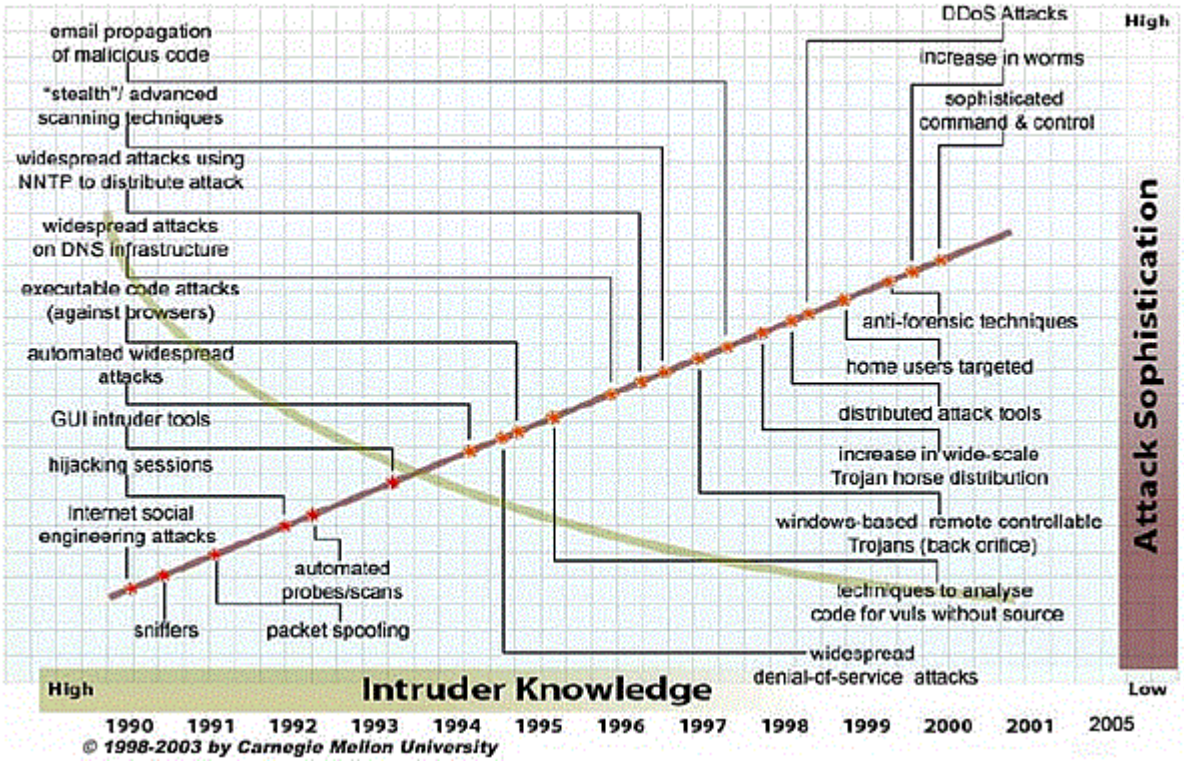
و يمكن أن نعرف كل من أمن المعلومات و أمن الشبكات كما يلي:

أمن (المعلومات) الحواسيب: مجموعة من الأدوات مهمتها حماية البيانات و منع القرصنة الالكترونية.

أمن الشبكات: الإجراءات و الأدوات المستخدمة لحماية البيانات خلال نقلها عبر الشبكات. و تتضمن الحيلولة دون (deter) و منع (prevent) و كشف (detect) و تصحيح (correct) أي انتهاك لأمن المعلومات (security violation) سواءً المنقولة أو المخزنة.

و سنستخدم مصطلح أمن المعلومات ليشمل أمن المعلومات و الشبكات.

يبين الشكل 1 تزايد المخاطر و محاولات الاختراق وتطورها مع الزمن و مع ازدياد القدرات التقنية لمحاولي الاختراق [CERT, 2006].



الشكل 1 تزايد عدد محاولات الاختراق من عام 1990 إلى 2005

و قد ارتبط التزايد الخطير في أعداد و محولات الاختراق بتزايد استخدام الانترنت و البروتوكولات و الخدمات المقدمة عبرها، إضافة إلى ازدياد المعرفة و أدوات الاختراق مما أدى إلى تطوير أدوات و تجهيزات لتأمين الحماية القصوى.

يمكن اعتبار أمن المعلومات مرتكزاً على الأساسيات التالية [Pfleeger, 2002]:

1. **السرية Confidentiality**: ضمان عدم الكشف عن المعلومات لأشخاص أو عمليات أو أجهزة غير المصرح لها بذلك.
2. **الأصالة Authentication**: يتعلق بأن ما نتعامل معه عبر الشبكات حقيقي و يمكن التحقق منه و الثقة به، و هذا يشمل الرسالة الواردة و مرسلها.
3. **عدم الإنكار Non-repudiation**: يمتلك المستقبل إثباتاً لهوية المرسل، و بذلك لا يمكن لأحدهما إنكار أنه قام بمعالجة المعلومات أو أنه لم يستلمها.
4. **السلامة Integrity**: الحماية من تعديل المعلومات أو الرسائل المرسلة.
5. **الإتاحية Availability**: توفر الخدمات و البيانات و بالسرعة المناسبة للمستخدمين الموثوقين.

و يمكننا اعتبار جميع التجهيزات و البرامج و الحلول و الإجراءات التي تتعلق بأمن المعلومات و الشبكات متمحورة حول المشاكل الخمس السابقة، و قبل الدخول بتفاصيلها نبين في الشكل 2 بعض الحلول و موقعها بالنسبة لطبقات الشبكة.

أ – الطبقة الفيزيائية: حماية الكابلات بإحاطتها بطبقات و مواد (غازية مثلاً) و تعطي تنبيه Alarm عند محاولة النفاذ إليها.

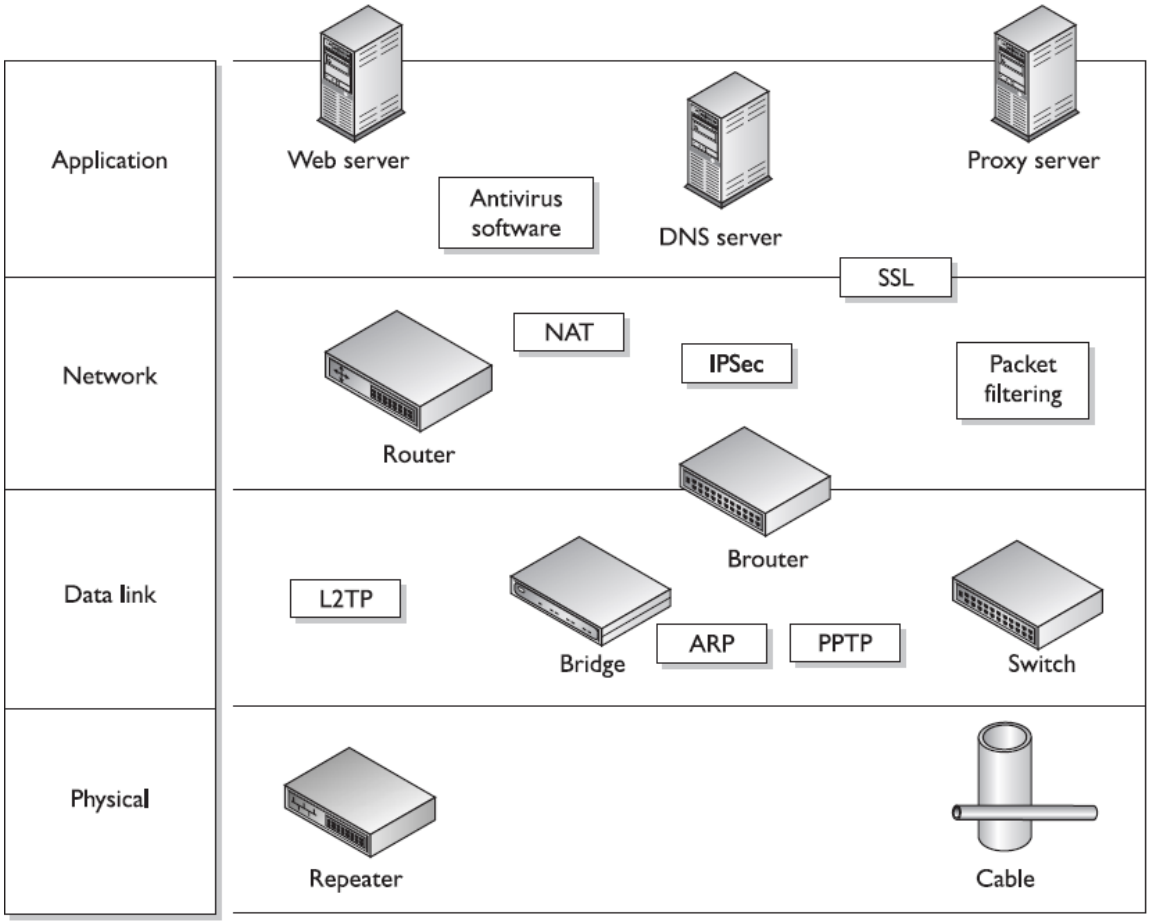
ب –طبقة ربط البيانات: يمكن استخدام التشفير لحماية البيانات المرسلة.

ت –طبقة الشبكة: يمكن استخدام جدار الحماية Firewall و بروتوكولات IPSec لتشفير و حماية الحزم.

ث –طبقة النقل: يمكن استخدام بروتوكول SSL لتشفير الحزم.

ج –طبقة التطبيقات: الأصالة و عدم الإنكار يمكن أن تُطبق هنا باستخدام عدة أدوات. كما يمكن استخدام مضادات الفيروسات و البرامج المضرة.

و لا بد من التأكيد على أن الحلول الموجودة لا تتأقلم جميعها مع نماذج الشبكة المعروفة OSI/ISO و TCP/IP وذلك لأن هذه النماذج وضعت قبل ظهور مشاكل أمن المعلومات و الشبكات، و لأن بعض نواحي أمن المعلومات يتعلق بشكل مباشر بالنواحي الاجتماعية (Social Security) كالمستخدمين و الوثائق وغيرها.



الشكل 2 بعض حلول أمن الشبكات و مكان عملها في طبقات الشبكة

2.1.1 بنية الأمن في النموذج OSI:

لمعرفة متطلبات أمن المعلومات و الشبكات لمؤسسة ما، و لاختيار التجهيزات و الإجراءات المناسبة لهذه المؤسسة، يحتاج مدير أمن المعلومات لطريقة ممنهجة لتعريف متطلباته و الخطوات المتبعة لتحقيق الحالة الأمنية المستقرة.

يعرف المعيار ITU-T Recommendation X.800[1] طريقة منهجية لمدراء المعلوماتية أو أمن المعلومات لتنظيم أمن الشبكات و الخدمات المقدمة عبر شبكات مؤسساتهم. و كونه طرح من خلال منظمة ISO فقد تم تبني هذا النموذج من قبل مصنعي أجهزة الحواسيب و الاتصالات و الشبكات.

[1] The International Telecommunication Union (ITU) Telecommunication Standardization Sector (ITU-T) is a United Nations sponsored agency that develops standards, called Recommendations, relating to telecommunications and to open systems interconnection (OSI).

و قد تم التركيز فيه على المفاهيم التالية [Bishop M. , 2003]:

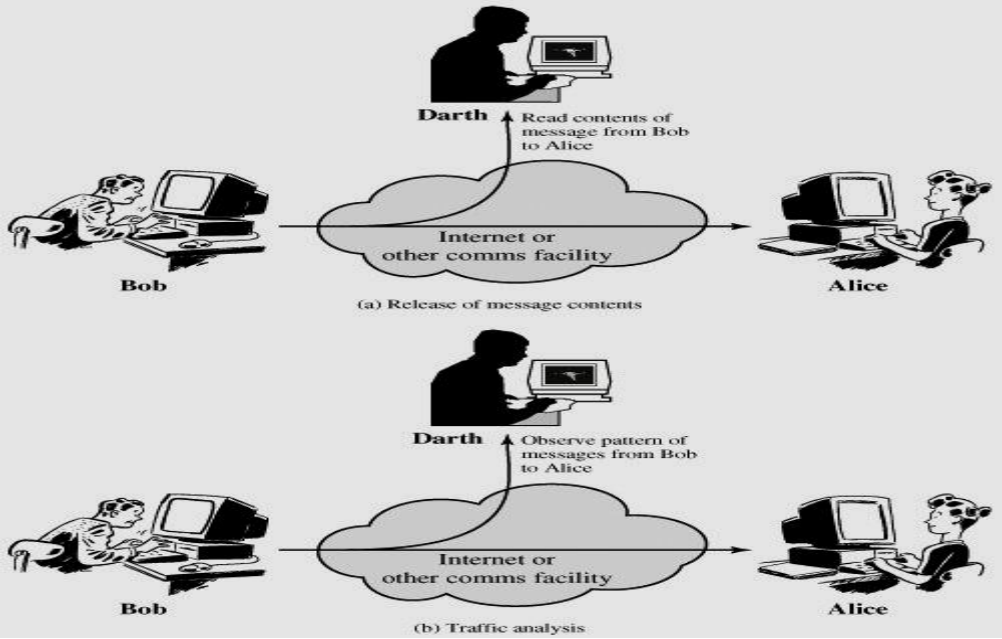
1. **الهجوم الأمني Security Attack**: أي عمل يعرض للخطر أمن المعلومات المملوكة للأفراد أو المؤسسات.
2. **الآلية الأمنية Security Mechanism**: عملية Process (أو الجهاز الذي ينفذ العملية)، و التي صممت لكشف أو منع الهجوم أو استعادة الوضع الصحيح بعد الهجوم الأمني.
3. **الخدمة الأمنية Security Service**: خدمة المعالجة أو خدمة الاتصالات، و التي تُحسن أمن أنظمة معالجة البيانات و أنظمة نقل البيانات التي تقدمها المؤسسات, و هذه الخدمات موجهة لمجابهة الهجمات الأمنية و تستخدم آليات أمنية محددة لتحقيق ذلك.

و سنقوم بشرح المصطلحات السابقة.

-**الهجوم الأمني Security Attack**: و يصنف بنوعين:

أ – الهجوم غير الفعال Passive Attack: و هو من نوع التجسس أو المراقبة. و الهدف منه الحصول على المعلومات المنقولة عبر الشبكات, و يصنف ضمن نوعين:

i. قراءة محتوى الرسائل المتبادلة Release of message content: حيث يقوم المهاجم بقراءة محتوى الرسائل المتبادلة, كما يبين الشكل 3 - a.
ii. تحليل حركة نقل البيانات Traffic Analyzer: في حال لم يتمكن المهاجم من قراءة محتوى الرسائل كونها محمية – مشفرة– فيمكنه الاستفادة من مواعيد الإرسال أو أسماء الأجهزة المستخدمة أو طول الرسائل لاستنتاج معلومات قد تفيده لاحقاً. الشكل 3–b يوضح هذا النوع.



الشكل 3 يوضح نوعي الهجوم غير الفعال

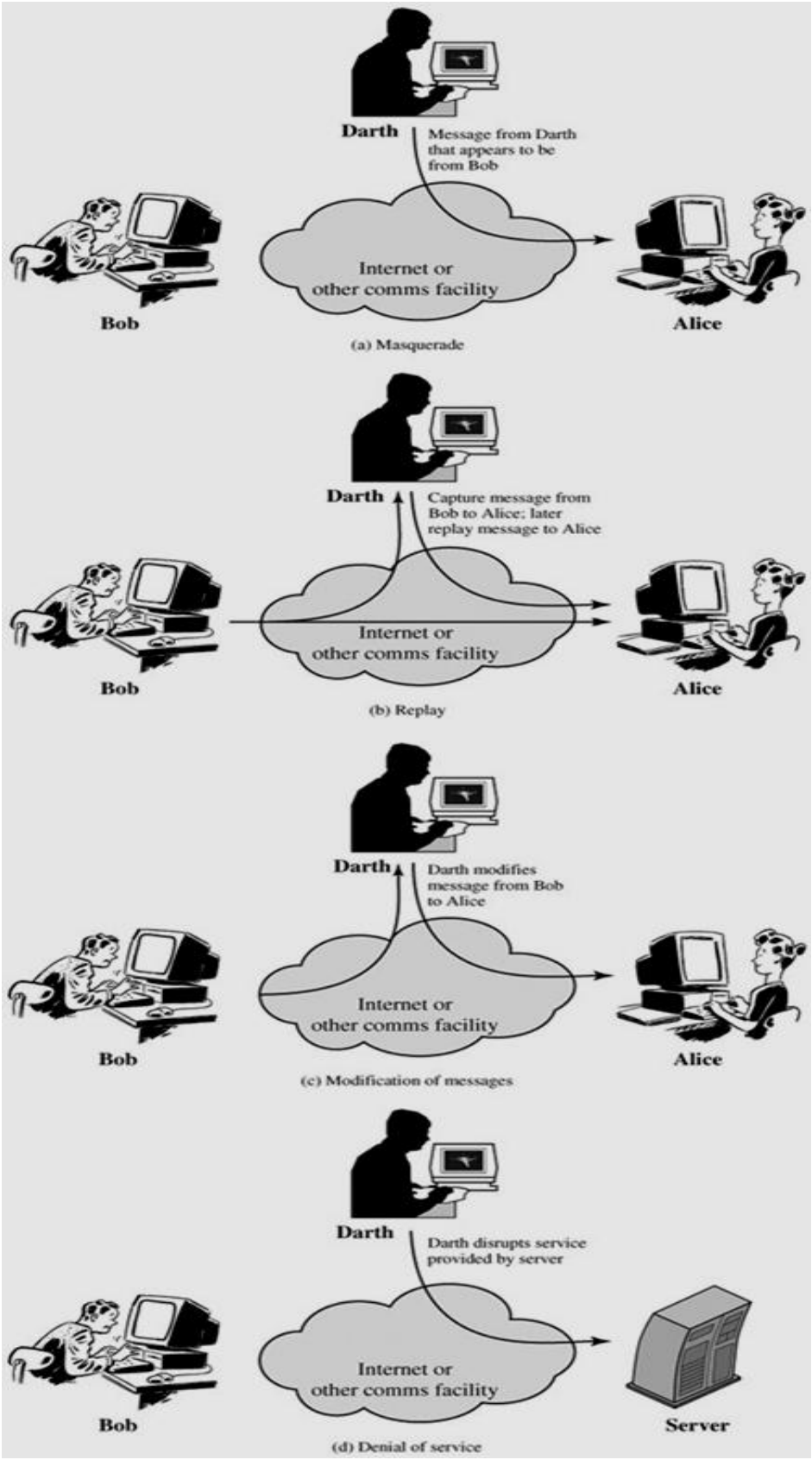
ب –الهجوم الفعال Active Attack: و يتضمن تعديلاً للبيانات المرسلة لخلق بيانات جديدة و يتضمن أربعة أنواع:

i. التنكر Masquerade: يتنكر المهاجم بشخصية طرف آخر موثوق للضحية. و يمكنه ذلك عن طريق معرفة اسم المستخدم الحقيقي و كلمة سره. الشكل 4–a.

ii. إعادة الإرسال replay: بعد أن يقوم المهاجم بقراءة الرسالة الحقيقية المرسلة و إعادة إرسالها دون تعديل و ذلك للتحقق من وجود الاتصال بينه و بين الضحية. الشكل 4–b.

iii. تعديل الرسائل Modification of Messages: يقوم المهاجم بالتقاط الرسائل المرسلة و تعديلها و من ثم إعادة إرسالها للضحية. الشكل 4–c.

iv. منع الخدمة Denial of Service: يقوم المهاجم بمهاجمة المخدم الذي يقدم الخدمات للشبكة كخدمة الرسائل الالكترونية أو غيرها و بالتالي يمنع استخدامه من قبل جميع المستخدمين. الشكل 4–d.



الشكل 4 أنواع الهجوم الفعال

- **الخدمات الأمنية Security Services:** و هي الخدمات التي تقدم في كل طبقة من طبقات الشبكة و التي تضمن المستوى الأمني المناسب للبيانات المتبادلة و للأنظمة و التجهيزات العاملة على الشبكة. و تتضمن ما يلي:

1. الأصالة Authentication: التأكد على أن أطراف الاتصال هي حقيقةً من تدعي أن تكون. و هنا نميز حالتين:
   أ - أصالة المكونات الشبكية المتقابلة في كل طبقة Peer Entity Authentication: تستخدم للتحقق من طرفي الاتصال المنطقي بين طبقتين متقابلتين من طرفي الاتصال كطبقة النقل Transport Layer .
   ب -أصلة مصدر البيانات Data Origin Authentication: تستخدم في خدمات نقل البيانات غير الموثوق Connectionless مثل بروتوكول UDP للتحقق من مصدر البيانات.
2. التحكم بالنفاذ Access Control: منع غير المصرح لهم بالدخول أو استخدام خدمات الشبكة.
3. سرية البيانات Data Confidentiality: حماية البيانات من كشفها لغير المصرح لهم. و تتضمن:
   أ - سرية الاتصال Connection Confidentiality: حماية كافة البيانات أثناء الاتصال.
   ب -سرية الاتصال غير الموثوق Connectionless Confidentiality: حماية بيانات المستخدم المرسلة.
   ت -سرية حقل محدد من بيانات المستخدم Selective Field Confidentiality: سرية أي جزء (حقل) من بيانات المستخدم المرسلة.
   ث -سرية تدفق البيانات Traffic Flow Confidentiality: حماية من المعلومات التي يمكن أن تستنتج من مراقبة البيانات المتبادلة عبر الشبكة.
4. سلامة البيانات Data Integrity: ضمان سلامة البيانات المرسلة من أي تعديل. و تتضمن:
   أ - سلامة الاتصال مع تصحيح البيانات Connection Integrity with Recovery: تؤمن سلامة كافة بيانات المستخدم خلال الاتصال و اكتشاف أي محاولة لتعديل أو تغيير البيانات و تصحيح أي خطأ قد يحصل.

ب –سلامة الاتصال بدون تصحيح البيانات Connection Integrity without Recovery: نفس المهام السابقة و لكن دون تصحيح للبيانات في حال تعديلها.

ت –سلامة حقل محدد من بيانات الاتصال Selective Field Connection Integrity: تؤمن سلامة حقل محدد من بيانات المستخدم أو من رزمة البيانات المرسلة. وتقوم على تحديد إذا ما كان حقل ما قد تم تعديله أو حذفه أو إعادة إرساله.

ث –سلامة الاتصال غير المضمون Connectionless Integrity: تضمن سلامة رزمة اتصال غير مضمون.

ج – سلامة حقل محدد من بيانات الاتصال غير المضمون Selective Field Connectionless Integrity: تؤمن سلامة حقل محدد من بيانات المستخدم من رزمة البيانات المرسلة. وتقوم على تحديد إذا ما كان حقل ما قد تم تعديله أو حذفه أو إعادة إرساله.

5. عدم الإنكار Non-repudiation: تؤمن حماية ضد إنكار أحد أطراف الاتصال من أنه شارك في هذا الاتصال أو جزء منه. و تتضمن:

أ – عدم الإنكار للمصدر: إثبات أن الرسالة قد أرسلت فعلاً من المصدر.

ب –عدم الإنكار للمُستقبل: إثبات أن الرسالة قد وصلت فعلاً إلى وجهتها.

- **الآليات الأمنية Security Mechanisms**: و تقسم إلى نوعين:

1. الآليات المندمجة في طبقات النموذج OSI: وهي تقدم خدمات أمنية من طبقة محددة.

أ – التشفير Encipherment: و هو استخدام خوارزميات رياضية لتحويل البيانات إلى شكل لا يمكن فهمه بسهولة. إن عملية التحويل (التشفير) و الاستعادة (فك التشفير) تتعلق بالخوارزمية المستخدمة و عدد و نوع مفاتيح التشفير.

ب –التوقيع الرقمي Digital Signature: و هو بيانات تُلحق بالبيانات الأصلية أو عملية تشفير للبيانات الأصلية. يسمح التوقيع الرقمي لمستقبل البيانات بتأكيد هوية المرسل و سلامة هذه البيانات. إضافة إلى حمايتها من التزوير (مثلاً من قبل المستقبل).

ت –التحكم بالنفاذ Access Control: وهو مجموعة آليات تؤمن التطبيق الحازم لحقوق الوصول لمصادر المعلومات.

ث –تبادل الأصالة Authentication Exchange: و هو آلية تهدف إلى تأكيد هوية طرفي الاتصال عن طريق تبادل معلومات معينة.

ج – ملء فراغات مسار البيانات Traffic Padding: حشر بيتات bits معينة في الفراغات الموجودة في دفق البيانات (Data Steam) لإحباط محاولات تحليل حركة مرور البيانات.

ح – التحكم بالتوجيه Routing Control: تفعيل اختيار طرق آمنة لمرور البيانات و السماح بتغيير التوجيه عندما يكون هناك احتمال اختراق البيانات أو وجود خطر أمني في طريق أو اتجاه ما.

خ – الحياد Notarization: و هو استخدام جهة خارجية موثوقة لضمان خصائص معينة أثناء تبادل البيانات (مثل الشهادة الرقمية).

2. الآليات غير الموجودة أو القابلة للاندماج في طبقات النموذج OSI: و هي آليات لا تنتمي لطبقة محدد.

أ – التشغيل الموثوق Trusted Functionality: مثل السياسات الأمنية و الإدارية للمؤسسات و التي تضمن العمل بشكل آمن.

ب – اللافتة الأمنية Security Label: و هي بطاقة تعريف توضع على مصادر البيانات و تحوي مواصفات أمنية محددة.

ت – اكتشاف الأحداث Event Detection: اكتشاف الأحداث الأمنية كمحاولات الاختراق و غيرها.

ث – سجل التدقيق الأمني Security Audit Trail: معلومات مجمعة للمراجعة و التدقيق الأمني و تساعد في المراجعة المستقلة لنشاطات و ملفات الأنظمة المعلوماتية و التجهيزات الشبكية.

ج – استعادة البيانات الأمنية Security Recovery: استعادة البيانات لمصلحة آليات و أنظمة أخرى، مثل استعادة أنظمة التشغيل بعد توقفها عن العمل.

و يبين الجدول 1 الخدمات الأمنية و الآليات المستخدمة لتحقيقها [Bishop M. , 2003].

و كما هو ملاحظ من الجدول 1 فإن تقنيات (خدمات) التشفير تحل معظم مشاكل أمن المعلومات و الشبكات و هي موضوع القسم التالي. كما نجد أنه باستخدام التشفير مع التوقيع الرقمي و السياسات

الخاصة بالتحكم بالوصول لمصادر البيانات (Access Control) يمكن حل الجزء المتبقي من المشاكل الأمنية؛ آخذين بعين الاعتبار أن الإتاحية (Availability) لا تعتبر مشكلة أمنية خطيرة[2].

Mechanism								
Service	**Encipherment**	**Digital Signature**	**Access Control**	**Data Integrity**	**Authentication Exchange**	**Traffic Padding**	**Routing Control**	**Notarization**
Peer entity authentication	Y	Y			Y			
Data origin authentication	Y	Y						
Access control			Y					
Confidentiality	Y						Y	
Traffic flow confidentiality	Y					Y	Y	
Data integrity	Y	Y		Y				
Non-repudiation		Y		Y				Y
Availability				Y	Y			

جدول 1 العلاقة بين الخدمات و الآليات الأمنية

[2] لا تعتبر الإتاحية لدى العديد من الباحثين مشكلة أمنية بالمقارنة مع البنود الأخرى.

2.1 علم التعمية (التشفير)

1.2.1 مقدمة

يعتبر التشفير أهم أنواع الحلول لمشاكل أمن المعلومات و الشبكات و قد ازداد الاهتمام به و بتطويره في السنوات الأخيرة. و لكن العديد من الدراسات و الأبحاث المدعمة بالوثائق أثبتت أن العرب أول من درس و صنف علم التشفير (التعمية) و فك التشفير (استخراج المعمى)، علاوة على ذلك كان العرب منذ عصور الجاهلية يستخدمون الرمز و الملاحن و المعاريض و أمثالها، ليخفوا معانيهم و مراميهم فلا يفهم عنهم إلا الفطن ذو النباهة. فلما جاء الإسلام و استبحر العمران و ازدهرت الحضارة العربية و تشابكت مصالح الدول التي امتدت أطرافها و كثرت صلاتها بالدول الأخرى، تهيأت الأسباب المسعفة ليخطو العرب خطوات فساحاً، فأبدعوا في طرائق إخفاء أسرارهم و مقاصدهم، و سلكوا في سبيل ذلك أساليب متنوعة و مبتكرة، فيها الرمز و الألغاز و الملاحن و التعمية و المحاجات و المعاياة و التورية وما إليها. ساعدهم في ذلك تطور علم اللغة و الرياضيات و الترجمة.
و نذكر هنا فيما يخص علم التعمية [طيان، 1987] ثلاث رسائل هي:

1. رسالة في استخراج المعمى ليعقوب بن إسحاق الكندي.
2. و المُؤلّف للملك الأشرف لعلي بن عدلان.
3. و مفتاح الكنوز في إيضاح المرموز لعلي بن الدريهم.

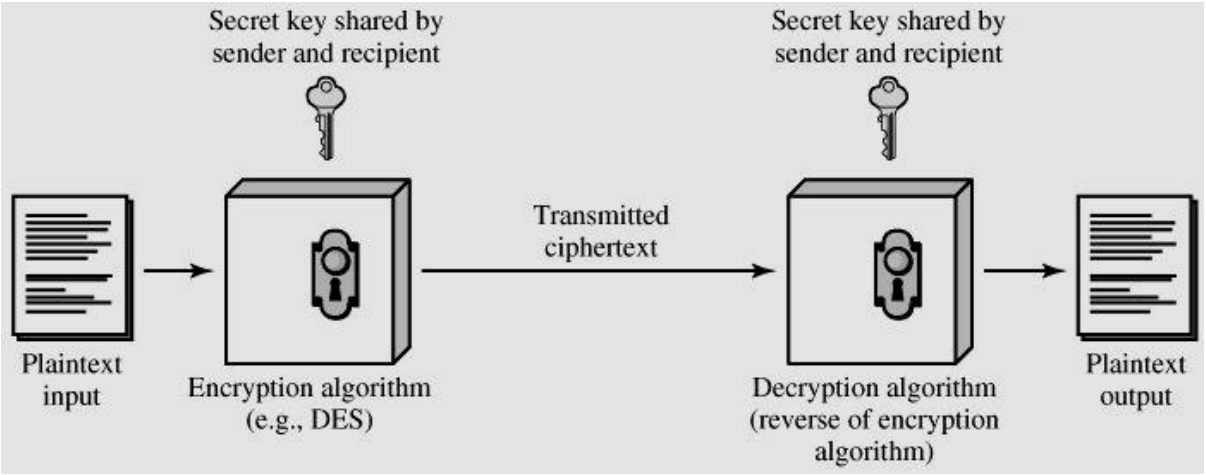
و قد عرّف العرب التعمية بأنه تحويل نص واضح إلى آخر غير مفهوم باستخدام طريقة محددة يستطيع من يعرفها أن يسترجع النص الأصلي. و ما استخدام مصطلح Algorithm أي خوارزمية نسبة للعالم المشهور الخوارزمي و الذي يستخدم في عدد من العلوم و منها التشفير، إلا دليلاً على فضل العرب على العالم في كافة العلوم و خصوصاً العلوم المعاصرة و التي بنيت على إنجازاتهم.
يمكن أن تصنف أهم طرق التشفير إلى نوعين المتناظرة Symmetric و غير المتناظرة Asymmetric أو ما يعرف بتقنيات المفتاح العام Public-key. و سنعرض لكلا النوعين في الفقرات التالية.

2.2.1 نموذج التشفير المتناظرة Symmetric- key Model

تسمى أيضاً بنموذج التشفير التقليدي Conventional Encryption. يعتمد نموذج التشفير المتناظر على المقومات الخمس التالية [Stallings W. C., 2005]:

1. النص الواضح Plaintext: و هو الرسالة الأصلية أو البيانات المراد تشفيرها.
2. خوارزمية تشفير Encryption Algorithm: و تقوم بعمليات استبدال Substitutions و تغيير أحرف Transformation للنص الواضح لتحويله إلى نص مشفر.
3. المفتاح السري Secret Key: و هو مفتاح يستخدم كدخل في خوارزمية التشفير، و يكون المفتاح السري مشتركاً فقط بين المرسل و المستقبل. و تكون قيمة المفتاح مستقلة عن النص المراد تشفيره و عن الخوارزمية المستخدمة. أما خرج الخوارزمية فهو متعلق بقيمة المفتاح المستخدم في كل دورة تشفير. أما عدد عمليات الاستبدال و تغيير الأحرف التي تقوم بها الخوارزمية تتعلق مباشرة بالمفتاح المستخدم.
4. النص المشفر Ciphertext: و هو الرسالة المشفرة الناتجة كخرج نهائي لعملية تشفير الرسالة الأصلية. و تتعلق بالرسالة الأصلية و المفتاح المستخدم، بمعنى مع تغيير المفتاح يتغير النص المشفر لنفس النص الأصلي.
5. خوارزمية فك التشفير Decryption Algorithm: و تعمل بشكل أساسي عكس عمل خوارزمية التشفير؛ فتأخذ كدخل النص المشفر و مفتاح التشفير و تعطي كخرج النص الأصلي.

و يوضح الشكل 5 نموذج التشفير المتناظر:

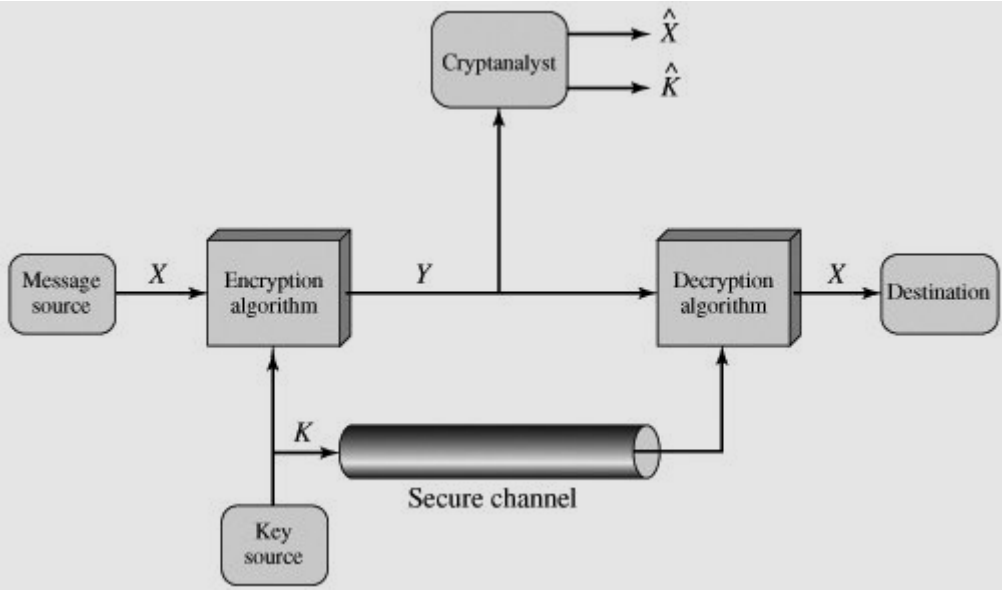


الشكل 5 نموذج التشفير المتناظر Symmetric Encryption

يتطلب الاستخدام الآمن للتعمية المتناظرة أمرين:

1. نحتاج إلى خوارزمية قوية. حيث يلزم على الأقل أن تكون الخوارزمية على النحو الذي لا يكون فيه المعتدي، والذي يعرف هذه الخوارزمية ولديه نص مشفر أو أكثر، قادر على فك تشفير النص المشفر أو استخراج المفتاح .يوضع هذا المطلب بشكل أقسى على النحو :يجب أن يكون المعتدي غير قادر على فك تشفير النص المشفر أو اكتشاف المفاتيح حتى ولو توفر لديه عدد من النصوص الصريحة والنصوص المشفرة الموافقة لها.
2. يجب على كل من المرسل والمستقبل الحصول على نسخة من المفتاح السري بشكل آمن وأن يبقى هذا المفتاح سريا بينهما .فإذا استطاع أحد ما الحصول على المفتاح أو اكتشافه وكان على دراية بالخوارزمية المستخدمة، فستصبح كل الاتصالات التي تستخدم هذا المفتاح مقروءة.

يوضح الشكل 6 العناصر الأساسية لنموذج التشفير المتناظر:



الشكل 6 العناصر الأساسية لنموذج التشفير المتناظر

يصدر المنبع رسالة على شكل النص الصريح $X = [X_1, X_2, \ldots, X_M]$.

العناصر m من الرسالة X هي أحرف الرسالة ممثلة بشكل ثنائي {0,1} binary. ولإنجاز عملية التعمية يتم توليد المفتاح ذي الشكل $K = [K_1, K_2, \ldots, K_J]$، فإذا تم توليد المفتاح لدى المصدر فيجب نقله

بأمان للمستقبل، الطريقة البديلة لذلك هي أن يتم توليد المفتاح من قبل طرف ثالث و من ثم إيصاله للمصدر و المستقبل.

ثم تقوم الخوارزمية E() باستخدام النص X و المفتاح K بتوليد النص المشفر $Y = [Y_1, Y_2, \ldots, Y_N]$.

و يمكن أن نعبر عن ذلك بالتابع $Y = E(K, X)$.

أما في الطرف الآخر (المستقبل) تقوم خوارزمية فك التشفير D() باستخراج الرسالة الأصلية X و ذلك باستخدام مفتاح التشفير K، كما يلي $X = D(K, Y)$.

أما في حال حصول المعتدي (طرف غير مصرح له بالحصول على الرسالة الأصلية) على الرسالة المشفرة Y و في كونه يعرف خوارزمية التشفير E() و خوارزمية فك التشفير D() و لا يعرف المفتاح K، يحاول استخراج نص افتراضي للنص الأصلي و ليكن $\hat{X}$, و هدفه الحصول على الرسالة الحقيقية بتزويد الخوارزمية D() بمفتاح افتراضي $\hat{K}$.

1.2.2.1 خصائص نظام التشفير:

يمكن توصيف أنظمة التشفير من خلال النقاط الثلاث المستقلة التالية:

1. **نمط العملية المستخدمة لتحويل النص الصريح إلى نص مشفر:** تعتمد كل خوارزميات التشفير على المبدأين العامين التاليين :التبديل Substitution، حيث يتم فيه تحويل كل عنصر من النص الصريح (خانة، حرف، مجموعة من الخانات أو الحروف) إلى عنصر مقابل آخر. و على مبدأ تغيير المواضع Transposition، حيث تتم عملية إعادة ترتيب العناصر في النص الصريح. المطلب الأساسي هنا هو عدم إضاعة أي عنصر (أي أن تكون كل العمليات قابلة للعكس). تتضمن معظم أنظمة التشفير عدة مراحل من التبديل وتغيير المواضع.
2. **عدد المفاتيح المستخدمة:** إذا استخدم كل من المرسل والمستقبل نفس المفتاح، عندها يطلق على نظام التشفير بالمتناظر، أو التشفير بالمفتاح الوحيد أو التشفير بالمفتاح السري أو التشفير التقليدي Conventional Encryption. أما إذا استخدم المرسل والمستقبل مفتاحين مختلفين عن بعضهما بعض، عندها يسمى نظام التشفير بغير متناظر Asymmetric أو ذات المفتاحين أو التشفير بالمفتاح العمومي Public key encryption.
3. **الطريقة التي يعالج فيها النص الصريح:** و هنا نميز نوعين

أ – **التشفير الكتلي Block Cipher:** يعالج التشفير الكتلي الدخل على شكل كتلة واحدة من العناصر في كل مرة، بحيث ينتج في كل مرة كتلة خرج توافق كتلة الدخل.

ب – **التشفير التدفقي Stream Cipher**: فيعالج عناصر الدخل بشكل متواصل أو باستمرار، و يعطي لكل عنصر من الدخل عنصر خرج مقابل واحد في كل مرة.

3.2.1 طرق مهاجمة نُظم التشفير:

تهدف عملية الهجوم على أي نظام تشفير كشف مفتاح التشفير المستخدم، هناك طريقتان عامتان لمهاجمة نُظم التشفير:

1. **تحليل التشفير Cryptanalysis**: يعتمد الهجوم على استخدام تحليل التعمية على طبيعة الخوارزمية بالإضافة إلى بعض المعرفة عن المميزات العامة للنص الصريح وربما على بعض النماذج من أزواج (النص الصريح ، النص المشفر). يستغل هذا النوع من الهجوم مميزات الخوارزمية المستخدمة، لمحاولة استنتاج نص صريح محدد أو لاستنتاج المفتاح المستخدم.
2. **هجوم القوة الكاملة Brute-Force**: يحاول المهاجم في هذه الحالة تجريب كل المفاتيح المحتملة على جزء من النص المشفر، ويتابع هذه المحاولات حتى يحصل على نص صريح مفهوم أو واضح. يجب وسطيا تجريب نصف المفاتيح الممكنة للوصول إلى النجاح. و يوضح الجدول 2 الزمن اللازم لإيجاد مفتاح تشفير بحسب طوله.

Key size (bits)	Number of alternative keys		Time required at 1 decryption/μs		Time required at 10^6 decryption/μs
32	2^{32}	= 4.3×10^9	2^{31} μs	= 35.8 minutes	2.15 milliseconds
56	2^{56}	= 7.2×10^{16}	2^{55} μs	= 1142 years	10.01 hours
128	2^{128}	= 3.4×10^{38}	2^{127} μs	= 5.4×10^{24} years	5.4×10^{18} years
168	2^{168}	= 3.7×10^{50}	2^{167} μs	= 5.9×10^{36} years	5.9×10^{30} years
26 characters (permutation)	26!	= 4×10^{26}	2×10^{26} μs	= 6.4×10^{12} years	6.4×10^6 years

جدول 2 الزمن الوسطي لايجاد مفتاح تشفير بالمقارنة مع طول المفتاح

4.2.1 مبادئ التشفير الكتلي Block Cipher Principles

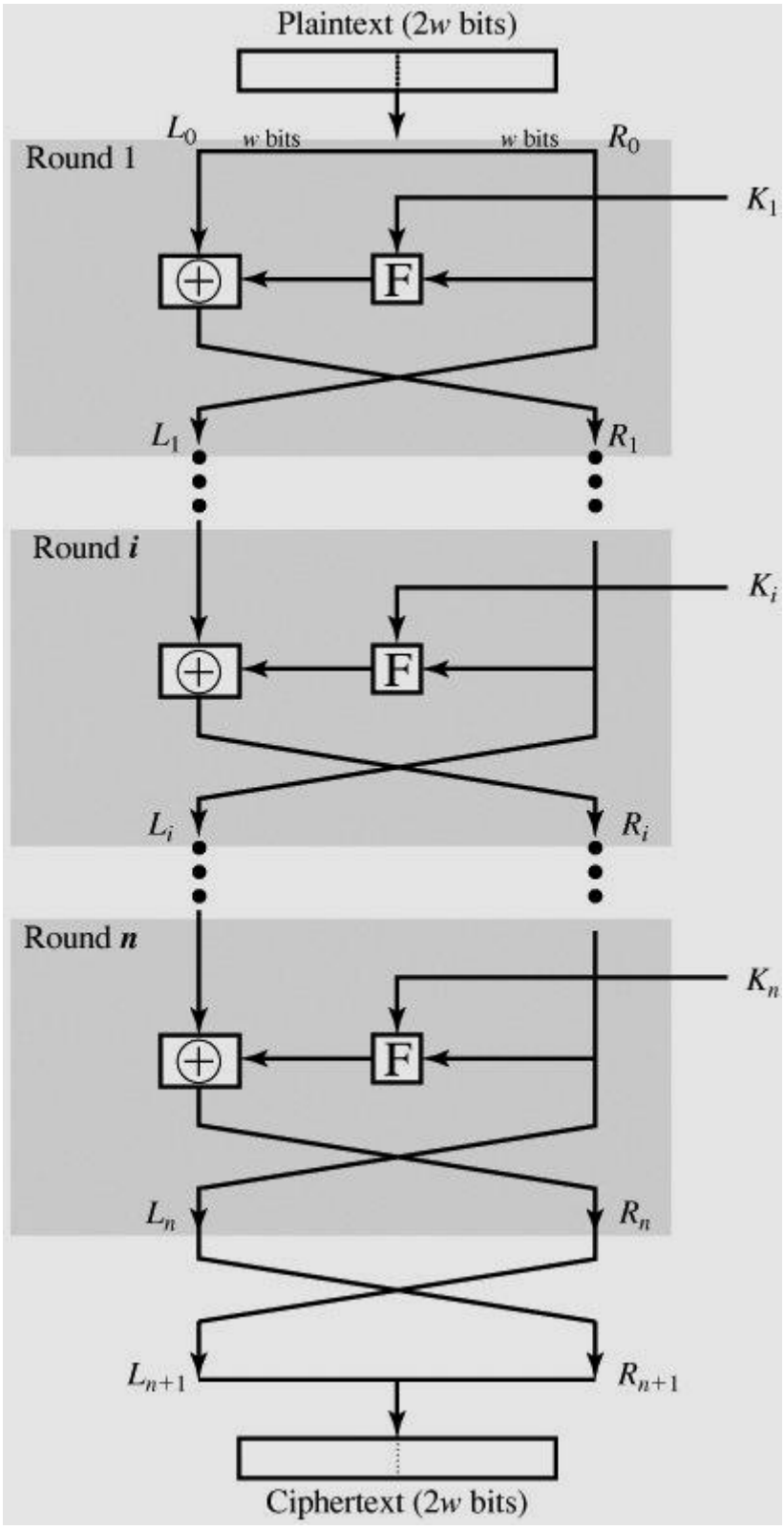
تعمل معظم خوارزميات التشفير المتناظر على بنية أساسية تدعى Feistal Block Cipher [Feistel, 1973]، و الذي سنقوم بشرحه في هذه الفقرة.

تقوم خوارزميات التشفير الكتلي بمعالجة (تشفير) كتلة Block من بيانات النص الصريح كاملة و إنتاج كتلة مشفرة كخرج للخوارزمية. و بشكل عام تحدد كتلة البيانات بحجم 64 أو 128 بيت.

1.4.2.1 بنية تشفير الكتلة بحسب Feistal

يعتمد هذا التشفير على مبدأ استخدام المشفر المنتج Product Cipher، و الذي يتم بتنفيذ دورتين أو أكثر من التشفير البسيط و الذي ينتج في النهاية تشفيراً قوياً صعب الاختراق. و يتم ذلك باستخدام مفتاح تشفير k و كتلة بيانات مكونة من n بيت، تسمح بالقيام ب 2^n عملية تحويل لبيانات الكتلة المدخلة. بالإضافة إلى ذلك تقوم الخوارزمية و بشكل متتالي، بعمليات استبدال Substitution و تبديل مواقع Permutation متتالية لأحرف (أو بيتات) النص الأصلي.

و يوضح الشكل 7 بنية Feistal Cipher، بحيث يتم إدخال كتلة من بيانات النص الأصلي بطول 2w بيت، و مفتاح تشفير k. تُقسم كتلة الدخل إلى نصفين يميني R_0 بطول w و يساري L_0، بطول w. يخضع النصفان اليميني و اليساري لدورات معالجة (تشفير) بعدد n دورة. و في كل دورة تشفير i يكون الدخل النصفين اليميني R_{i-1} و يساري L_{i-1}، الناتجين عن دورة التشفير السابقة (i-1)، بالإضافة إلى مفتاح التشفير الجزئي k_i، و الذي يُشتق عن المفتاح الأساسي k باستخدام خوارزمية محددة.



الشكل 7 بنية تشفير Feistal

تتكون جميع دورات التشفير و عددها n من بنية متطابقة، بحيث يتم في كل منها ما يلي:

- تبديل Substitution للنصف الأيسر من البيانات، و الذي يتم باستخدام تابع F على النصف الأيمن و من ثم تطبيق XOR مع النصف الأيسر.
- يلي ذلك عملية تغيير مواقع Permutation يتم عن طريق تبديل النصف الأيمن بالأيسر.

أما عملية فك التشفير فتتم بطريقة معاكسة للتشفير. و يمكن اختصار بنية Feistal بالعوامل التالية:

1. حجم الكتلة: مع زيادة حجم الكتلة المدخلة تزداد صعوبة اختراق التشفير. و لكن ذلك يؤدي إلى بطء عملية التشفير. لذلك تم اعتماد حجم 64 بيت. و تستخدم بعض الخوارزميات الحديثة مثل AES 128 بيت.
2. عدد دورات التشفير: بزيادة دورات التشفير المستخدمة يتحسن أمن بنية التشفير، و تستخدم بنية Feistal 16 دورة.
3. خوارزمية توليد المفاتيح الجزئية: مع استخدام خوارزميات آمنة لتوليد المفاتيح، تزداد صعوبة الاختراق.
4. تابع التدوير F: أيضاً باستخدام توابع متطورة و صعبة الكشف، تتحسن البنية.

و تعتبر خوارزمية DES، من أشهر الخورزميات المتناظرة التي تعتمد بنية Feistel.

2.4.2.1 خوارزمية Data Encryption Standard (DES)

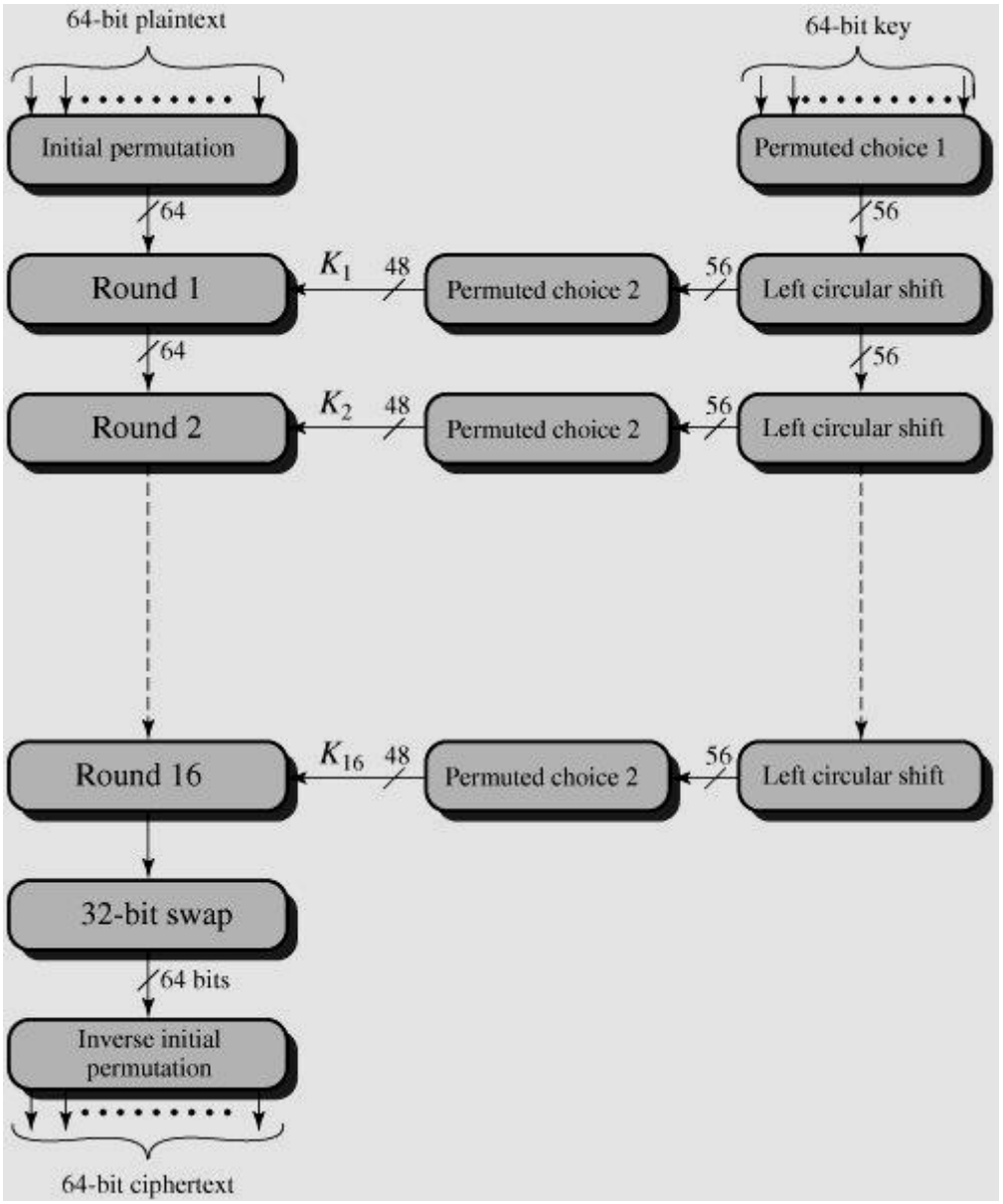
تم تبني خوارزمية DES من قبل معهد NIST في الولايات المتحدة عام 1977، و استمرت التوصية باستخدامه إلى عام 1999 حيث تم تبني خوارزمية Triple-DES و المبنية على DES.

يشرح الشكل 20 بنية التشفير الخاصة بخوارزمية DES، و التي تقبل كدخل كتلة من البيانات بحجم 64 بيت و مفتاح التشفير بطول 56 بيت.

و بالنظر إلى النصف الأيسر من الشكل 8، نرى أن الخوارزمية تتكون من ثلاث مراحل:

1. مرحلة تغيير المواقع الأولية Initial Permutation (IP): بحيث يتم تغيير مواقع البيانات المدخلة، و هي كتلة من البيانات بحجم 64 بيت.
2. 16 دورة تشفير تستخدم نفس التابع، و تتضمن عمليات تغيير مواقع و تبديل للبيانات، و هنا يستخدم مفتاح التشفير k_i.
3. مرحلة تغيير المواقع العكسية Reverse IP: و هو معاكس للمرحلة الأولى IP.

و ينتج في النهاية نص مشفر بحجم 64 بيت.

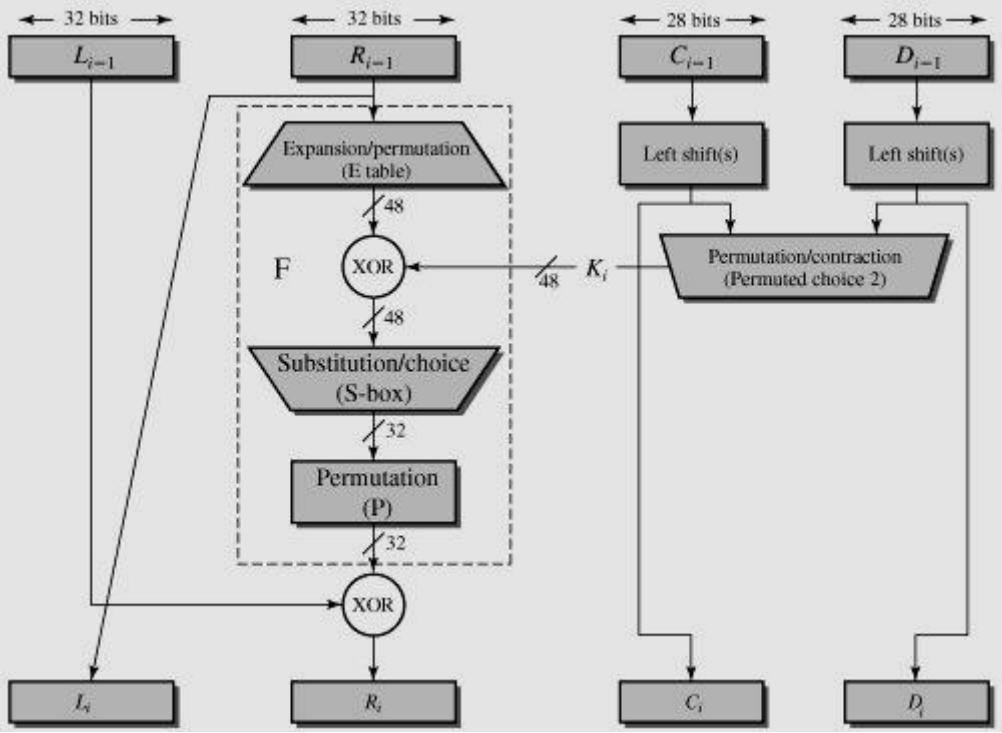


الشكل 8 بنية خوارزمية DES

و يوضح الشكل 8 القسم الأيمن آلية توليد مفتاح التشفير بطول 56 بيت و يشتق منه المفاتيح الجزئية k_i بطول 48 بيت، و التي تولد من كتلة البيانات المدخلة نفسها، بالإضافة إلى تابع تغيير مواقع.

تفاصيل دورة التشفير في DES:

تقوم الخوارزمية ب 16 دورة تشفير متماثلة، يمكن شرحها بالشكل 9 و التي تتضمن ما يلي:



الشكل 9 تفاصيل دورة التشفير في خوارزمية DES

بالتركيز على الجهة اليسرى من الشكل 9 ، نلاحظ أن دخل المرحلة i يُقسم إلى قسم يميني R_{i-1} و يساري L_{i-1}، كل منهما بحجم 32 بيت. و يكون الخرج في كل مرحلة و المبني على بنية Feistel:

$$L_i = R_{i-1}$$
$$R_i = L_{i-1} \times F(R_{i-1}, K_i)$$

أما مفاتيح التشفير الجزئية k_i و التي تكون بطول 48 بيت فتنتج عن كتلة البيانات المدخلة نفسها، بعد أن تقسم إلى قسمين و تخضع لإزاحة و تغيير مواقع Permutation.

أما التابع F(R,K)، فيتم فيه عمليات استبدل و XOR لإنتاج 32 بيت من البيانات المشفرة.

و تتم عملية فك التشفير بنفس الخوارزمية و بشكل معاكس لعملية التشفير.

تحليل قوة خوارزمية DES

- **استخدام مفاتيح بطول 56 بيت:** بوجود مفتاح بطول 56 بيت يكون لدينا 2^{56} مفتاح محتمل، أي ما يعادل حوالي 7.2×10^{16} مفتاح. و بالتالي فإن محاولة الهجوم بطريقة Brute-Force سيكون غير عملي، لأنه باستخدام حاسب بقدرات معالجة تصل إلى عدة أجزاء من الألف من الثانية Microseconds، ستحتاج لآلاف السنوات لكسر التشفير. الجدول 5 يوضح ذلك.

و لكن في عام 1998 تم خرق خوارزمية DES و ذلك بسبب التطور الكبير للمعالجات و استخدام المعالجة بالتوازي Parallel Processing. و بالتالي تم تطوير Triple-DES، و AES.

- **طبيعة خوارزمية DES:** وجدت نقطة ضعف أخرى في خوارزمية DES و هي استخدام ثمانية مراحل تبديل Substitution، أظهرت مع الاستخدام نقاط ضعف متعددة، مما أدى إلى اختراقها.

3.4.2.1 خوارزمية Advanced Encryption Standard (AES)

كما ذكرنا قام معهد National Institute of Standards and Technology (NIST) في الولايات المتحدة، عام 1999 باستبدال خوارزمية DES ب Triple-DES، و الذي استخدم مفتاح تشفير بطول 128 بيت، و بنفس بنية DES مكررة ثلاث مرات. إلا أن الخوارزمية كانت بطيئة، و بما أنها استخدمت نفس بنية DES، فبقيت المشاكل الأمنية نفسها.

نتيجة للأسباب السابقة و الحاجة لخوارزميات تشفير تقبل حجم كتلة أكبر، قام NIST في عام 1997 بطرح مسابقة لاختيار خوارزمية تشفير جديدة باسم AES. و تم في النهاية تبني خوارزمية Rijndael[1]، وقد تم إطلاقه للاستخدام عام 2001.

تعمل الخوارزمية AES بدخل كتلي بحجم 128 بيت، و مفتاح تشفير بعدة أطوال 128 أو 192 أو 256 ، و بعدد دورات تشفير مختلفة 10 أو 12 أو 14 دورة. يلخص الجدول 3 عوامل خوارزمية AES [Simovits، 1996].

Key size (words/bytes/bits)	4/16/128	6/24/192	8/32/256
Plaintext block size (words/bytes/bits)	4/16/128	4/16/128	4/16/128
Number of rounds	10	12	14
Round key size (words/bytes/bits)	4/16/128	4/16/128	4/16/128
Expanded key size (words/bytes)	44/176	52/208	60/240

جدول 3 عوامل خوارزمية AES

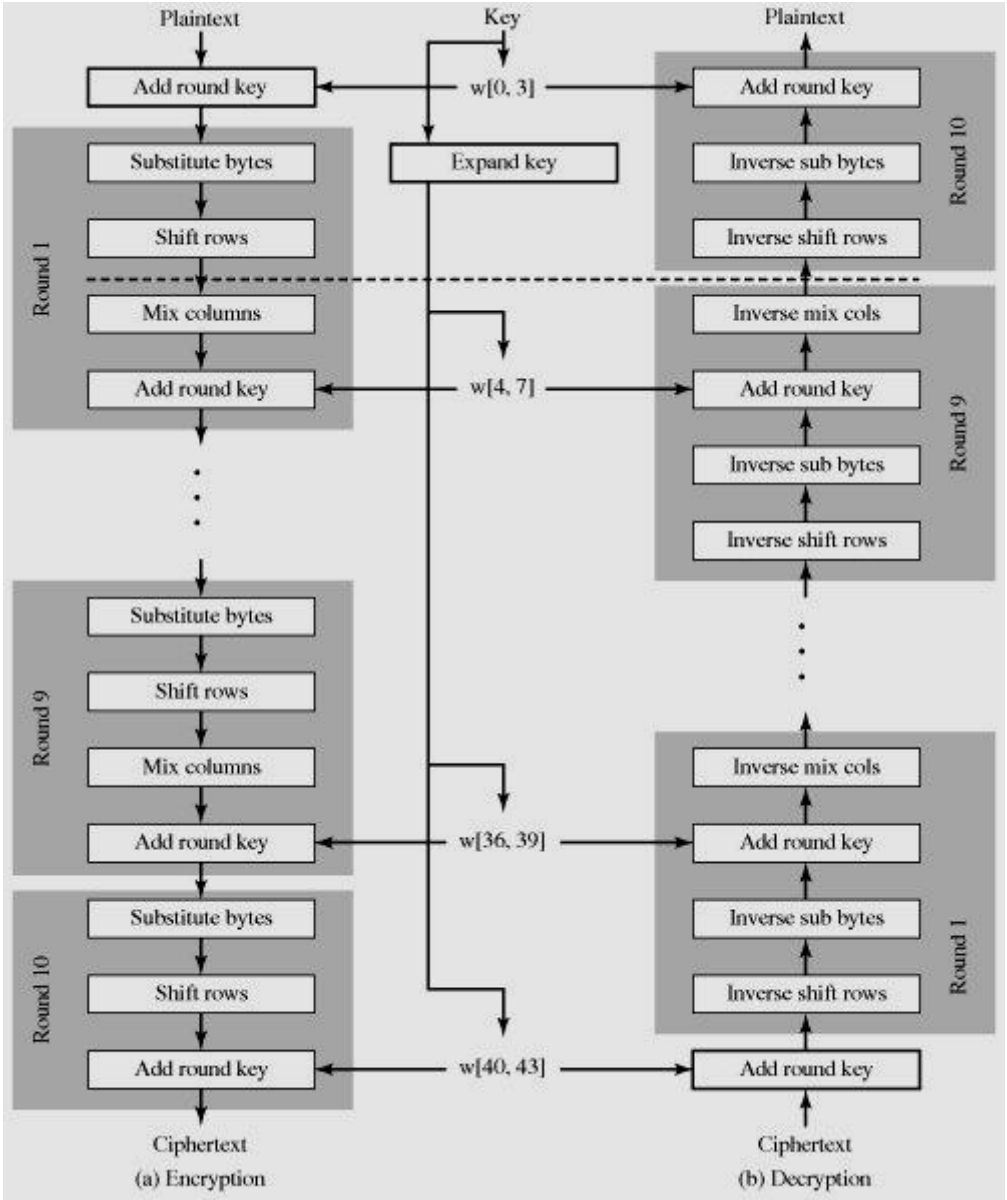
تعمل خوارزمية AES كما يلي:

- يتكون الدخل من كتلة بيانات بحجم 128 بيت، على شكل مصفوفة ثنائية البعد من أربعة أعمدة و أربعة صفوف، و كل عنصر هو كلمة Word من بايت واحد.
- مفتاح الدخل يمدد إلى مصفوفة من الكلمات.

[1] The two researchers who developed and submitted Rijndael for the AES are both cryptographers from Belgium: Dr. Joan Daemen and Dr.Vincent Rijmen.

- يتم إدخال المفتاح و مصفوفة الدخل إلى دورات تشفير (بعدد 10 أو 12 أو 14). و في كل دورة يتم ما يلي:
  1. استبدال كل كلمة Byte Substitution.
  2. إزاحة لصفوف المصفوفة Shift Rows.
  3. خلط الأعمدة Mix Columns.
  4. إضافة مفتاح التشفير الجزئي عن طريق دارات XOR.

و يوضح الشكل 10 آلية التشفير و فك التشفير في AES.



الشكل 10 آلية التشفير و فك التشفير في AES

و تتم عملية فك التشفير بآلية بسيطة معاكسة للتشفير.

مميزات المشفر AES:

1. ممانعة لكل أنواع الهجوم لكسر الخوارزميات المعروفة حتى الآن.
2. سريعة و قابلة للتنفيذ على أي منصة Hardware Platform.
3. بساطة التصميم.

5.2.1 التشفير باستخدام المفتاح العام Public-Key Cryptography

بعد دراسة بعض أهم خوارزميات التشفير المتناظرة، و التي تستخدم مفتاح تشفير مشترك في التشفير و فك التشفير. ننتقل إلى دراسة خوارزميات التشفير باستخدام المفتاح العام، و الذي يستخدم مفتاحين للتشفير و فك التشفير، مفتاح عام معروف للجميع و مفتاح خاص يعرفه صاحبه فقط.

و يعتمد ذلك على أن ما شُفر بالمفتاح العام، يفك تشفيره بالمفتاح الخاص، و العكس صحيح. و تحقق خوارزميات التشفير بالمفتاح العام متطلبات السرية Confidentiality و الأصالة Authenticity.

تعتبر خوارزمية RSA الأشهر من بين خوارزميات المفتاح العام.

تم تطوير التشفير غير المتناظر أو التشفير بالمفتاح العام لمواجهة مشكلتين أساسيتين في التشفير المتناظر و هما:

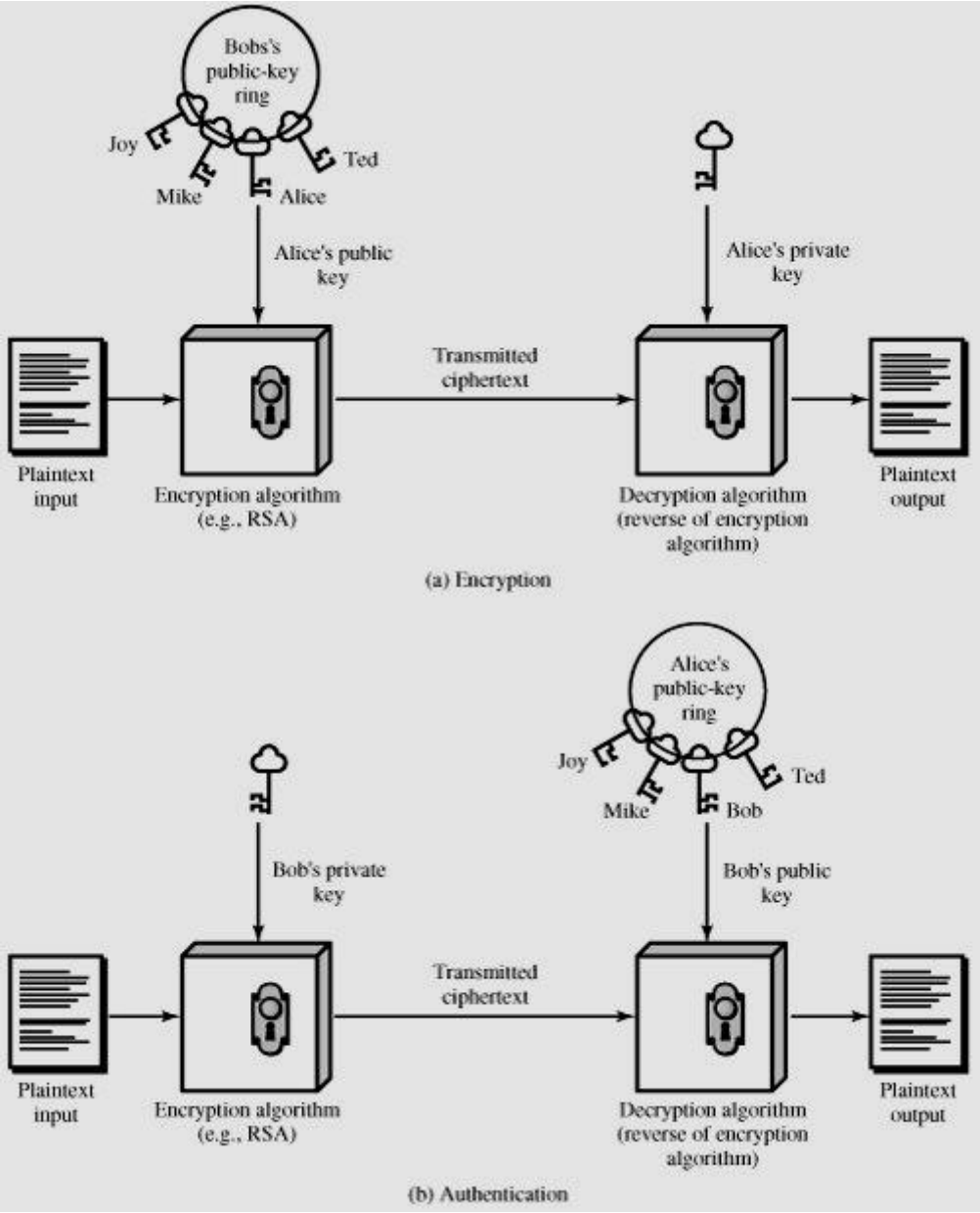
1. توزيع المفتاح: كيف يمكن إرسال مفتاح التشفير للمرسل أو للمستقبل دون احتمال اكتشافه.
2. التوقيع الرقمي: كيف يمكن التأكد من سلامة الرسالة الواردة، و بأنها من المصدر الذي يدعي إرسالها.

1.5.2.1 عناصر التشفير غير المتناظر (بالمفتاح العام)

1. النص الواضح Plaintext: و هو الرسالة الأصلية أو البيانات المراد تشفيرها.
2. خوارزمية تشفير Encryption Algorithm: و تقوم بعمليات رياضية على النص الواضح لتحويله إلى نص مشفر.
3. مفاتيح التشفير العامة و الخاصة: و ذلك بحيث إذا تم التشفير بأحد المفاتيح يتم فك التشفير بالآخر.

4. النص المشفر Ciphertext: و هو الرسالة المشفرة الناتجة كخرج نهائي لعملية تشفير الرسالة الأصلية. و تتعلق بالرسالة الأصلية و المفتاح المستخدم، بمعنى مع تغيير المفتاح يتغير النص المشفر لنفس النص الأصلي.
5. خوارزمية فك التشفير Decryption Algorithm: و تعمل بشكل أساسي عكس عمل خوارزمية التشفير؛ فتأخذ كدخل النص المشفر و مفتاح التشفير الآخر و تعطي كخرج النص الأصلي.

و يوضح الشكل 11 التشفير بالمفتاح العام.



الشكل 11 التشفير بالمفتاح العام لحالتين a المفتاح العام b المفتاح الخاص

2.5.2.1 خصائص التشفير بالمفتاح العام:

1. من غير الممكن عملياً، في حال معرفة أحد المفاتيح و خوارزمية التشفير المستخدمة، استنتاج المفتاح المقابل.
2. من السهل التشفير أو فك التشفير عند معرفة المفتاح المطلوب.
3. بعض خوارزميات المفتاح العام يمكن أن تستخدم أياً من المفتاحين للتشفير.

3.5.2.1 تطبيقات التشفير بالمفتاح العام:

كما أشرنا، تعمل خوارزميات التشفير بالمفتاح العام باستخدام خوارزمية تشفير و مفتاح عام معروف للجميع و مفتاح خاص لا يعرفه إلا صاحبه. و بحسب المفتاح المستخدم للتشفير (عام أو خاص)، يمكن أن نصنف التطبيقات التي تعمل باستخدام هذه التقنية إلى ما يلي:

1. التشفير أو فك التشفير: يقوم المرسل بالتشفير باستخدام المفتاح العام للمستقبل. و هذا يؤمن السرية.
2. التوقيع الرقمي: يقوم المرسل بتوقيع الرسالة باستخدام مفتاحه الخاص (الذي لا يعرفه غيره)، و يتم التوقيع عن طريق تابع خاص يستخدم إما الرسالة كاملة أو جزءاً منها. و بالتالي يستطيع المستقبل التحقق من التوقيع باستخدام المفتاح العام للمرسل. و هذا يؤمن الأصالة Authentication، و عدم الإنكار Non-Repudiation.
3. تبادل المفاتيح: يتعاون المرسل و المستقبل لتبادل مفتاح الجلسة Session Key، و الذي يمكن أن يتم باستخدام المفاتيح الخاصة للطرفين.

و لا بد من التنويه بأن بعض خوارزميات التشفير مناسبة لجميع التطبيقات السابقة، و بعضها الآخر يستخدم لتطبيق و احد أو اثنين فقط. و الجدول 4 يعرض بعض أشهر خوارزميات التشفير بالمفتاح العام و التطبيقات التي تدعمها.

Algorithm	Encryption/Decryption	Digital Signature	Key Exchange
RSA	Yes	Yes	Yes
Elliptic Curve	Yes	Yes	Yes
Diffie-Hellman	No	No	Yes
DSS	No	Yes	No

جدول 4 أهم خوارزميات التشفير بالمفتاح العام و التطبيقات التي تدعمها

و سنقوم في الفقرة التالية بدراسة خوارزمية RSA، و التي تعتبر من أشهر خوارزميات التشفير غير المتناظر.

4.5.2.1 خوارزمية RSA

تعتبر هذه الخوارزمية الأكثر استخداماً في التشفير بالمفتاح العام. و طورت هذه الخوارزمية من قبل ثلاثة باحثين هم Rivest و Shamir و Adleman العاملون في معهد MIT في الولايات المتحدة الأمريكية، و ذلك عام 1977. تعتمد هذه الخوارزمية على استخدام الأعداد الأولية بطول كبير (مثل 1024 بيت) و التوابع الأسية للحقول المنتهية في الرياضيات [Stallings W. A., 2002].

تعمل خوارزمية RSA على توليد المفاتيح و التشفير و فك التشفير، كما يلي:

- توليد المفاتيح: يقوم كل طرف من الاتصال بتوليد مفاتيحه العام و الخاص كما يلي (لمرة واحدة):
  1. اختيار عددين أوليين بشكل عشوائي و بطول كبير و ليكونا p و q.
  2. احتساب جداء العددين و ليكن $n=p\times q$.
  3. احتساب التابع ø() كما يلي: $ø(n)=(p-1)(q-1)$.
  4. اختيار مفتاح تشفير e عشوائياً، بحيث يحقق: $1<e<ø(n)$ و القاسم المشترك الأكبر بينهما هو 1، $gcd^2(e, ø(n))=1$.
  5. احتساب مفتاح فك التشفير d و الذي يحقق: $e\times d \bmod ø(n)=1$ ، أي باقي قسمة $e\times d$ على التابع ø(n) يساوي 1، أي أنهما أوليان بالنسبة لبعضهما، و $0\le d\le n$.

[2] القاسم المشترك الأكبر لعددين هو أصغر عدد صحيح يقبل العددين القسمة عليه

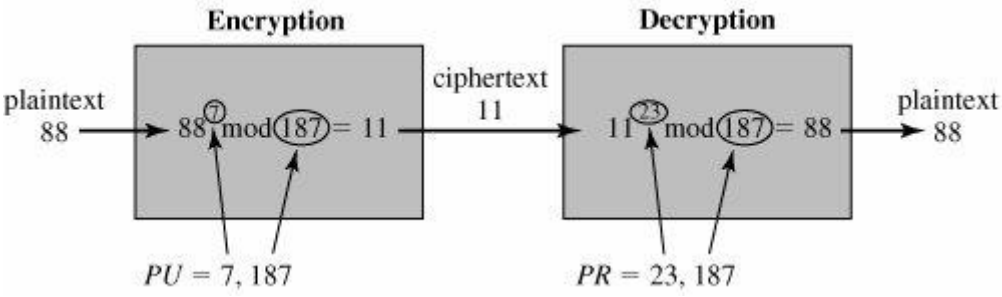
6. ينتج عن ذلك مفتاح التشفير العام وهو PU={e,n}. و مفتاح التشفير الخاص PR={d,n}.
7. يرسل كل طرف مفتاحه العام للآخر.

- التشفير: لنفترض رسالة M، لتشفيرها و بعد معرفة المفتاح العام للمستقبل PU، يكون النص المشفر C كما يلي: $C = M^e \bmod n$, where $0 \le M < n$.
- فك التشفير: يقوم المستقبل باستخدام مفتاحه الخاص PR، باستنتاج النص الأصلي M كما يلي: $M = C^d \bmod n$.

مثال:

1. Select primes: p=17 & q=11
2. Compute n = p×q =17 x 11=187
3. Compute ø(n)=(p–1)×(q-1)=16 x 10=160
4. Select e: gcd(e,160)=1; choose e=7
5. Determine d: d×e mod 160 =1, and d < 160 Value is d=23 since 23x7=161= 10x160+1
6. Publish public key PU={7,187}
7. Keep secret private key PR={23,187}

و يوضح الشكل 12 مثال التشفير السابق على الرسالة 88.



الشكل 12 مثال على خوارزمية RSA

أمن خوارزمية RSA

هناك أربع طرق للهجوم على خوارزمية RSA [Shamir, 2003]:

1. استخدام هجوم Brute-Force و ذلك بتجريب كل احتمالات المفتاح الخاص. و الذي يمكن أن يكون غير فعال مع استخدام مفتاح تشفير بالطول المناسب.

2. الهجوم الرياضي Mathematical Attack، و الذي يكون بتحليل جداء العددين الأوليين المستخدمين.
3. Timing Attack: و يتعلق ذلك بالزمن اللازم لفك التشفير و ربطه بطول مفتاح التشفير الخاص.
4. اختيار النص المشفر: و هي طريقة تستغل خصائص خوارزمية RSA بحيث تحاول اكتشاف المفتاح الخاص من نص المشفر بمواصفات خاصة.

3.1 المعايير العالمية في أمن المعلومات و الشبكات

تم في الآونة الأخيرة تطوير عدد من المعايير و الإرشادات و آليات العمل متعلقة بأمن المعلومات و الشبكات، تساعد هذه المعايير جميع المؤسسات على الوصول لمستوى أمني عالي و متحكم به.

و تعتبر معايير ISO 27K الصادرة عن المنظمة العالمية للمعايير ISO، الأهم من بين جميع المعايير، بالإضافة إلى معايير CobiT، و المعايير الصادرة عن المعهد الوطني للمعايير و التقانة في الولايات المتحدة NIST من الوثائق الهامة في هذا المجال.

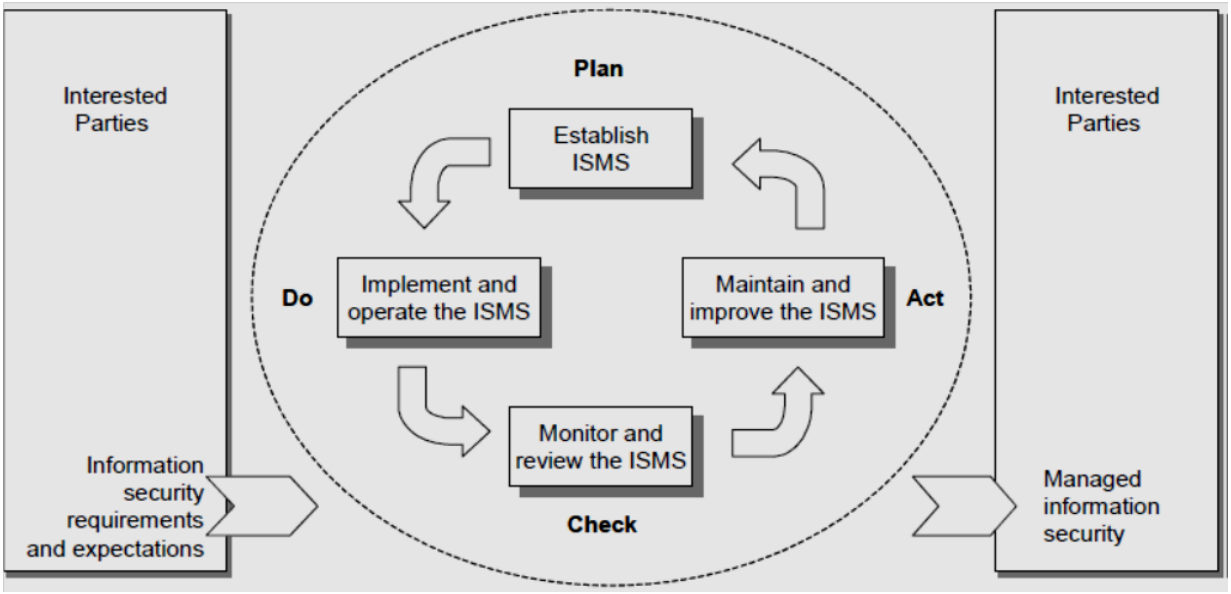
و سنقوم في هذا الفصل بدراسة أهم هذه المعايير.

1.3.1 المعايير الدولية ISO 27000 Family

و تتضمن هذه السلسلة مجموعة معايير تهدف لتنظيم و التحكم و تحقيق استقرار و ظروف آمنة لعمل جميع المؤسسات بغض النظر عن طبيعة عملها. و تتضمن هذه السلسلة المعايير التالية:

1. ISO 27001 (Information Security Management System) ISMS: يحدد متطلبات تأسيس و تطبيق و مراجعة و مراقبة و تحسين توثيق نظام إدارة أمن المعلومات، في إطار سياسة المؤسسات لمعالجة المخاطر [ISO/IEC 27001, 2005].

و يشمل ذلك إجرائية من أربع مراحل: التخطيط و التنفيذ و التحقق و إجراء التعديلات، و يوضح الشكل 13 هذه الإجرائية.



الشكل 13 إجرائية العمل الخاصة بالمعيار ISMS

- التخطيط (تأسيس ISMS): تأسيس أهداف و سياسة و إجرائيات نظام ISMS فيما يتعلق بإدارة المخاطر و تحسين مستوى أمن المعلومات.
- التنفيذ و التشغيل لنظام ISMS: في هذه المرحلة يتم البدء بتطبيق النظام المؤسس.
- التحقق (الرقابة و مراجعة ISMS): يتم هنا تقييم أداء نظام ISMS بالمقارنة مع الأهداف الموضوعة في مرحلة التأسيس، و يتم تسليم تقارير النتائج إلى الإدارة.
- التطوير (تحسين و دعم نظام ISMS): يتم في هذه المرحلة اتخاذ الإجراءات التصحيحية و الاحترازية بموجب المراجعات السابقة و قرارات الإدارة.

2. ISO 27002 و هو تطوير للمعيار ISO 17799 Code of Practice for Information Security Management: يهدف لوضع دلائل عمل و آليات لتحقيق إدارة آمنة للمعلومات. وزعت هذه الآليات على أحد عشر مجالاً [ISO/IEC 27002, 2005]:

أ – السياسة الأمنية.

ب – تنظيم أمن المعلومات.

ت – إدارة الأصول.

ث – أمن الموارد البشرية.

ج – أمن البيئة المحيطة.

ح – إدارة الاتصالات و التشغيل.

خ – التحكم بالوصول للموارد.

د – امتلاك الأنظمة المعلوماتية.

ذ – إدارة حوادث أمن المعلومات.

ر – إدارة استمرارية العمل.

ز – الامتثال.

و تتضمن كل فقرة من المجالات السابقة الغاية من التحكم Control Objective و عدد من الآليات لتحقيق الغاية المطلوبة Controls.

3. ISO 27003 Information security management system implementation guidance: و يتضمن إرشادات و مساعدة لتحقيق المعيار ISO 27001 ISMS.
4. ISO 27004 Information Security Management Measurement: تتضمن إرشادات لتطوير و استخدام مقاييس لتقييم فعالية نظام أمن المعلومات المطبق.
5. ISO 27005 Information Security Risk Management: توفر إرشادات لإدارة المخاطر المحتملة لأمن المعلومات.
6. ISO 27006 Requirements for bodies providing audit and certification of information security management systems: و تتضمن متطلبات الجهات المخولة بمنح شهادات و مراجعة أمن المعلومات للمؤسسات.

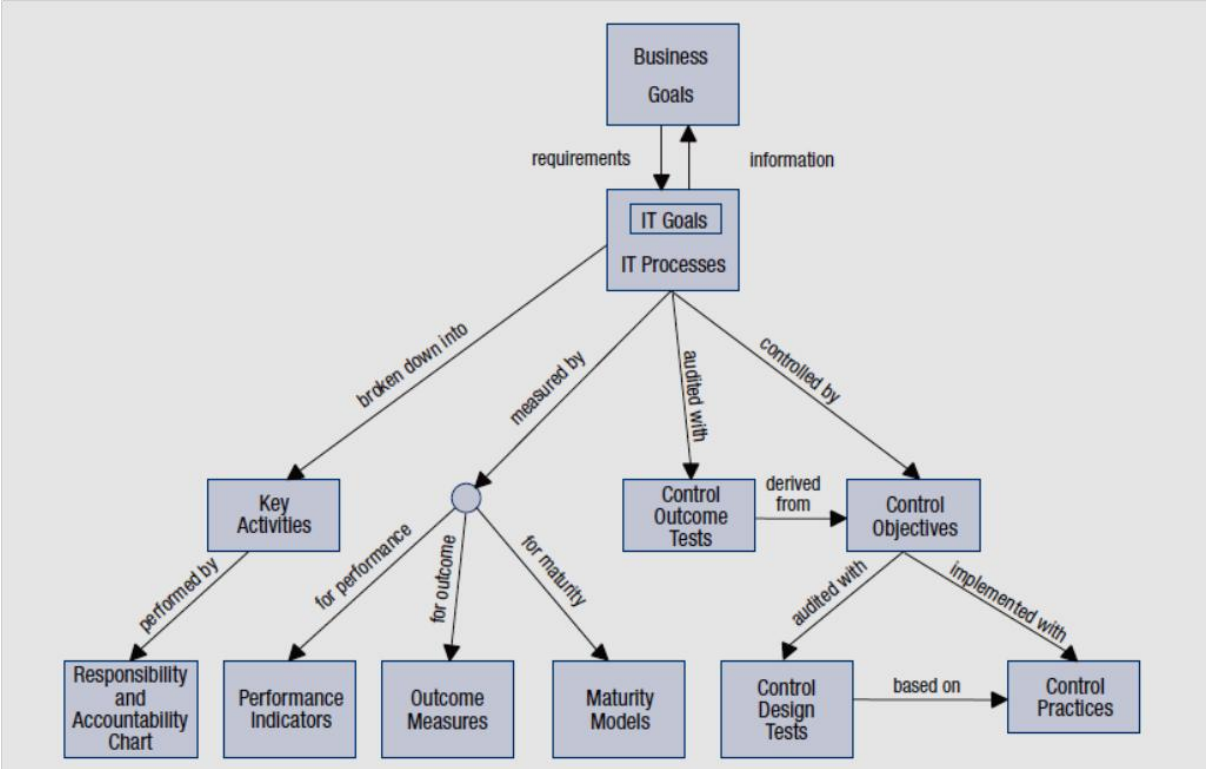
2.3.1 المعيار (CobiT) Control Objectives for Information and related Technology

و هو إطار عمل طُوّر من خلال تجميع أفضل التجارب Best Practices للتحكم بتقانة المعلومات و مراجعتها و التحقق منها. يتبنى هذا المعيار معهد حوكمة تقانة المعلومات IT Governance Institute في الولايات المتحدة [ISACA and ITGI, 2007].

يعتبر المعيار CobiT 4.1، و هو آخر إصدار من هذا المعيار أن التحقيق الأفضل لمتطلبات العمل في المؤسسات من خلال أنظمة المعلومات يتم من خلال ما يلي:

- تحقيق متطلبات العمل، أي أهداف المؤسسة المرجوة من النظام المعلوماتي.
- تنظيم عمل النظام المعلوماتي بنموذج محدد و واضح و مقبول بشكل عام.
- تحديد المصادر المطلوبة لنظام المعلومات، حتى تتمكن المؤسسة من تأمينها.
- تعريف أهداف التحكم الإدارية المطلوب توافرها في النظام المعلوماتي المطور.

و يوضح الشكل 14 العلاقة بين مكونات إطار العمل في CobiT 4.1:

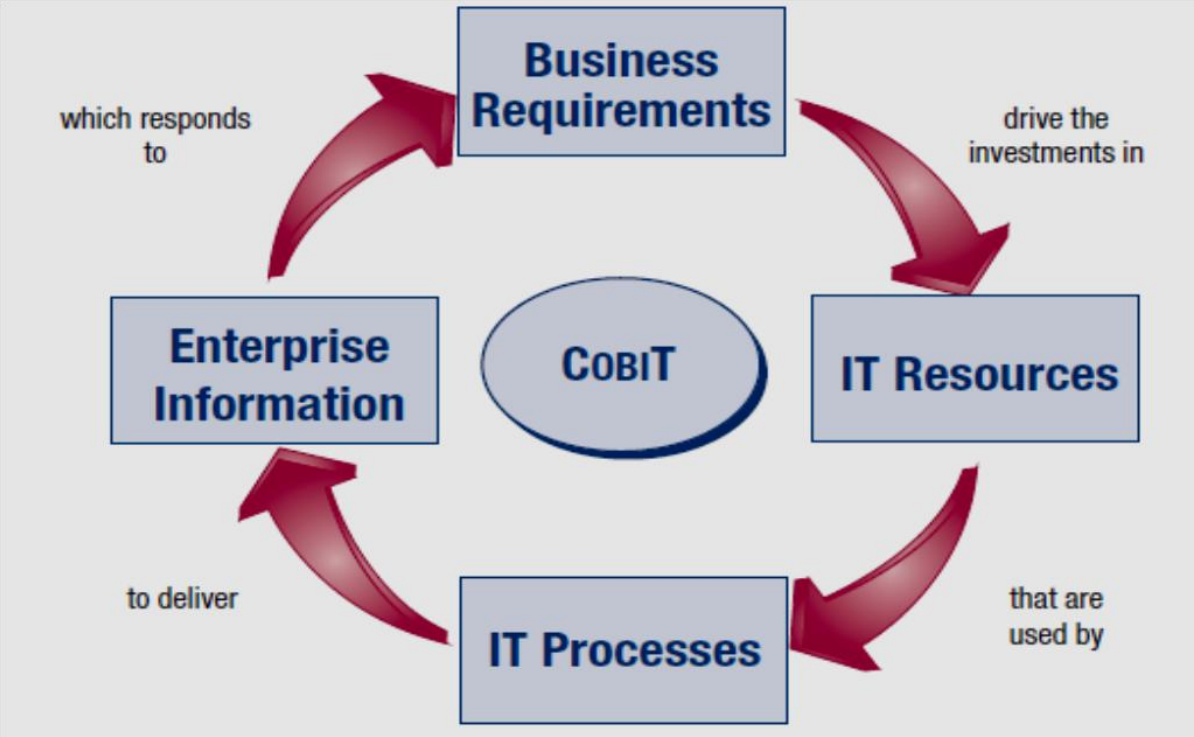


الشكل 14 العلاقات بين مكونات إطار العمل CobiT 4.1

1.2.3.1 شرح إطار العمل المقترح CobiT Framework

يعتمد إطار العمل على المبدأ التالي: توفير المعلومات التي تحتاجها المؤسسة لتحقيق أهدافها، و بالتالي يتطلب ذلك إنفاق المؤسسة للأموال و الاستثمار و التحكم بموارد المعلومات، و يتم ذلك عن طريق مجموعة من الإجراءات لتقديم الخدمات المطلوبة التي توفر في النهاية المعلومات الصحيحة و العملية للمؤسسة.

إدارة المعلومات و التحكم بها يعتبر لب إطار العمل CobiT و الذي وضع بالتوازي مع متطلبات و أهداف عمل المؤسسة. يوضح الشكل 15 المبدأ الأساسي لإطار العمل CobiT4.1.

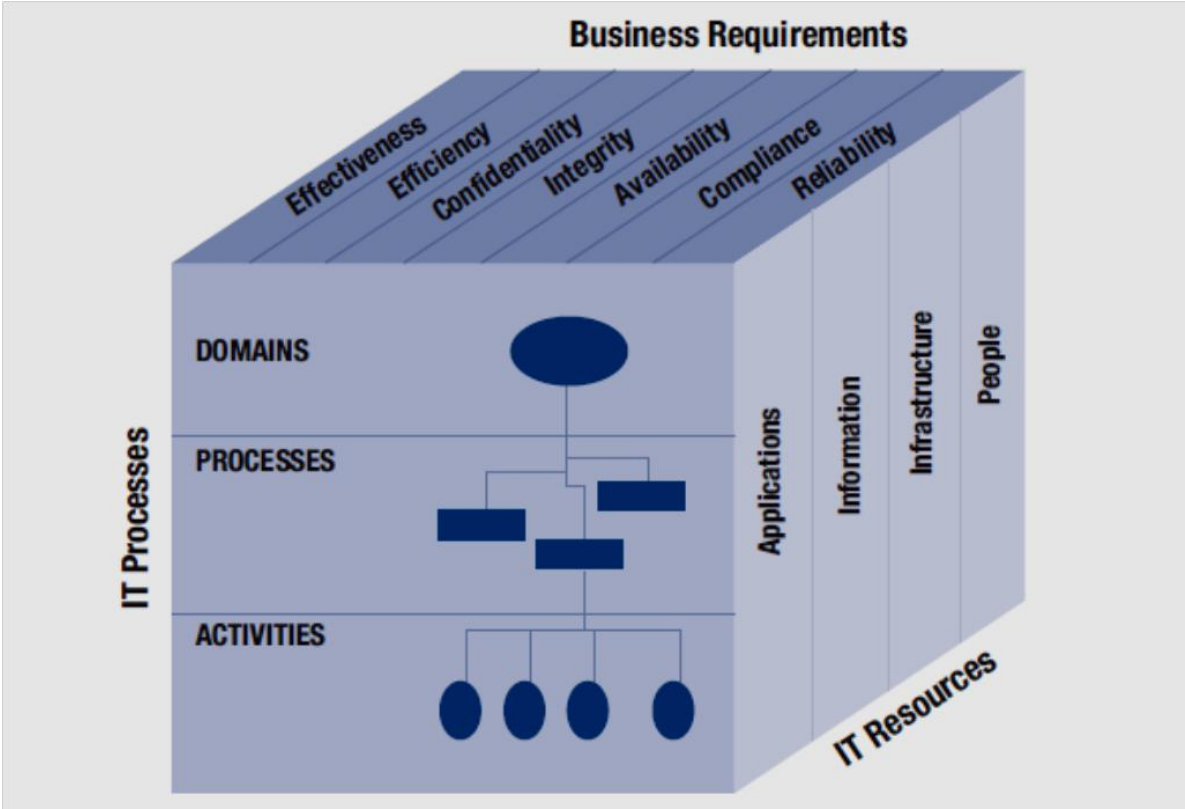


الشكل 15 المبدأ الأساسي لإطار العمل CobiT4.1

لتحقيق أهداف العمل في المؤسسات، يجب أن تحقق أنظمة المعلومات العاملة في المؤسسات المعايير التالية:

1. الفعالية Effectiveness: و تتحقق بكون المعلومات مرتبطة و مفيدة لعمل المؤسسة، و متوفرة عند الحاجة إليها و بالصيغة و الشكل المناسب للمؤسسة.
2. الكفاءة Efficiency: الاستخدام الأمثل و في أقصى حدوده للأنظمة المعلوماتية للاستفادة القصوى من مصادر المعلومات و بشكل اقتصادي لموارد المؤسسة.
3. السرية Confidentiality: حماية المعلومات من الوصول إليها لغير المصرح لهم.
4. السلامة Integrity: سلامة المعلومات و دقتها.
5. الاتاحية Availability: توفر المعلومات عند الحاجة إليها الآن و في المستقبل.
6. الامتثال Compliance: امتثال المعلومات و أنظمة المعلومات للقوانين و الأنظمة الحاكمة داخل و خارج المؤسسة.
7. الموثوقية Reliability: إمداد الإدارة بالمعلومات المناسبة التي تساعدها على اتخاذ القرارات الصائبة.

يوضح الشكل 16 الترابط الوثيق بين متطلبات العمل و إجرائيات أنظمة المعلومات و المصادر (التطبيقات و المعلومات و البنية التحتية و المستخدمين).



الشكل 16 مكعب CobiT

و فيما يخص متطلبات العمل المتعلقة مباشرة بأمن المعلومات فقد حددت CobiT 4.1 عدة معايير أهمها ISO 27000 Series، و التي تطرقنا لها سابقاً.

4.1 المنشورات الخاصة بالمعهد الوطني للمعايير و التقانة

تعتبر المنشورات الخاصة Special Publication SP800 Series الصادرة عن المعهد الوطني للمعايير و التقانة National Institute of Standards and Technology في الولايات المتحدة، من أهم الوثائق الخاصة بأمن المعلومات و أسس قياسها و معايير و إرشادات تطبيقها.

Special Publication SP800-53A 1.4.1

طبعت هذه الوثيقة بعنوان "دليل تقييم متحكمات أمن المعلومات لأنظمة المعلومات الاتحادية و للمؤسسات" [NIST 800-53, 2010]. و يقصد هنا بمتحكمات أمن المعلومات الإجراءات و آليات العمل التي تتحكم بأمن المعلومات التي تتبعها المؤسسات.

و قد وضع بهدف تسهيل عملية تقييم متحكمات أمن المعلومات في المؤسسات في إطار إدارة المخاطر، و الذي يزود إدارة المؤسسة بما يلي:

1. مدى فعالية هذه المتحكمات في أنظمة المعلومات المستخدمة في المؤسسة.
2. مؤشرات على جودة نظام إدارة المخاطر المعتمد.
3. معلومات عن نقاط القوة و الضعف في الأنظمة المعلوماتية في إطار أهداف المؤسسة و الخدمات التي تقدمها.
4. مساعدة الإدارة في اتخاذ القرار.

1.1.4.1 إجرائية العمل (التقييم) في SP800-53A

تتضمن إجرائية التقييم النقاط التالية:

1. نشاطات (واجبات) المؤسسة و المقيمين لتحضير تقرير تقييم أمن المعلومات.
2. تطوير خطة تقييم أمن المعلومات.
3. القيام بعملية التقييم و التحليل و التوثيق و تحضير التقرير النهائي.
4. تقرير المتابعة بعد قيام المؤسسة بالإجراءات و النصائح الواردة في التقرير النهائي.

و سنقوم في الفقرات التالية بشرح خطوات الإجرائية.

التحضير لتقييم متحكمات أمن المعلومات:

تعتبر عملية تقييم أمن المعلومات في أي مؤسسة و بخاصة المؤسسات الكبرى، عملية صعبة و معقدة و تتطلب التعاون الكامل من جميع الأطراف ذات العلاقة مثل إدارة المؤسسة و المسؤولين عن أنظمة المعلومات و المستخدمين و الجهات الخارجية المشغلة و المطورة لأنظمة المعلومات العاملة في المؤسسة –إن وجدت– بالإضافة إلى مسؤولي أمن المعلومات في المؤسسة. و من وجهة نظر المؤسسة المدروسة، يجب أن تتضمن نشاطات التقييم النقاط التالية:

- التأكد من استخدام السياسات الأمنية المناسبة للتقييم و بأن تكون مفهومة لجميع عناصر المؤسسة ذات العلاقة.
- التأكد من تعريف الأهداف Objectives و الغاية من التقييم و نطاقه Scope.
- إعلام مسؤولي المؤسسة بإجراءات التقييم و ذلك قبل إجراء التقييم و ذلك لتأمين الموارد اللازمة لإجراء التقييم.
- تعريف المجال الزمني لعملية التقييم.
- اختيار عناصر فريق عمل كفؤ لإجراء التقييم.
- تعريف آلية العمل بين فريق التقييم و المؤسسة لتحقيق المطلوب من التقييم.

إعداد خطة تقييم أمن المعلومات

تعرف خطة تقييم أمن المعلومات أهداف التقييم و خارطة طريق واضحة و مفصلة لطريقة التقييم المتبعة. و تتضمن الخطوات التالية ما يراعيه المقيّمون في إعداد الخطة:

1. تحديد متحكمات أمن المعلومات التي يجب أن تتضمنها الخطة.
2. اختيار إجراءات التقييم المناسبة و التي ستستخدم خلال التقييم. و التي تهدف لتحسين متحكمات أمن المعلومات.
3. تعديل إجراءات التقييم بما يضمن أهداف الخطة.
4. إعداد إجراءات تقييم إضافية و بحسب الحاجة، في حال لم يتضمنها المعيار SP800-53.
5. إنهاء الخطة و مصادقتها من المؤسسة و الحصول على تفويض بتنفيذ الخطة.

إجراء عملية التقييم

بعد أن تم تصديق الخطة من المؤسسة، يمكن لفريق التقييم البدء بتنفيذ الخطة، و ذلك ضمن جدول زمني محدد. و يسمى الخرج المطلوب من عملية التقييم بتقرير تقييم أمن المعلومات.
يحوي التقرير النقاط التالية:

- اسم نظام المعلومات المدروس.
- تصنيف النظام من الناحية الأمنية.
- موقع التقييم و التاريخ.
- اسم المقيّم.
- التقييم السابق –إن وجد–.
- متحكم الأمن المستخدم، أو التحسينات المقترحة عليه.
- أهداف التقييم و الطريقة المتبعة في التقييم.
- مدى التقييم.
- ملخص نتائج التقييم.
- ملاحظات المقيّم.
- توصيات المقيّم.

و يوضح الشكل 17 مثالاً على تقرير عملية التقييم لخطة طوارئ المؤسسة لنظام المعلومات المستخدم.

CP-2.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization develops a contingency plan for the information system that:* - *identifies essential missions and business functions and associated contingency requirements;* **(S)** - *provides recovery objectives, restoration priorities, and metrics;* **(S)** - *addresses contingency roles, responsibilities, assigned individuals with contact information;* **(O)** - *addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure;* **(S)** - *addresses eventual, full information system restoration without deterioration of the security measures originally planned and implemented;* **(S)** *and* - *is reviewed and approved by designated officials within the organization;* **(O)** *(ii) the organization defines key contingency personnel (identified by name and/or by role) and organizational elements designated to receive copies of the contingency plan;* **(O)** *and* *(iii) the organization distributes copies of the contingency plan to organization-defined key contingency personnel and organizational elements.* **(O)** **Comments and Recommendations:** CP-2.1 (i) is marked as *other than satisfied* because the contingency plan prepared by the organization did not assign individuals to contingency roles and provide contact information. There was also no evidence that the contingency plan had been reviewed and approved by designated organizational officials. CP-2.1 (iii) is marked as *other than satisfied* because the organization had not distributed copies of the contingency plan to key contingency personnel and organizational elements critical to executing the plan.

الشكل 17 تقرير التقييم لخطة الطوارئ لنظام المعلومات

تحليل نتائج تقرير تقييم المعلومات

تقوم المؤسسة من خلال المختصين فيها بأمن المعلومات بتحليل التقرير النهائي للتقييم و دراسة نتائجه من حيث نقاط الضعف المكتشفة و إجراءات تحسين مستوى أمن المعلومات المقترحة من فريق التقييم. من ثم تقوم المؤسسة باتخاذ الإجراءات اللازمة لتنفيذ المقترحات. ويتم ذلك بتطوير خطة أمن المعلومات و تنفيذها. و في النهاية إعلام فريق التقييم بالإجراءات التي تمت، و طلب إعادة التقييم، إذا رغبت الإدارة ذلك. و بعد ذلك يزود فريق التقييم الإدارة بتقرير المتابعة بعد قيام المؤسسة بالتعديلات المطلوبة و الحالة الأمنية النهائية للمؤسسة.

2.4.1 دليل العمل لقياس الأداء لأمن المعلومات NIST SP800-55 rev1

يعتبر هذا المعيار هام جداً فيما يخص موضوع البحث لتصميم نموذج جديد لأمن المعلومات و الشبكات و تحويل النموذج لنظام مؤتمت قادر على قياس مستوى أمن المعلومات كقيم رقمية تعكس حالة المؤسسة المدروسة و الإجراءات الواجب اتخاذها للوصول لمستوى أمني مقبول مقارنة بالمعايير العالمية الواردة في هذا البحث و خاصة ISO 27000 Series.

و لكي نتمكن من تحقيق أهداف البحث بإيجاد آلية لقياس مستوى أمن المعلومات كمياً – رقمياً– مما يسهل تقييم المؤسسة المدروسة و تحسين مستوى أمن المعلومات فيها، لا بد من دراسة المعايير العالمية المنشورة و أوراق البحث المتعلقة بالقياس الكمي و أصوله.

و تعتبر الطبعة الخاصة SP800-55 rev1 من المطبوعات الهامة في هذا المجال [NIST 800-55, 2005]، و سنقوم فيما يلي بشرح أهم التوجيهات الموجودة فيها.

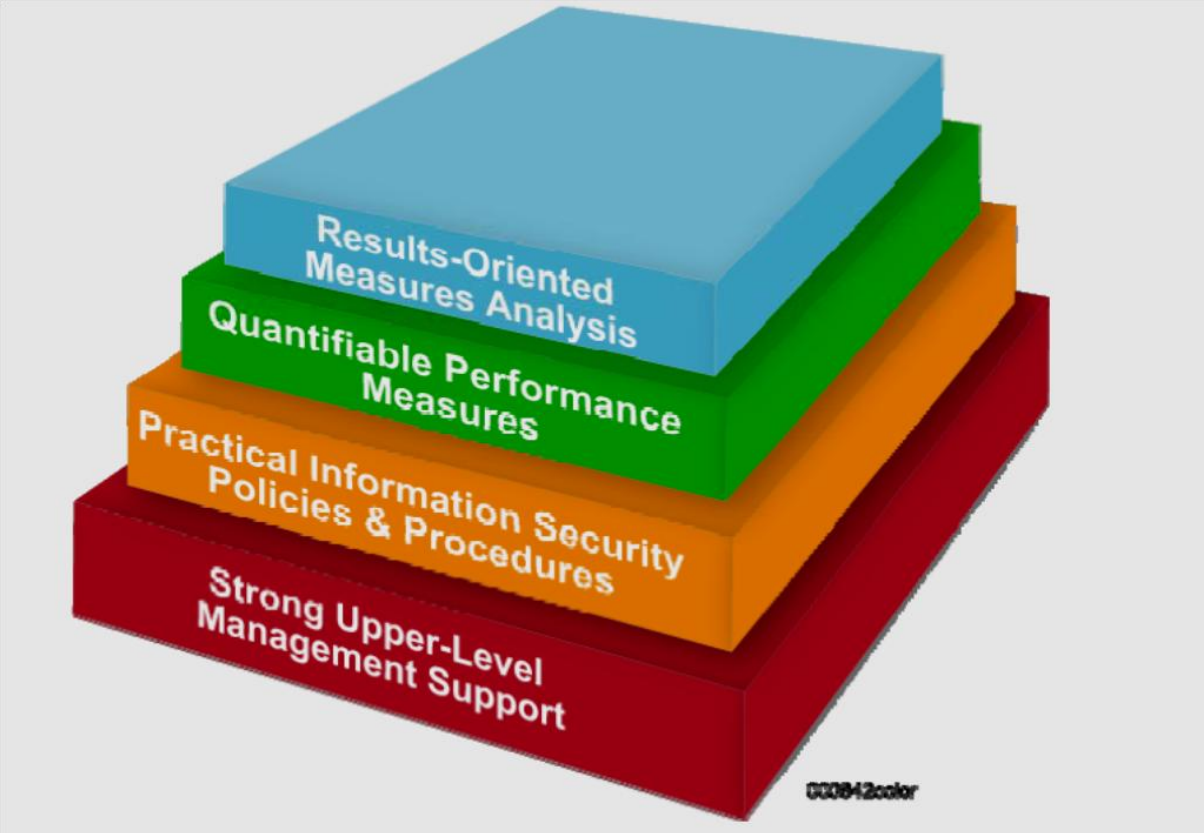
1.2.4.1 هدف الدليل و مداه

تعتبر الوثيقة دليل عمل لتطوير و اختيار و تطبيق قياسات لأنظمة المعلومات و البرامج المستخدمة لدراسة فعاليتها و كفاءتها و فعالية متحكمات أمن المعلومات المستخدمة. و تقدم دليل عمل للمؤسسة باستخدام قياسات حقيقية، لتقييم إجراءاتها و متحكمات أمن المعلومات المستخدمة و سياساتها الأمنية.

يوضح الدليل بنية برنامج قياس أمن المعلومات بعوامل النجاح التالية:

- الدعم الواضح للإدارة العليا في المؤسسة لعملية القياس و لأمن المعلومات بشكل عام، بما يتضمن تخصيص الأموال و الكادر الخاص بذلك.
- سياسات و إجراءات أمن المعلومات العملية المطبقة.
- القياس الكمي لأداء الأنظمة المعلوماتية من الناحية الأمنية.
- تحليل نتائج القياس.

و يوضح الشكل 18 بنية برنامج قياس أمن المعلومات.



الشكل 18 بنية برنامج قياس أمن المعلومات

2.2.4.1 الفوائد من استخدام المقاييس Measures

يقدم برنامج القياس الكمي فوائد عديدة للمؤسسات و أهمها:

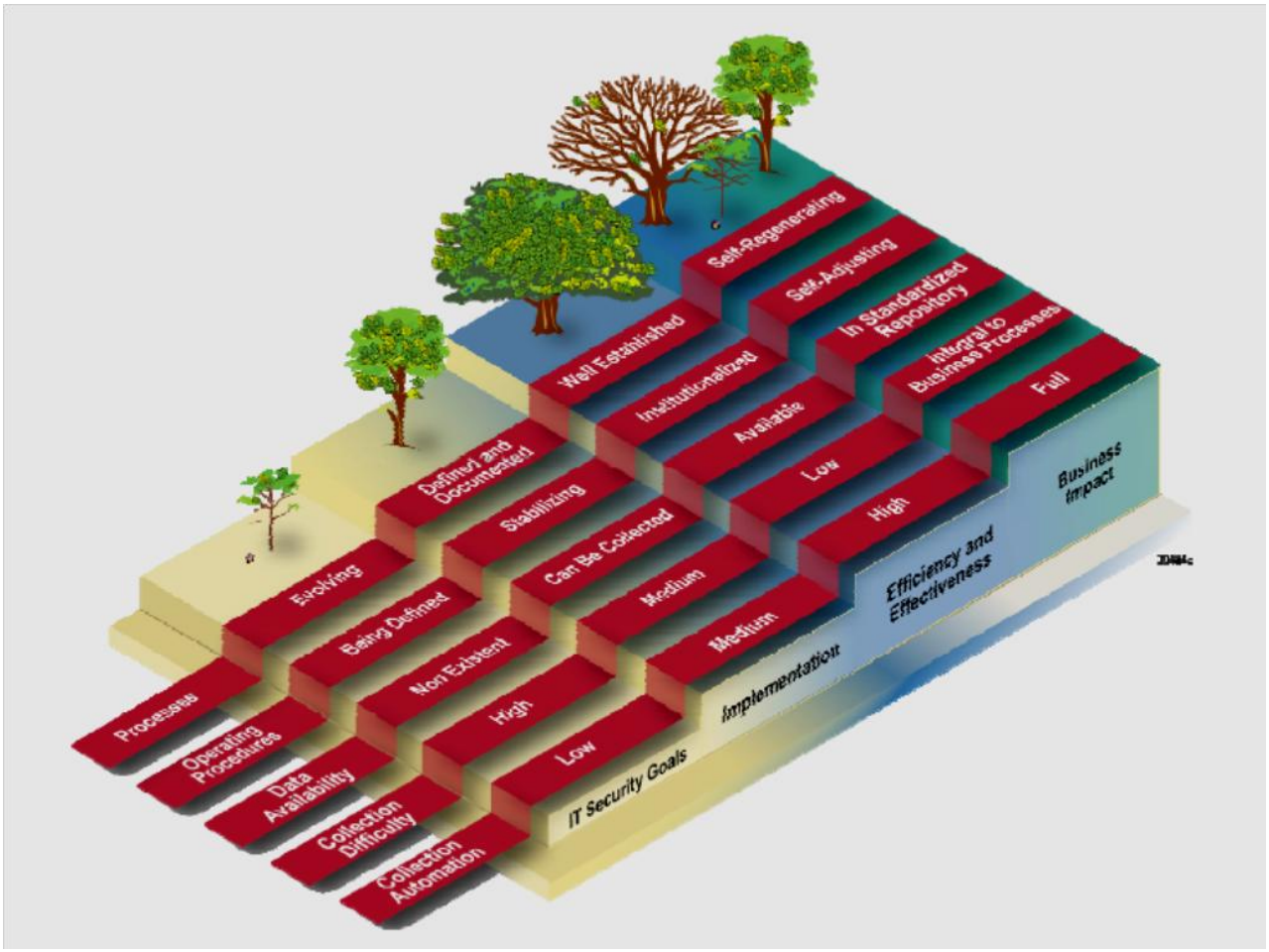
1. تعزيز المحاسبة Increase Accountability: يمكن لقياس أمن المعلومات تعزيز إمكانيات الإدارة لتقييم و محاسبة نظام أمن المعلومات المستخدم في المؤسسة من خلال تقييم متحكمات أمن المعلومات و تحديد الخلل فيها، كما يمكن من خلال عملية جمع المعلومات و تحليل واقع أمن المعلومات في المؤسسة تسهيل تعريف المسؤوليات و الأشخاص المسؤولين عن هذه الإجراءات و بالتالي التحكم بها و تعديلها بما يخدم تحسين المحاسبة.
2. تحسين فاعلية نظام أمن المعلومات Improve Information Security Effectiveness: يتيح برنامج قياس أمن المعلومات للمؤسسات متابعة التطور الحاصل لنظام أمن المعلومات و الحصول على معلومات رقمية –كمية– عن تحسين قدرة النظام المعلوماتي للوصول لأهداف المؤسسة و استراتيجياتها. كما يؤمن تحديد فاعلية البرامج و الإجراءات و السياسات المطبقة في

المؤسسة، و خاصة عند حصول حوادث أمنية كمحاولات الاختراق أو تعطل البرامج أو انهيار التجهيزات الصلبة Hardware.

3. الامتثال Compliance: يمكن للمؤسسات التحقق من امتثال المؤسسة للقوانين و الأنظمة و القواعد التي تخضع لها المؤسسة، عن طريق تنفيذ برنامج قياس أمن المعلومات. كما يساعد البرنامج تقارير المؤسسة السنوية و مدى تطابقها مع القوانين الناظمة للرقابة الحكومية.
4. تزويد المؤسسة بدخل كمي لدعم قرارات تخصيص الموارد Resource Allocation Decisions: تجبر الضغوط المالية و شروط السوق الحكومات و المؤسسات لتخفيض ميزانياتها. و في مثل هذه البيئة، يصعب تبرير الإنفاق على أنظمة أمن المعلومات، و التي يجب أن تطرح كداعم لنظام إدارة المخاطر. و يمكن للقياس الكمي للمخاطر المساعدة في دعم القرار بتخصيص الأموال الضرورية لنظام المخاطر و أمن المعلومات.

3.2.4.1 أنواع القياسات Types of Measures

يحدد نُضج برنامج أمن المعلومات في المؤسسة نوع القياسات التي يجب الحصول عليها. و يمكن تعريف نُضج البرنامج بوجود و تأسيس الإجراءات و العمليات. و عندما ينضج برنامج أمن المعلومات تكون جميع تفاصيله معرفه و موثقه و متوافقة مع المعايير و القوانين ذات الصلة. يوضح الشكل 19 أن برامج أمن المعلومات غير الناضجة بحاجة لتطوير أهدافه و إجراءاته قبل أن يتمكن من قياسات فعالة.



الشكل 19 نضج برنامج أمن المعلومات و أنواع القياسات

يمكن تصنيف أنواع القياسات كما يلي:

1) قياسات التطبيق Implementation Measures: يستخدم لإظهار التقدم في تطبيق برامج أمن المعلومات و متحكمات أمن المعلومات و السياسات و الإجراءات. و كأمثلة على هذا النوع متعلقة ببرامج أمن المعلومات نورد: النسبة المئوية لتطابق الأنظمة المعلوماتية مع خطط نظام أمن المعلومات المصدقة من المؤسسة، و النسبة المئوية لتطابق أنظمة المعلومات مع سياسة كلمات السر للدخول للبرامج، و الذي يكون من 100%.
2) قياسات الفعالية و الكفاءة Effectiveness/Efficiency Measures: تستخدم لمراقبة فيما إذا كانت إجراءات البرامج و متحكمات الأمن على مستوى الأنظمة قد طبقت بشكل صحيح و تعمل كما هو مطلوب و تعطي الخرج المتوقع. و كمثال على ذلك النسبة المئوية لتحصين نقاط الضعف في أنظمة التشغيل المستخدمة عن طريق تطبيق Patches أو توقيف الخدمات غير المستخدمة.

3) قياسات التأثير Impact Measures: تستخدم لتوضيح تأثير أمن المعلومات على مهمة المؤسسة و أهدافها. و بحسب نوع المؤسسة و الغاية منها، يمكن تصنيف قياسات التأثير كما يلي:

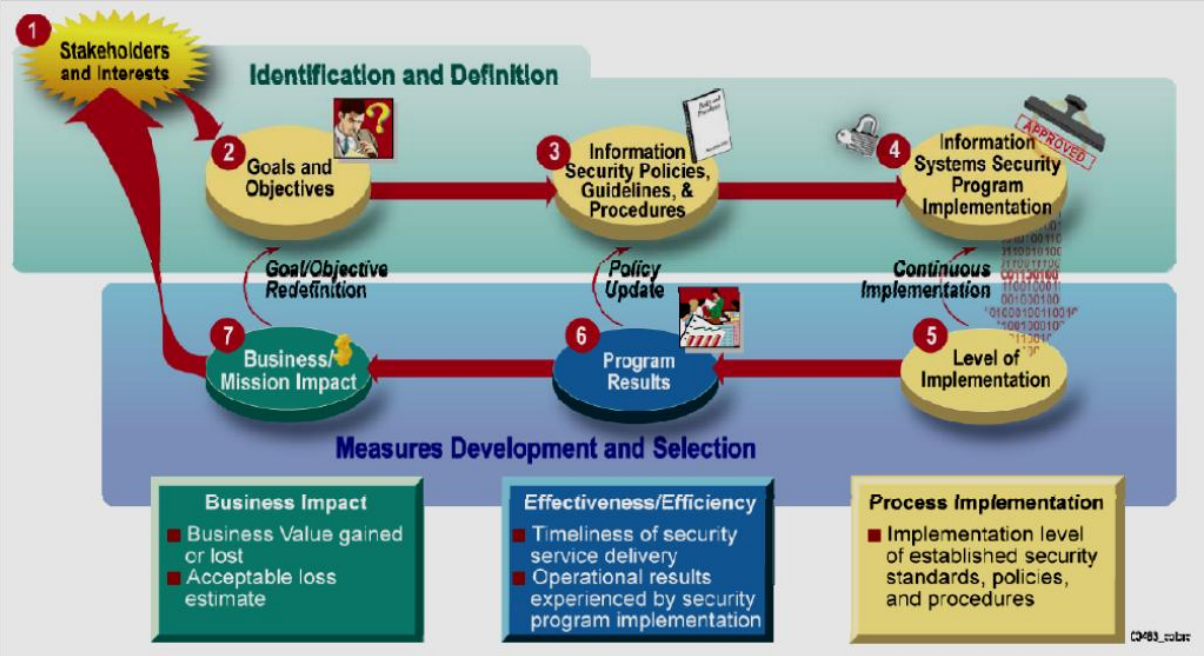
- توفير التكاليف الناتجة عن برنامج أمن المعلومات عن طريق تعديل و تطوير الإجراءات و غيرها أو بالإجراءات الفعالة عند الحوادث التي تؤدي إلى توقف الخدمات و بالتالي إلى خسائر مادية، فالإجراءات الفعالة توقف هذه الخسائر.
- درجة ثقة المستهلكين (الزبائن) بالمؤسسة، و التي تتدعم ببرنامج أمن المعلومات.
- التأثيرات الأخرى المتعلقة بمهمة المؤسسة.

4.2.4.1 تصميم عملية القياس

يتضمن تصميم و تطوير عملية القياس النقطتين التاليتين:

- تعريف و تحديد برنامج أمن المعلومات.
- تطوير و اختيار آليات قياس محددة لقياس التطبيق و الفعالية و الكفاءة و التأثير لمتحكمات أمن المعلومات.

يوضح الشكل 20 المراحل المتبعة في تصميم و تطوير عملية القياس.



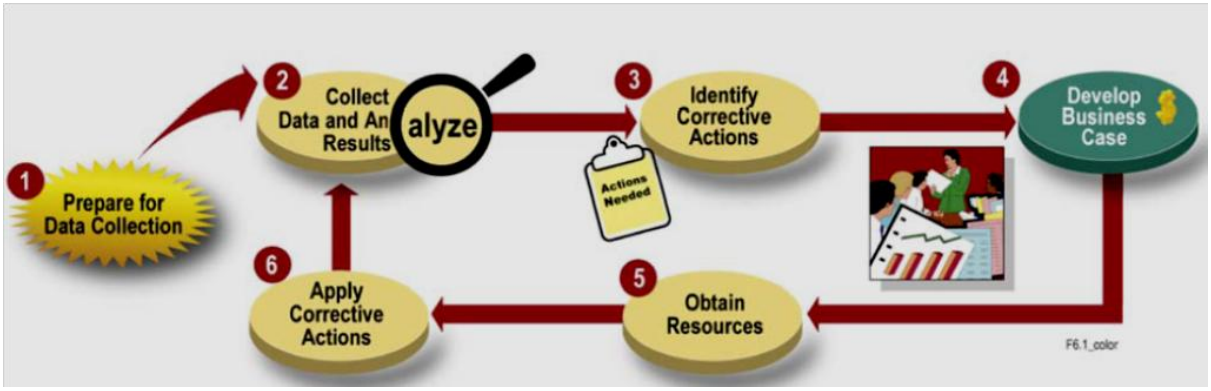
الشكل 20 مراحل تصميم و تطوير عملية القياس

و التي تشمل المراحل التالية:

1. تعريف أهداف المالكين: و يتضمن تحديد أهداف إدارة المؤسسة و مالكيها التي ترجوها من نظام أمن المعلومات الذي تهدف العملية لتطويره.
2. أهداف و غايات النظام: تعريف و توثيق الهدف و الغاية من النظام المطور بما فيها الأهداف التقنية و المالكين و مدى التطابق مع المعايير الدولية و القوانين التي تخضع لها المؤسسة.
3. مراجعة سياسات أمن المعلومات و أدلة العمل و الإجراءات: و تتضمن مراجعة كاملة لإجراءات المؤسسة الحالية في ما يخص أمن المعلومات و مدى فعاليتها. و التطويرات اللازمة.
4. مراجعة تطبيق برنامج أمن المعلومات: مراجعة و تحديد كافة البيانات و المصادر المتوفرة و تحديد دلائل تطبيق الإجراءات و تعديلها.
5. اختيار و تطوير القياسات: تتضمن المراحل 5 و 6 و 7 يتم تحديد طرق القياس و أدواتها، بما يضمن التطبيق و الفعالية/الكفاءة و التأثير.
6. التغذية الراجعة (رد الفعل) لعملية تطوير نظام أمن المعلومات: و هي مرحلة مهمة جداً لتقييم العمل المنجز و تطويره بما يحقق أهدافه.

5.2.4.1 تنفيذ برنامج أمن المعلومات

بعد تطوير البرنامج و تصديقه من المؤسسة يمكن البدء في تنفيذه. و يتضمن التنفيذ عدة مراحل تبدأ بجمع المعلومات و تحليلها و تحديد الإجراءات التصحيحية و توثيقها و تحديد تكاليف التنفيذ و أخيراً تطبيق التعديلات. يوضح الشكل 21 تنفيذ برنامج أمن المعلومات.



الشكل 21 تنفيذ برنامج أمن المعلومات

من الجدير بالذكر أن الوثيقة NIST SP800-55 rev1 لم تذكر قياسات محددة لمتحكمات أمن المعلومات، بل وضحت آلية تطوير القياسات و أهميتها و ذلك لاختلافها و اختلاف أهميتها بحسب نوع المؤسسة و أهدافها و الخدمات التي تقدمها المؤسسة.

5.1 الهندسة الاجتماعية و حماية المعلومات من المستخدمين

1.5.1 مقدمة

تُنفِق جميع المؤسسات و الشركات في العالم مبالغ طائلة لتأمين شبكاتها و معلوماتها. و قد أوردنا في الدراسات السابقة المعايير العالمية و بعض الدراسات العالمية حول أمن المعلومات و الشبكات و التي تمحورت على البنية التحتية – Firewalls, IPS/IDS, Antivirus, ... – و إعدادات هذه التجهيزات بالإضافة إلى السياسات الأمنية و التي تتضمن ضوابط للعمل على التجهيزات و التحكم بالنفاذ و غيرها. ولكن جميع هذه الإجراءات و المتحكمات لم تعطي الأهمية الواجبة للمستخدمين و الخطر الداخلي للمؤسسات من موظفيها و بخاصة مدراء الأنظمة و مسؤولي أمن المعلومات و المستخدمين الحاليين و السابقين و ما يشكلونه من خطرٍ حقيقيٍ على أمن المعلومات.

كما يمكن استغلال العاملين في المؤسسة للحصول على معلومات هامة تسمح بإلحاق ضرر بالمؤسسة أو بالأفراد.

سنورد في هذا الفصل دراسة لهذا الموضوع و سرد لأهميته و بعض التعريفات ذات العلاقة.

2.5.1 الهندسة الاجتماعية Social Engineering

تُعَّرف الهندسة الاجتماعية [Simon, 2003] بالطريقة التي تُستخدم للحصول على المعلومات من الأشخاص بطريقة الإقناع و الخداع لإقناعهم بأن المعتدي هو شخص آخر يحق له الحصول على المعلومات و ذلك دون استخدام أية تقنية من خلال التجهيزات الأمنية.

و تستخدم الهندسة الاجتماعية للحصول على معلومات تُسهل في مرحلة لاحقة استخدام تقنيات –برامج– للدخول لقواعد البيانات و الحصول على معلومات أو إيقاف خدمات الهدف و بالتالي إلحاق الضرر بالهدف.

3.5.1 الإنسان أهم عامل في نجاح أي مهمة أو فشلها

تتمحور الهندسة الاجتماعية حول الإنسان و نقاط ضعفه و قوته. و كما قال القائد الخالد حافظ الأسد: "الإنسان هو العامل الحاسم في المعركة"، و هذا القول ينطبق على جميع المهام و منها أمن المعلومات فمهما أنفقت المؤسسات و الدول و حتى الأفراد من تقانة و أدوات لحماية معلوماتهم يبقى الإنسان نقطة الضعف و القوة الأساسية. و هنا لا بد أن نؤكد بأن أمن المعلومات هو معركة حقيقية ضد قراصنة

الحواسيب و البرامج الضارة ... Viruses, Worms, Trojan Horses, و الأعداء و المنافسين و غيرهم.

و قد أظهرت الإحصاءات [CERT, 2006] و الدراسات أن 70%-80% من المخاطر على أمن المعلومات تأتي من داخل المؤسسة و ليس من خارجها.

الشكل 22 الإنسان الحلقة الأضعف في أية سلسلة عمل

4.5.1 العوامل التي تجعل الهندسة الاجتماعية فعالة في الحصول على المعلومات

يمكن تصنيف العوامل التي تجعل الهندسة الاجتماعية خطرة و فعالة كالتالي:

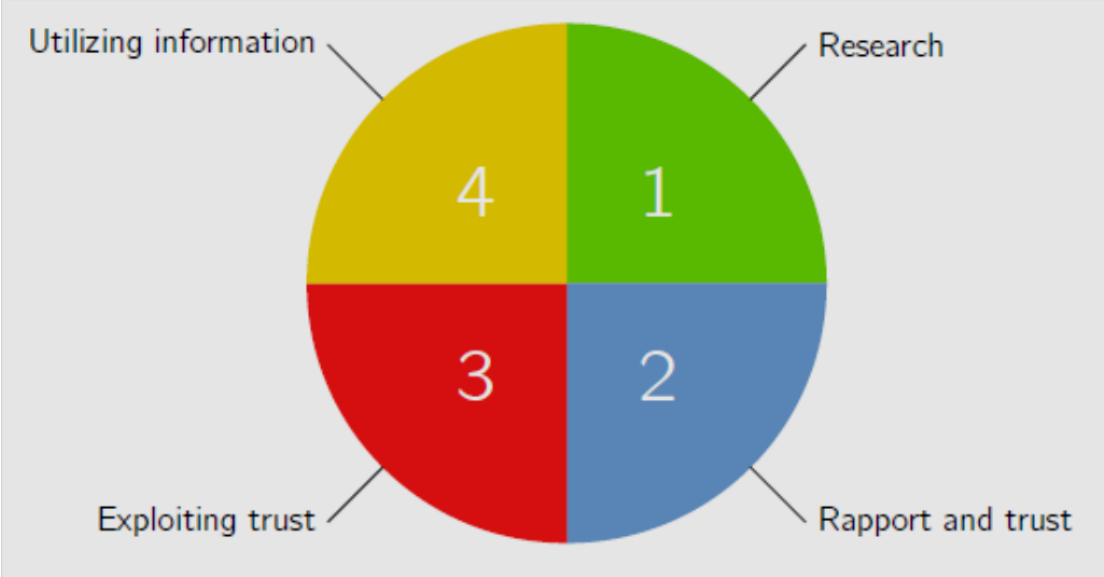
1. عدم وجود تقنيات محددة –برامج أو تجهيزات– للتصدي للهندسة الاجتماعية.
2. التركيز على الإنسان و هو أكثر نقطة ضعف في أية منظومة.
3. صعوبة كشف محاولات الاختراق المبنية عليها.
4. عدم استخدام المهاجمين لسلوك ثابت أو محدد في محاولاتهم.

5.5.1 دورة حياة الهندسة الاجتماعية

إن تعريف دورة حياة محددة للهندسة الاجتماعية ليس بالأمر السهل وذلك لأنه يتمحور حول الإنسان و طريقة استدراج المعلومات و التي تتغير بحسب كفاءة المعتدي و قدرته على الإقناع بالإضافة إلى مناعة و وعي الضحية و ثقافته ضد هذا النوع من الاحتيال، بالإضافة إلى إجراءات المؤسسة للحماية من الهندسة الاجتماعية.

يمكن أن نلخص دورة [Thornburgh, 2004] حياة الهندسة الاجتماعية بالشكل 23.

و من الجدير بالذكر أن دورة الحياة هذه يمكن أن تكون تكرارية بحيث تعاد المرحلة أو المراحل حتى يتحقق الهدف.



الشكل 23 دورة حياة الهندسة الاجتماعية

المرحلة الأولى: البحث Research

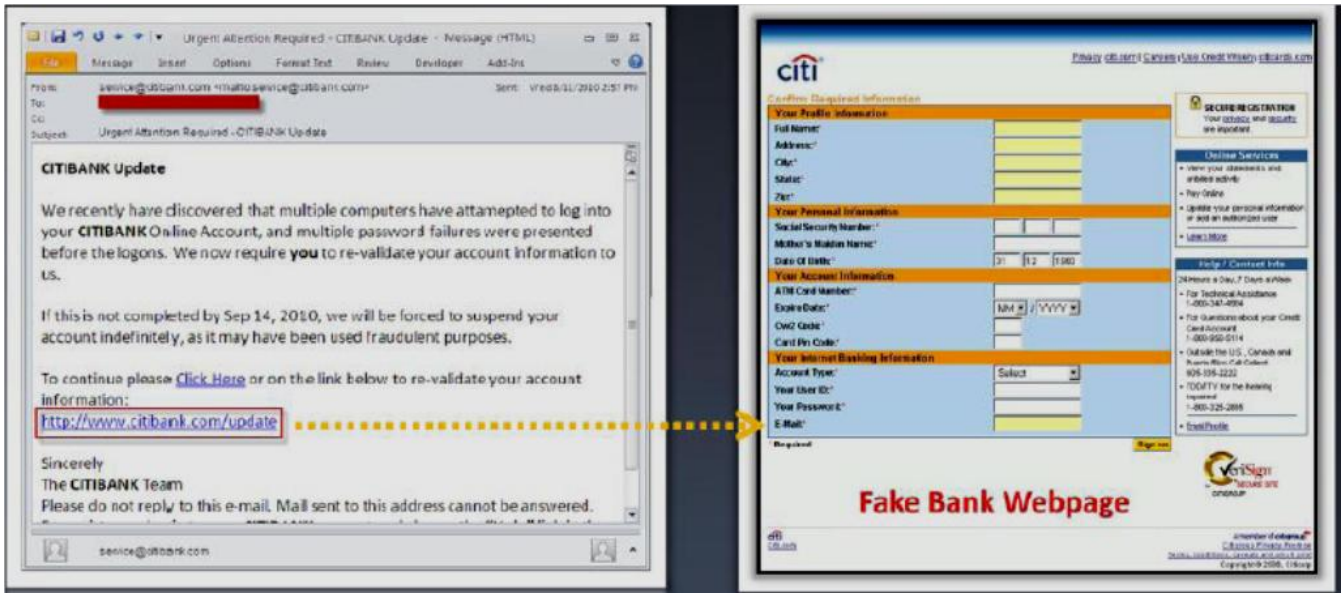
تتضمن هذه المرحلة عدة طرق للحصول على أكبر قدر ممكن من المعلومات حول الهدف. و بعد الحصول على هذه المعلومات يمكن بناء علاقة وثيقة مع الضحية و استغلاله.

و يمكن تصنيف بعض طرق البحث بالتالي:

1. الموقع الالكتروني للمؤسسة Corporate Website: يمكن أن يكون موقع المؤسسة المستهدفة أول مكان يتم البحث فيه عن معلومات. مثل أسماء المدراء و بعض أهم العاملين و أرقام الهواتف و الفاكسات بالإضافة إلى البريد الإلكتروني للمؤسسة و بعض العاملين و الدعم الفني و غيرها.
2. الموقع الالكتروني الشخصي Personal Website: يضع الكثير من الأشخاص على مواقعهم الشخصية معلومات خاصة يمكن الاستفادة منها.
3. البحث في حاويات المهملات Dumpster Diving: تستخدم هذه الطريقة منذ زمن طويل من قبل الجواسيس [Lively, 2003] للحصول على بعض المعلومات الهامة الملقاة في حاويات القمامة للأشخاص و للشركات. و هذه الطريقة مصدر معلومات هام جداً، فيمكن أن يلقي الأشخاص فواتير الهاتف و خطوط الانترنت ADSL أو وصول استلام بطاقات ائتمانية أو غيرها.

الشكل 24 مثال على بعض المعلومات المتوفرة في سلة المهملات

4. تقنية Phishing : و تتم باستخدام بريد إلكتروني مزيف أو موقع مزيف مطابق للموقع الأساسي لإقناع الهدف بأن الرسالة أو الموقع هو لشخص أو لشركة يتعامل معها مثل المصرف أو شركة تقدم الخدمات أو الدعم الفني للهدف و هو يتعامل معها في الواقع، ثم يقوم الهدف بإدخال معلوماته الشخصية كاسم المستخدم و كلمة السر معتقداً بأنه يدخل للموقع التقليدي للمصرف أو يرسل معلومات عادية للدعم الفني للشركة التي يتعامل معها. و بالتالي يتم الحصول على معلوماته الشخصية. و يوضح الشكل 25 مثالاً على رسالة الكترونية تزعم بأن أحد المصارف يطلب تعديل معلومات المستخدم و ذلك لحمايته.



الشكل 25 مثال على الاحتيال باستخدام تقنية Phishing

5. استخدام تقنية حصان طروادة Trojan Horses: و هي مشابهة للتقنية السابقة مع فارق بأن استنتاج المعلومات يتم بشكل آلي بعد تسلل البرنامج إلى حاسب الهدف و إرسال المعلومات المخزنة عليه دون تدخل الهدف.

6. مواقع التواصل الاجتماعي: تشكل مواقع التواصل الاجتماعي مثل Facebook و Twitter و غيرها خطراً كبيراً من ناحية المعلومات التي يضعها المتواصلون على الصفحات المختلفة و التي قد تكون صفحات مخصصة لتجميع معلومات يمكن استخدامها لمهاجمتهم. هذا عدا عن كون الموقع الشهير facebook يعتبر أحد مواقع التجسس و تجنيد العملاء للصالح الحكومة الأمريكية و الموساد الإسرائيلي، كما يمكن اعتبار كافة مواقع التواصل الاجتماعي و Skype و Wikileaks وغيرها وسائل تجسس تتبع لحكومات غربية و أجهزة استخبارات [Russia Today, 2011]. وكان جوليان اسانج مؤسس موقع ويكيليكس وصف شبكة الفيسبوك للتواصل الإجتماعي بأنها "أعظم وسيلة للتجسس في التاريخ". ويقول اسانج إن الفيسبوك تجمع تلقائيا المعلومات السرية المسجلة في مواقع مستخدمي الإنترنت ثم تنتقل تلك المعلومات الى الدوائر الأمنية في الولايات المتحدة. ومن جانبها اضطرت الفيسبوك على الاعتراف بواقع التعاون مع الدوائر الأمنية الأميركية، لكنها تنكر وقائع ممارسة التجسس.
7. مواقع تأمين العمل Job Sites: تدعي هذه المواقع بأنها تملك شواغر للعمل. و تطلب إملاء الاستمارات الخاصة بطالبي العمل و بالتالي يقوم الضحية بتقديم معلوماته الشخصية كالاسم و البلد و الشهادات و الخبرات و أرقام الهواتف و البريد الالكتروني و غيرها، مما يسهل تجميع المعلومات و استخدامها لاحقاً.

المرحلة الثانية و الثالثة: توطيد العلاقة و كسب الثقة Trust و استغلالها

بعد أن تم جمع المعلومات الكافية حول الهدف – الضحية– من خلال المرحلة الأولى, و انتقاء الشخص الذي يعتقد المهاجم بأنه مناسب لاستدراج معلومات إضافية تفيد لاحقاً في الهجوم. يتم في المرحلة الثانية الاتصال به لتأمين المعلومات غير المتوفرة من المرحلة الأولى و اكتساب ثقة الضحية. و يمكن أن يستخدم المهاجم الطرق التالية [Jones, 2004]:

1. الاتصال الهاتفي: يعتبر الاتصال الهاتفي المباشر بالضحية من أهم الوسائل للحصول على المعلومات. كالاتصال بالدعم الفني أو المبيعات لمؤسسة ما. و يستخدم المهاجم معلومات حصل عليها في المرحلة الأولى كأسماء بعض المدراء و الادعاء بمعرفتهم و حاجته لبعض المعلومات. و يستغل المهاجم بعض الصفات الإنسانية و منها:
   - الرغبة في المساعدة: من الطبع البشري حب المساعدة و تقديم العون، عدا عن أن المهمة الأساسية للدعم الفني في المؤسسات هي تقديم المساعدة.

- كسب زبون جديد وتحقيق أرباح للمؤسسة: من مهمة قسم المبيعات الترويج للمنتجات و اكتساب زبائن جدد للمؤسسة التي يعمل بها فلا يمانع الضحية من إعطاء بعض المعلومات الخاصة التي تعزز رغبة الزبون المفترض – المهاجم– بالتعامل مع مؤسسته. و من هذه المعلومات التجهيزات الموجودة في المؤسسة و أنواعها و حجومها و الخدمات و بعض أهم الزبائن و الميزات غير المتوفرة علانية.
- التجاوب للإطراء و المديح: يميل البشر للتجاوب مع الأشخاص اللطفاء و التعاون معهم و بخاصة عند الإطراء عليهم. فيقدمون المساعدة و المعلومات المطلوبة بسهولة ويسر.
- الجنس اللطيف: من المعروف أن الرجال و خاصة الشرقيين يتعاملون بلُطف و تجاوب كبير مع الجنس اللطيف، ولذلك تَستخدم معظم المؤسسات فتيات جميلات للترويج لمنتجاتهم. و بالتالي يمكن استخدام ذلك لاستدراج العاملين و بخاصة المدراء لإعطاء معلومات خاصة بالعمل و سرية. و مثال على ذلك يمكن لمندوبة شركة تجهيزات حاسوبية أو شبكية –المهاجم– استدراج مدير المعلوماتية في مؤسسة ما لإعطائها معلومات عن بنية الشبكة و Real IPs المستخدمة و تجهيزات الحماية المتوفرة و ذلك لإثبات كفاءة المدير و انجازاته و قدرة مؤسسته.
- الخوف: يعتبر الخوف أيضاً من العوامل الهامة لتقديم المعلومات و هو معاكس للحالة السابقة. فإدعاء المهاجم بكونه شخصاً مهماً و خطيراً يمكن أن يسهل حصوله على المعلومات. و تسمى هذه التقنية الهندسة الاجتماعية المعاكسة Reverse Social Engineering. و كمثال عليها نذكر الاتصال الهاتفي الذي تم من قبل أحد المخربين من خارج سورية بمكتب القرآن الكريم في وزارة الأوقاف السورية مدعياً بأنه ضابط كبير و يريد رقم الهاتف الشخصي للسيد مفتي الجمهورية العربية السورية و يُرهبه باعتقاله اذا لم يتجاوب [لطف، 2011].
- الانتقام: تقوم الكثير من المؤسسات بالتخلي عن بعض كوادرها لأسباب مختلفة، منها التطوير و منها أسباب شخصية أو تغير الإدارة و بالتالي يجد الكثير من العاملين أنفسهم خارج المؤسسة و يعتقد الكثير منهم بأنه تعرض لظلم و إجحاف بحقه و قدراته و لا يمانع إعطاء معلومات تضر بمؤسسته السابقة بدافع الانتقام. أو يقوم هو شخصياً بمهاجمة المؤسسة مستغلاً معلوماته و خبرته. وهذا خطير جداً في حال كان الموظف السابق مهندس معلوماتية أو مدير نظام أو مدير معلوماتية أو حتى مدير أي قطاع أو قسم مهم في المؤسسة.
- اللامبلاة و الإهمال و حب الظهور: يتمتع البعض بخاصية اللامبلاة و الإهمال للمعلومات التي يقدمونها كما يتمتع آخرون بخاصية حب الظهور و تقديم اثباتات –على شكل معلومات موثوقة–

على أهميتهم و مكانتهم في أعمالهم. مما يسمح للمهاجم باستدراجهم للحصول على معلومات هامة.

و يمكن للمهاجم الاتصال بالضحية و الادعاء بأنه من قسم المعلوماتية أو الدعم الفني في نفس المؤسسة، و بأن الضحية لديه مشكلة في حسابه أو أن الضحية قام بعملية خاطئة مؤخراً و يريد مساعدته. كأن يتصل المهاجم بأحد العاملين في قسم البوالص في أحد المصارف و يدعي بأنه من المؤسسة نفسها و بأن الضحية قام بإدخال خاطئ لإحدى البوالص و يستدرج منه بعض المعلومات.

2. زيارة مواقع المؤسسة: يمكن للمهاجم زيارة مواقع المؤسسة و الادعاء بأنه زبون محتمل أو مندوب شركة ما أو غير ذلك للدخول إلى المؤسسة و من ثم جمع معلومات من خلال:
   - كلمات السر: يقوم الكثير من المستخدمين بوضع كلمة السر الخاصة به و اسم المستخدم على ورقة صغيرة بالقرب منه أو على شاشة الحاسب حتى يتذكرها.
   - الأوراق و الحاجيات –كالخلوي وغيرها–الموجودة على سطح المكتب، و التي يمكن أن تحوي معلومات هامة. فيقوم المهاجم بسرقتها أو نقل معلومات منها.
   - بعض الأجهزة الحاسوبية المتروكة: يميل معظم العاملين إلى تشغيل حواسيبهم منذ دخولهم إلى مكاتبهم و إغلاقها قبل ذهابهم مباشرة بعد انتهاء ساعات العمل. مما يتيح الفرصة للمهاجم السريع و الماهر بالحصول على معلومات من الحاسب مباشرة، أو تنصيب برنامج خطر على الحاسب، ليقوم بالاتصال به لاحقاً.
   - سلال المهملات في مقرات العمل: يميل معظم العاملين و المدراء إلى إلقاء وثائق هامة في سلال المهملات.
   - وسائل النسخ الاحتياطي: يقوم المهندسون و العاملون في أقسام المعلوماتية بأخذ نسخ احتياطية لمخدمات المؤسسة و قواعد البيانات على أدوات مثل Backup Tapes, CDs, DVDs, و غيرها، ويمكن بزيارة أقسام المعلوماتية رؤية هذه الأدوات موضوعة في أماكن غير محمية كمكتب مدير المعلوماتية أو أمن المعلومات، مما يسهل للمهاجم سرقتها.
3. البريد الالكتروني E-mail: يمكن للمهاجم إرسال رسالة الكترونية للضحية يدعي فيها بأنه شخص موثوق و يطلب بعض المعلومات أو يقدم برامج للضحية.
4. المحادثات الالكترونية Chat: يمكن من خلال غرف المحادثات الالكترونية تشجيع الضحية على تقديم معلومات بعد كسب ثقته أو تنزيل برامج ضارة إلى حاسبه و التي تبدو مفيدة. و يمكن في

البداية أن يقدم المهاجم برامج جيدة و غير ضارة و التي يقدمها مجاناً مع أنه دفع ثمنها و يقدمها بحكم الصداقة. ثم وفي مرحلة لاحقة يستغل الثقة و يرسل برامج ضارة.

المرحلة الرابعة: استخدام المعلومات و الهجوم

بعد أن تم تجميع المعلومات الأساسية أو تنصيب برامج ضارة على أجهزة الهدف لإرسال هذه المعلومات ينتقل المهاجم للمرحلة الأخيرة و هي استخدام هذه المعلومات و الهجوم. و من ذلك:

- أن يستغل المهاجم الحساب المصرفي للضحية و سحب أموال.
- أو مهاجمة مخدمات المؤسسة/موقعها الالكتروني و إيقافها عن العمل Denial of Service.
- ابتزاز الأشخاص أو المؤسسات بالمعلومات التي لديه.
- بيع هذه المعلومات للمنافسين أو الأعداء.
- استغلال هذه المعلومات من قبل الدول أو أجهزة الاستخبارات و التجسس لتجنيد عملاء أو تحضير مؤامرات و بث الشائعات و الأكاذيب مستفيدة من المعلومات الصحيحة التي حصلت عليها و غير ذلك.

6.5.1 الخطر الداخلي Insiders Threats

افترضنا في المقاربة السابقة بأن الضحية لا يعلم أنه يقدم معلومات خطيرة قد تلحق الضرر به أو بالمؤسسة التي يعمل بها. و لا بد أن نذكر الحالة التي يكون فيها المهاجم من الداخل أي عامل حالي أو سابق ضمن المؤسسة. و قد ذكرت الإحصائيات [Christopher, 2011] بأن الخسائر المادية للاختراقات في الولايات المتحدة قد تصل بين مليون إلى 53 مليون دولار للاختراق الواحد للمؤسسات الكبرى و المتوسطة. و ذكرت الإحصائيات بأن 90% من هذه الاختراقات تسبب بها الدخول عبر الانترنت أو استخدام برامج ضارة أو المستخدمين الداخليين في المؤسسة و بأن الخطر من المستخدمين الداخليين يحتل المرتبة الأولى بين الأنواع الثلاثة المذكورة. لأن المستخدمين الداخلين يستطيعون النفاذ بحكم عملهم إلى الأنظمة و البرامج و يعرفون نقاط الضعف فيها.

7.5.1 الخلاصة

تتمحور جميع المهام حول الإنسان و هو نقطة الضعف و القوة في أية منظومة. و تعتبر الهندسة الاجتماعية من أكثر الطرق فعاليةً و أقلها تكلفةً للحصول على المعلومات و استخدام هذه المعلومات

للهجوم على المؤسسات و الأفراد و استغلالهم و التسبب بالضرر و الخسائر و استخدامها لأغراض أخرى غير نزيهة. و قد اعتبر التدريب و التوعية المناعة الأساسية ضد الهندسة الاجتماعية.

6.1 أوراق البحث المنشورة في مجال اختبار و تقييم نماذج أمن المعلومات

في إطار البحث لتصميم نموذج جديد لأمن المعلومات و الشبكات، تمت دراسة عدة أوراق بحث نشرت في مجال تقييم و اختبار نماذج أمن المعلومات و قد أوردنا في الفقرات السابقة بعض المعايير العالمية و المطبوعات من منظمات عالمية معروفة في هذا المجال. و هنا سنورد بعض أوراق البحث التي تطرقت لهذا الموضوع بالإضافة لطرق القياس الكمي لأمن المعلومات و نتائج دراستها.

1.6.1 دليل العمل التقني لاختبار و تقييم أمن المعلومات للباحث Karen Scarfone

نشرت هذه الورقة برعاية المعهد الوطني للمعايير و التقانة في الولايات المتحدة في العام 2008 تحت الرقم SP800-115.

تتلخص هذه الورقة [Scarfone, 2008] بمجموعة توصيات عملية لتصميم و تنفيذ و مراجعة معلومات تقنية متعلقة بالاختبار و تقييم لإجراءات و عمليات تستخدم لأغراض معينة مثل إيجاد نقاط الضعف في الأنظمة أو الشبكات و التحقق من التطابق مع السياسات الأمنية و متطلبات العمل.

1.1.6.1 تقنيات المراجعة Review Techniques

تتضمن تحليل الواقع في المجالات التالية:

- مراجعة الوثائق: لتحديد نقاط الضعف فيها و النواقص في الوثائق التقنية المتوفرة لدى المؤسسة و التي تشرح الأنظمة المستخدمة و عملها و الإجراءات الأمنية الخاصة بها.
- مراجعة ملفات التدقيق Log Review: التحقق من أن ملفات التدقيق للأنظمة المستخدمة – مثل Event Viewer for Windows Operating Systems– تتضمن المعلومات الضرورية لتقييم العمل و المخاطر على هذه الأنظمة.
- مراجعة الأدوار Ruleset Review: و هي مجموعة النماذج الملتقطة على الشبكة أو خدمات الأنظمة و مقارنتها مع الإجراءات الواجب اتخاذها. و من ذلك تحديد إعدادات جدار الحماية الناري Firewall و نظام كشف الاختراق Intrusion Detection System IDS.

- مراجعة إعدادات الأنظمة: و يقصد بها أنظمة التشغيل المستخدمة مثل Windows و Linux و Unix و غيرها. و توقيف الخدمات غير المستخدمة و التي تعتبر نقاط ضعف تستخدم لاختراق النظام.
- التقاط بيانات الشبكة Network Sniffing: و التي تستخدم لتحديد الأجهزة الموجودة على الشبكة و البروتوكولات المستخدمة و أنظمة التشغيل العاملة و تحديد كلمات السر غير المشفرة.
- التحقق من سلامة الملفات File Integrity Checking: و التي توفر حماية للملفات المتبادلة على الشبكة عن طريق تقنيات التشفير.

يوضح الجدول5 ملخص للمراجعات التقنية.

Technique	Capabilities
Documentation Review	• Evaluates policies and procedures for technical accuracy and completeness
Log Review	• Provides historical information on system use, configuration, and modification • Could reveal potential problems and policy deviations
Ruleset Review	• Reveals holes in ruleset-based security controls
System Configuration Review	• Evaluates the strength of system configuration • Validates that systems are configured in accordance with hardening policy
Network Sniffing	• Monitors network traffic on the local segment to capture information such as active systems, operating systems, communication protocols, services, and applications • Verifies encryption of communications
File Integrity Checking	• Identifies changes to important files; can also identify certain forms of unwanted files, such as well-known attacker tools

جدول 5 ملخص للمراجعات التقنية

و تضمنت الورقة شروحات للمواضيع التالية:

2.1.6.1 تقنيات التحديد و التحليل

و تتضمن استكشاف الشبكة و تحديد البوابات Ports و الخدمات المستخدمة على الشبكة و تحديد نقاط الضعف في الشبكة و يوضح الجدول 6 ملخصاً لذلك.

Technique	Capabilities
Network Discovery	• Discovers active devices • Identifies communication paths and facilitates determination of network architectures
Network Port and Service Identification	• Discovers active devices • Discovers open ports and associated services/ applications
Vulnerability Scanning	• Identifies hosts and open ports • Identifies known vulnerabilities (note: has high false positive rates) • Often provides advice on mitigating discovered vulnerabilities
Wireless Scanning	• Identifies unauthorized wireless devices within range of the scanners • Discovers wireless signals outside of an organization's perimeter • Detects potential backdoors and other security violations

جدول 6 تقنيات التحليل و التعريف

3.1.6.1 تقنيات اكتشاف نقاط الضعف

و تتضمن محاولة اكتشاف كلمات السر للمستخدمين و إجراء إختبارات الإختراق Penetration Testing و الهندسة الإجتماعية. كما هو موضح بالجدول 7.

Technique	Capabilities
Password Cracking	• Identifies weak passwords and password policies
Penetration Testing	• Tests security using the same methodologies and tools that attackers employ • Verifies vulnerabilities • Demonstrates how vulnerabilities can be exploited iteratively to gain greater access
Social Engineering	• Allows testing of both procedures and the human element (user awareness)

جدول 7 تقنيات اكتشاف نقاط الضعف

تساهم هذه الورقة بتحديد نقاط عملية لتقييم متحكمات أمن المعلومات. و لم تحدد قيم كمية أو أولويات للقياس.

2.6.1 إطار عمل كمية لتقييم مكونات الأمن في الأنظمة المعلوماتية الموزعة

نشرت هذه الورقة في عام 2004 للباحثين Andres Bond & Nils Pahlson العاملين في معهد التقانة بجامعة لينكوبنكس في السويد [Bond, 2004].

تهدف هذه الورقة لايجاد طريقة لتقييم مستوى أمن المعلومات لمكونات الأنظمة المعلوماتية الموزعة. و للوصول لذلك يجب الاجابة على الأسئلة التالية:

- كيف يمكن قياس الأمن كمياً؟. في البداية يجب أن نحدد ماذا نقيس، و بالتالي يجب تحديد خصائص النظام المدروس.
- هل يمكن تحسين أُطر العمل المتوفرة للقياس الكمي؟. تطبيق أُطر العمل الموجودة لتحديد نقاط القوة و الضعف فيها.
- هل يمكن تطوير مقياس فعال لأمن المعلومات؟. و ذلك لمكونات النظام و خصائصه.
- كيف يمكن التحقق من صحة القياس المقترح؟. و هذا يتحقق بالدقة و تطبيق القياس و مراقبة النتائج.

1.2.6.1 الأبحاث السابقة

من أهم الأبحاث المنشورة و التي اعتمد عليها Bond، ورقة البحث التي نشرها Richard Andresson [Andersson, 2003].

اعتمد Andresson على Common Criteria CC [Board, 1999]، كأساس لتقييم أمن مكونات الأنظمة المعلوماتية و مقارنتها مع الثلاثية Confidentiality, Integrity and Availability CIA. و قد استخدم معادلة لاحتساب أمن جزء محدد من نظام المعلومات المدروس:

$$SV = \frac{SV_1 + SV_2 + \ldots + SV_n}{n}$$

حيث تمثل Security Value SV القيمة الرقمية لعناصر المكون المدروس و هي هنا n عنصر. و تقيم كل SV بقيمة في المجال [0,1]. أما المكونات التي اعتمدها الباحث مع اختصاراتها فقد شملت:

- المراجعة الأمنية Security Audit FAU.
- الاتصالات Communication FCO.
- دعم التشفير Cryptographic Support FCS.
- حماية بيانات المستخدم User Data Protection FDP.
- التعريف و الأصالة Identification and Authentication FIA.
- إدارة الأمن Security Management FMT.
- الخصوصية Privacy FPR.
- استخدام الموارد Resource Utilization FRU.
- القنوات الموثوقة Trusted Path/Channel FTP.

2.2.6.1 تطبيق المعادلة على نظام التشغيل Windows 2000 server SP3

كانت نتائج التطبيق في مجال المراجعة الأمنية Security Audit FAU، كما يلي في الجدول 8. و الذي فصل عناصر مجال المراجعة الأمنية المدروسة.

ID	Descriptive Name	P_1P_2T	CIA	SV	C	I	A
FAU	Security audit			0,34	0,32	0,33	0,30
FAU_ARP	Security audit automatic response	P_2	CIA	0,00	0,00	0,00	0,00
FAU_GEN	Security audit data generation	P_1P_2T	CIA	0,85	0,85	0,85	0,85
FAU_GEN.1	Audit data generation	P_1P_2T	CIA	0,80	0,80	0,80	0,80
FAU_GEN.2	User identity association	P_1P_2T	CIA	0,90	0,90	0,90	0,90
FAU_SAA	Security audit analysis	P_2	CIA	0,00	0,00	0,00	0,00
FAU_SAA.1	Potential violation analysis	P_2	CIA	0,00	0,00	0,00	0,00
FAU_SAA.2	Profile based anomaly detection	-	CIA	NULL	NULL	NULL	NULL
FAU_SAA.3*	Attack heuristics	-	CIA	NULL	NULL	NULL	NULL
FAU_SAR	Security audit review	P_1P_2T	CIA	0,77	0,77	0,70	0,70
FAU_SAR.1	Audit review	P_1P_2T	CIA	0,70	0,70	0,70	0,70
FAU_SAR.2	Restricted audit review	P_1P_2T	C	0,90	0,90	-	-
FAU_SAR.3	Selectable audit review	P_1P_2T	CIA	0,70	0,70	0,70	0,70
FAU_SEL	Security audit event selection	P_1P_2	CIA	0,00	0,00	0,00	0,00
FAU_STG	Security audit event storage	P_1P_2T	IA	0,40	-	0,6	0,40
FAU_STG.1	Protected audit trail storage	P_1P_2T	IA	0,60	-	0,60	0,60
FAU_STG(2)	Guarantees of audit trail storage	P_1	A	0,00	-	-	0,00
FAU_STG.3*	Prevention of audit data loss	P_1P_2T	A	0,60	-	-	0,60

جدول 8 تطبيق معادلة Andresson في مجال المراجعة الأمنية Security Audit

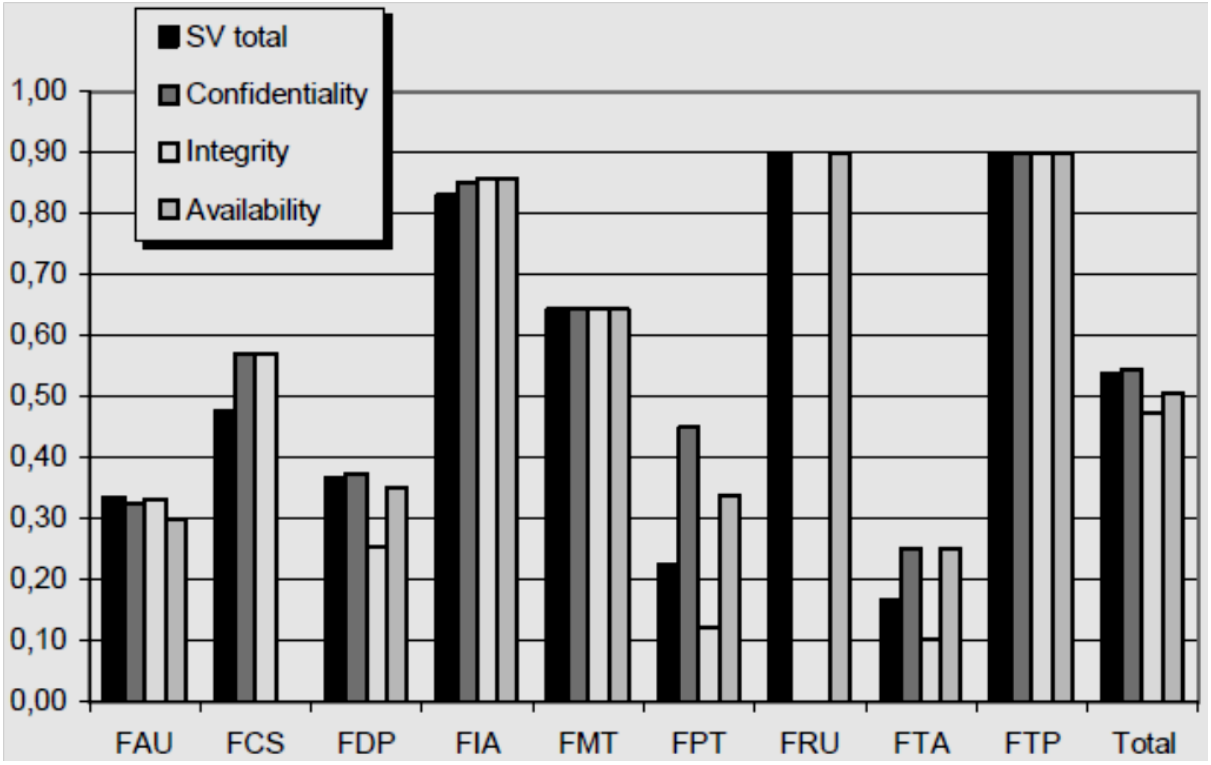
حيث تمثل الاختصارات:

C: Confidentiality السرية.

I: Integrity السلامة.

A: Authenticity الأصالة.

كما يوضح المخطط (الشكل 26) ملخصاً للجدول السابق.



الشكل 26 ملخص تطبيق معادلة Andersson في مجال المراجعة الأمنية

و يلخص الجدول 9 نتائج التطبيق على كافة المجالات لنظام التشغيل Windows 2000.

ID	Descriptive Name	SV	C	I	A
FAU	Security audit	0,34	0,32	0,33	0,30
FCO	Communication	NULL	-	NULL	-
FCS	Cryptographic Support	0,48	0,57	0,57	0,00
FDP	User Data Protection	0,37	0,37	0,25	0,35
FIA	Identification and Authentication	0,83	0,85	0,86	0,86
FMT	Security Management	0,64	0,64	0,64	0,64
FPR	Privacy	NULL	NULL	NULL	NULL
FPT	Protection of TOE Security Functions	0,23	0,45	0,12	0,34
FRU	Resource Utilisation	0,90	-	NULL	0,90
FTA	TOE Access	0,17	0,25	0,10	0,25
FTP	Trusted Path/Channels	0,90	0,90	0,90	0,90

جدول 9 نتائج التطبيق على كافة المجالات لنظام التشغيل Windows 2000

3.2.6.1 نقاط القوة في معادلة Andresson

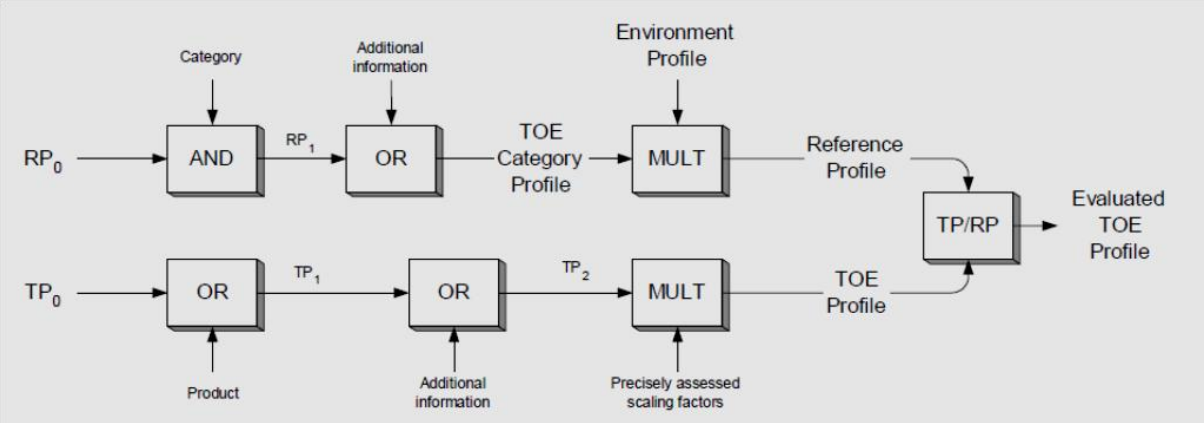
تعتبر قوة المعادلة باعتماد Common Criteria CC، وهي آلية جيدة لبعض القياسات الخاصة بأنظمة التشغيل.

4.2.6.1 نقاط الضعف في معادلة Andresson

وجد Bond أن المعادلة المقترحة و مكونات النظام لم تأخذ بعين الاعتبار البيئة المحيطة بأنظمة التشغيل، و التي تؤثر بشكل مباشر على أمن أنظمة التشغيل. النقطة الثانية أن نتائج المعادلة تسمح بمقارنة عدة أنظمة تشغيل مع بعضها في خصائص معينة و يمكن بالتالي الحكم بأن نظام تشغيل معين هو أفضل من نظام آخر، و لكن لا تعطي فكرة هل هذا النظام آمن ؟ و ما هي درجة أمانه ؟.

5.2.6.1 إطار العمل المقترح من قبل Bond

اقترح Bond إطار عمل لتقييم المستوى الأمني لخصائص منتج أمني معين. يتلخص هذا الإطار بالشكل 27.



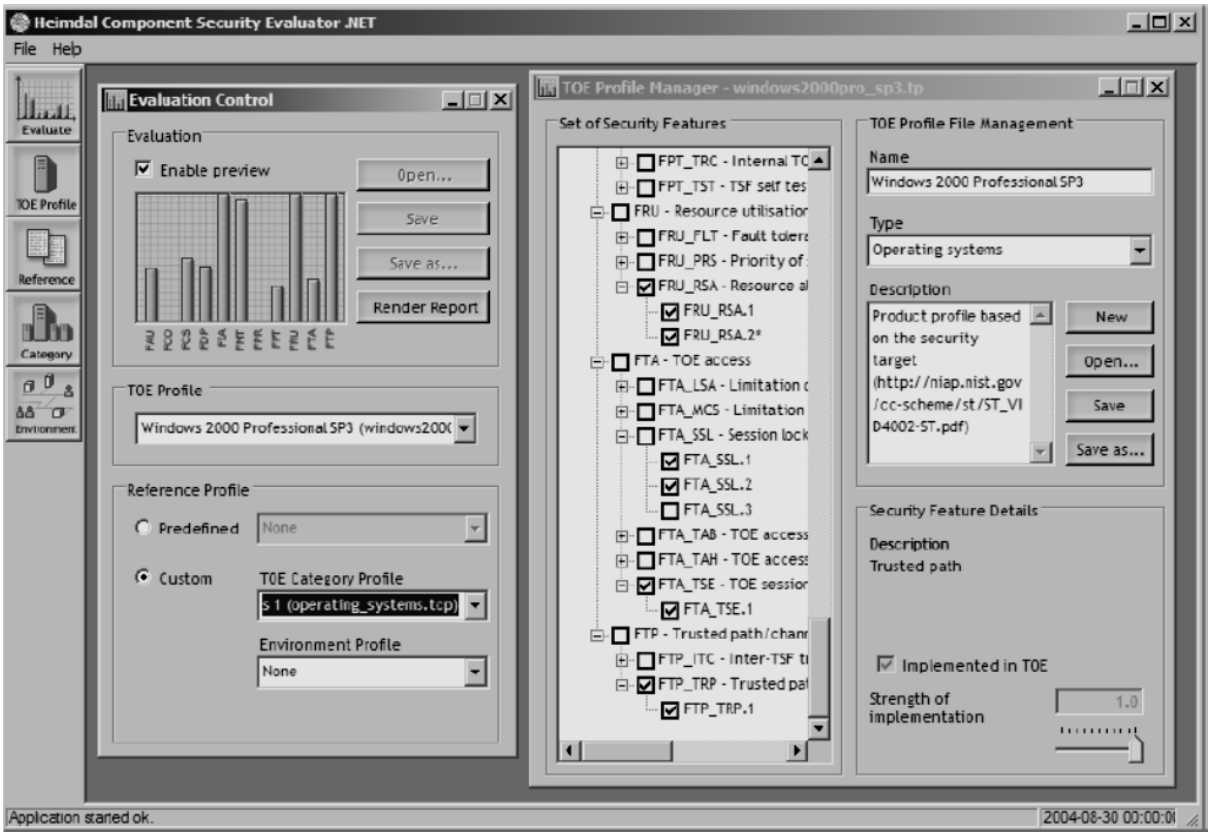
الشكل 27 إطار عمل Bond

حيث اعتبر المُنتَج قيد الدراسة Target of Evaluation (TOE)، و الخصائص الأمنية لهذا المُنتَج TOE Profile (TP)، و حالة البيئة المحيطة Environmental Profile (EP)، و الحالة المرجعية Reference Profile (RP)، و بعد إدخال المعلومات يتم أخيراً مقارنة كمية بين TOE Profile مع Reference Profile لإنتاج الخرج النهائي و سماه Evaluated TOE Profile.

و يمكن للقيم المدخلة للقياس أن تكون من المجال [0,1]. كما يكون الخرج لكل خاصة مقاسة من نفس المجال.

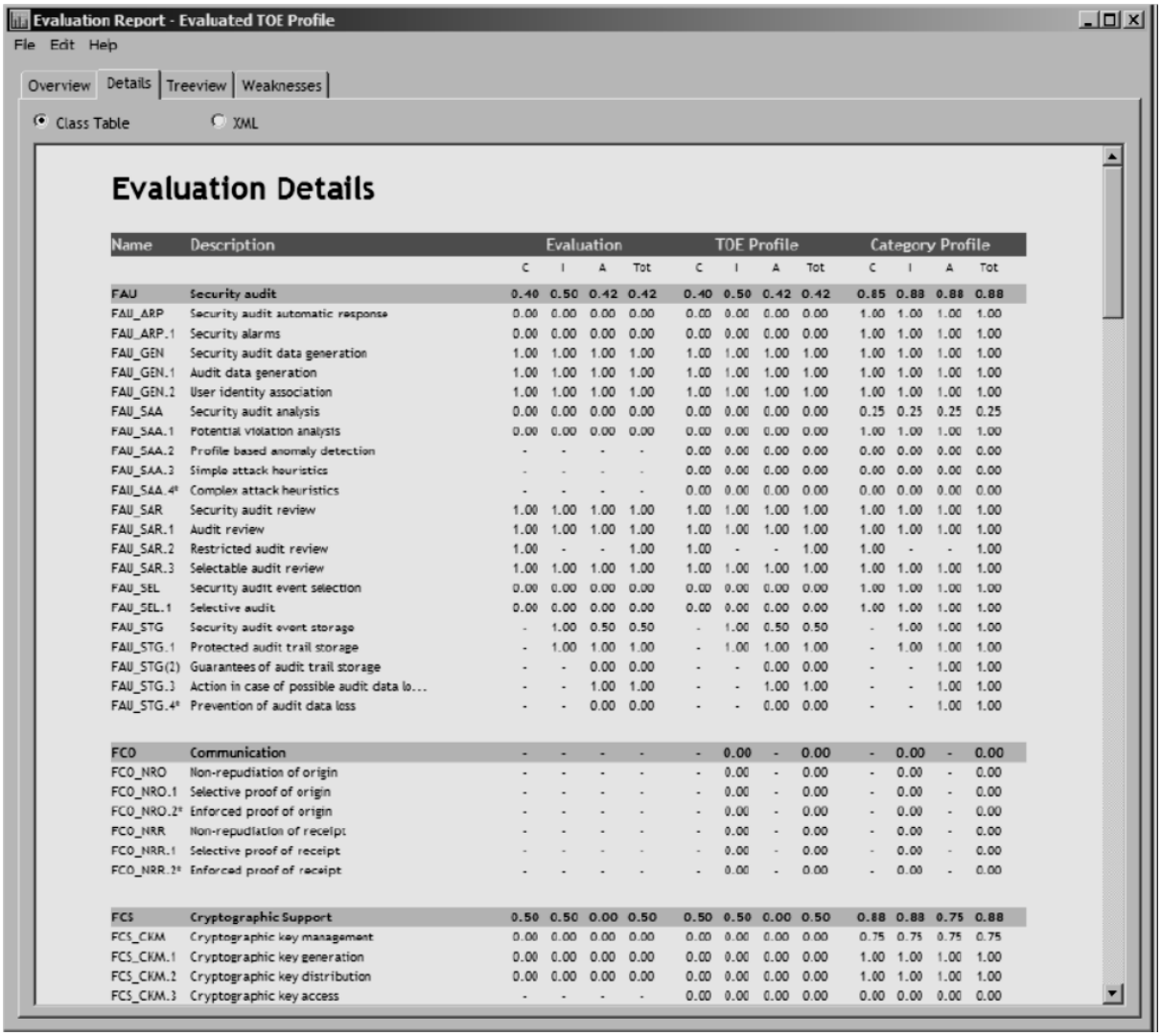
6.2.6.1 التطبيق العملي لإطار العمل المقترح من قبل Bond

قام الباحث بتطوير برنامج خاص لتطبيق إطار العمل المقترح سماه Heimdal Security Evaluator 3000 .NET. و يوضح الشكل 28 الواجهة الرئيسية للبرنامج عند تطبيقه على نظام التشغيل Windows 2000.



الشكل 28 تطبيق إطار عمل Bond على Windows 2000

كما يوضح الشكل 29 التقرير نتائج تطبيق البرنامج.



Name	Description	Evaluation				TOE Profile				Category Profile			
		C	I	A	Tot	C	I	A	Tot	C	I	A	Tot
FAU	**Security audit**	**0.40**	**0.50**	**0.42**	**0.42**	**0.40**	**0.50**	**0.42**	**0.42**	**0.85**	**0.88**	**0.88**	**0.88**
FAU_ARP	Security audit automatic response	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	1.00	1.00	1.00	1.00
FAU_ARP.1	Security alarms	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	1.00	1.00	1.00	1.00
FAU_GEN	Security audit data generation	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00
FAU_GEN.1	Audit data generation	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00
FAU_GEN.2	User identity association	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00
FAU_SAA	Security audit analysis	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.25	0.25	0.25	0.25
FAU_SAA.1	Potential violation analysis	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	1.00	1.00	1.00	1.00
FAU_SAA.2	Profile based anomaly detection	-	-	-	-	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
FAU_SAA.3	Simple attack heuristics	-	-	-	-	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
FAU_SAA.4[a]	Complex attack heuristics	-	-	-	-	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
FAU_SAR	Security audit review	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00
FAU_SAR.1	Audit review	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00
FAU_SAR.2	Restricted audit review	1.00	-	-	1.00	1.00	-	-	1.00	1.00	-	-	1.00
FAU_SAR.3	Selectable audit review	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00
FAU_SEL	Security audit event selection	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	1.00	1.00	1.00	1.00
FAU_SEL.1	Selective audit	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	1.00	1.00	1.00	1.00
FAU_STG	Security audit event storage	-	1.00	0.50	0.50	-	1.00	0.50	0.50	-	1.00	1.00	1.00
FAU_STG.1	Protected audit trail storage	-	1.00	1.00	1.00	-	1.00	1.00	1.00	-	1.00	1.00	1.00
FAU_STG(2)	Guarantees of audit trail storage	-	-	0.00	0.00	-	-	0.00	0.00	-	-	1.00	1.00
FAU_STG.3	Action in case of possible audit data lo...	-	-	1.00	1.00	-	-	1.00	1.00	-	-	1.00	1.00
FAU_STG.4[a]	Prevention of audit data loss	-	-	0.00	0.00	-	-	0.00	0.00	-	-	1.00	1.00
FCO	**Communication**	-	-	-	-	-	**0.00**	-	**0.00**	-	**0.00**	-	**0.00**
FCO_NRO	Non-repudiation of origin	-	-	-	-	-	0.00	-	0.00	-	0.00	-	0.00
FCO_NRO.1	Selective proof of origin	-	-	-	-	-	0.00	-	0.00	-	0.00	-	0.00
FCO_NRO.2[a]	Enforced proof of origin	-	-	-	-	-	0.00	-	0.00	-	0.00	-	0.00
FCO_NRR	Non-repudiation of receipt	-	-	-	-	-	0.00	-	0.00	-	0.00	-	0.00
FCO_NRR.1	Selective proof of receipt	-	-	-	-	-	0.00	-	0.00	-	0.00	-	0.00
FCO_NRR.2[a]	Enforced proof of receipt	-	-	-	-	-	0.00	-	0.00	-	0.00	-	0.00
FCS	**Cryptographic Support**	**0.50**	**0.50**	**0.00**	**0.50**	**0.50**	**0.50**	**0.00**	**0.50**	**0.88**	**0.88**	**0.75**	**0.88**
FCS_CKM	Cryptographic key management	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.75	0.75	0.75	0.75
FCS_CKM.1	Cryptographic key generation	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	1.00	1.00	1.00	1.00
FCS_CKM.2	Cryptographic key distribution	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	1.00	1.00	1.00	1.00
FCS_CKM.3	Cryptographic key access	-	-	-	-	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00

الشكل 29 تقرير التقييم الناتج عن تطبيق برنامج Bond على Windows 2000

7.2.6.1 الفوائد المستقاة من ورقة البحث السابقة

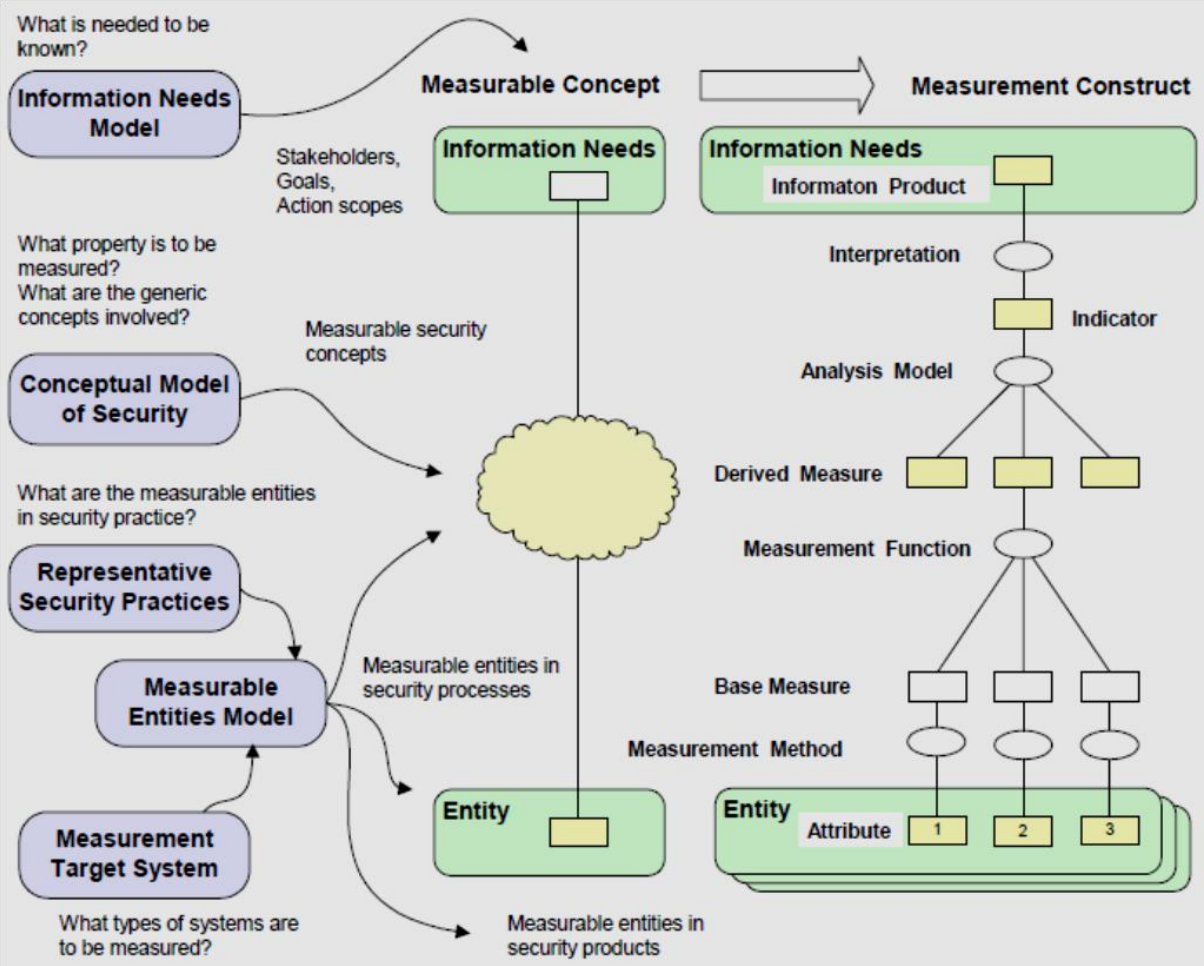
قدمت ورقة البحث السابقة آلية جديدة و فعالة لقياس مستوى أمن المعلومات كمياً. و عرفت بعض الخصائص الأمنية الواجب قياسها. و لكنها اقتصرت على أنظمة التشغيل الموزعة Distributed Operating Systems، و لم تشمل المؤسسات و الأنظمة المعلوماتية بشكل عام، كما لم تشمل الشبكات و قواعد البيانات و الأجهزة الأمنية كالجدار الناري و غيرها.

7.1 قياس أمن المعلومات

نشرت هذه الورقة Security Measurement في عام 2005 للباحث John Murdoch، العامل في قسم الدراسات الإدارية بجامعة يورك البريطانية [Murdoch, 2005].
اعتمد النموذج المقترح على النقاط التالية:

1. من هم الأشخاص الذين يتضمنهم المجال المدروس، و ما هي أدوارهم و مسؤولياتهم و أهدافهم في المؤسسة. مما يؤدي لتحديد متطلبات المعلومات Information Needs للمؤسسة بشكل عام.
2. ما هو المكون المدروس – المعد لقياس خصائصه الأمنية–، مثل برامج معلوماتية أو أصول Assets أو خدمات المؤسسة أو غيرها.
3. ما هو الأداء الأمني المطلوب. و الذي يكون كجسر بين متطلبات المؤسسة و متطلبات أمن المعلومات التقنية.
4. أخيراً Measurable Entity Model سيتم تطويره ، و الذي سيحدد القياس المطلوب.

يوضح المخطط (الشكل 30) آلية العمل المقترحة.



الشكل 30 استراتيجية العمل لقياس أمن المعلومات بحسب Murdoch

1.7.1 المكونات القابلة للقياس

اعتبرت ورقة البحث أن مفاهيم أمن المعلومات القابلة للقياس يمكن سردها في الجدول 10.

بنيت هذه المفاهيم على دراسة المخاطر المحيطة بالأنظمة و الشبكات العاملة في المؤسسة، بالإضافة إلى أهداف المؤسسة و أهداف أمن المعلومات.

Phase	Measurable Entity	Attributes	Notes
Context: Capability	Reference Process Model and Practices	Strengths and Weaknesses Practice Characterizations Goal Ratings PA ratings Capability Profiles	iCMM/ CMMI measures relating to the institutionalization of processes.
Start Up	Security Policy/ Plan	Security Process Definition Tasks Schedule Resources Work Products	Planning and deployment of security process assets on a particular project.
		Roles, responsibilities	Including independent security checks
		Staff Competencies Skills and Experience Matrix	
		Reporting Arrangements	
		Contractual Agreements	
		Dispute Resolution Provision	
Product Development; Pre-manufacture	Security Requirements / Objectives Log or database	Requirement Count Requirement Scope Requirement Source Status	Summary record of security requirements, including customer sourced, derived (developed by the security process) and requirements placed on suppliers
	Security Asset Log	Product Components Product Functions Product Modes Mission Phases Process Resources	
	Threat Tracking System	Threat Agent Count Threat Agent Status Threat Attack Tree Threat Risk	.
	Vulnerability Tracking System	Vulnerability Count Vulnerability Status Vulnerability Scope	
	Security Action/ Mitigation Log	Action Count Action Status	Summary record of all actions generated by the security process, including mitigations.

Post Manufacture: assembly, integration and test	Verification Test Log	Verification Count Verification Status Action Status Action Scope	Summary records of the tests and other data that demonstrate security requirements have been met.
	Acceptance Test Log	Validation Count Validation Status Action Status Action Scope	Summary record of the validation tests and other data that are agreed as acceptance criteria across customer/supplier interfaces.
Operations	Event Tracking System	Count Type/ severity Action Status Scope	Threat and vulnerability tracking systems remain to support operations
	Damage Tracking System	Count Type/ severity Action Status Scope	
	Security Policy Compliance	Check list Count Type Action Status	
Security Assurance	Security Assurance Case	% completion against planned argument structure	Replaced or augmented with Common Criteria approach, if applied.

جدول 10 Measuable Entity

2.7.1 آلية القياس المقترحة

اقترحت ورقة البحث ما اعتبرته دليل عمل لتطوير نظام قياس لأمن المعلومات يعتمد على مايلي:

- تحديد متطلبات أمن المعلومات. و منها المصادر و الأنظمة و العاملون في المؤسسة.
- تحديد المفاهيم و المكونات القابلة للقياس.
- تحديد المخاطر.
- تعريف مجالات أمن المعلومات المدروسة.
- تحديد مؤشرات لتخدم متطلبات أمن المعلومات، و تطوير نموذج خاص بذلك.
- تبني قياسات مناسبة للمخاطر و نقاط الضعف.
- اختبار القياسات المقترحة.

3.7.1 الفوائد المستقاة من ورقة البحث السابقة و النواقص

من الفوائد المستقاة من الورقة السابقة هي الآلية المقترحة لتطوير القياسات و تعريف مجالات أمن المعلومات و متطلبات القياس. أما فيما يخص البحث الذي نقوم به فلم نجد قياسات عملية –كمية– مقترحة لكامل أو لجزء من دليل العمل المقترح.

8.1 خلاصة الفصل الأول

تطرق الفصل الأول للدراسات المرجعية لمواضيع ذات علاقة مباشرة بالبحث:

- أمن المعلومات و الشبكات، حيث تم تعريف أساسيات أمن المعلومات كالسرية و الأصالة و عدم الانكار و السلامة و الإتاحية. كما تطرقنا إلى بنية الأمن في النموذج OSI/ISO.
- علم التعمية (التشفير)، حيث تم استعراض فضل العرب في هذا العلم، و عرض لنماذج التشفير المتناظرة و غير المتناظرة. كما تم شرح آلية عمل كل من خوارزميات التشفير DES، 3DES، AES، RSA.
- المعايير العالمية في أمن المعلومات و الشبكات، و بخاصة ISO27K series، CobiT 4.1 .
- المنشورات الخاصة بالمعهد الوطني للمعايير و التقانة National Institute of Standards and Technology، في الولايات المتحدة الأمريكية. و تضمنت دراسة الوثيقة SP800-53، و الوثيقة SP800-55. كما تم استعراض فوائد القياس الكمي لأمن المعلومات و آليات تطبيقه.
- الهندسة الاجتماعية Social Engineering: تم اعطاء أهمية خاصة للهندسة الاجتماعية و شرح دورة حياتها و ذلك لأهمية هذا الموضوع و حداثته.
- تتمحور جميع المهام حول الإنسان و هو نقطة الضعف و القوة في أية منظومة. و تعتبر الهندسة الاجتماعية من أكثر الطرق فعاليةً و أقلها تكلفةً للحصول على المعلومات و استخدام هذه المعلومات للهجوم على المؤسسات و الأفراد و استغلالهم و التسبب بالضرر و الخسائر و استخدامها لأغراض أخرى غير نزيهة. و قد اعتبر التدريب و التوعية المناعة الأساسية ضد الهندسة الاجتماعية.
- أوراق البحث المنشورة في مجال القياس الكمي لأمن المعلومات و تحليل نتائجها.

الفصل الثاني (الدراسات التحليلية و التصميمية)

1.2 مقدمة

يهدف هذا البحث بشكل عام إلى:

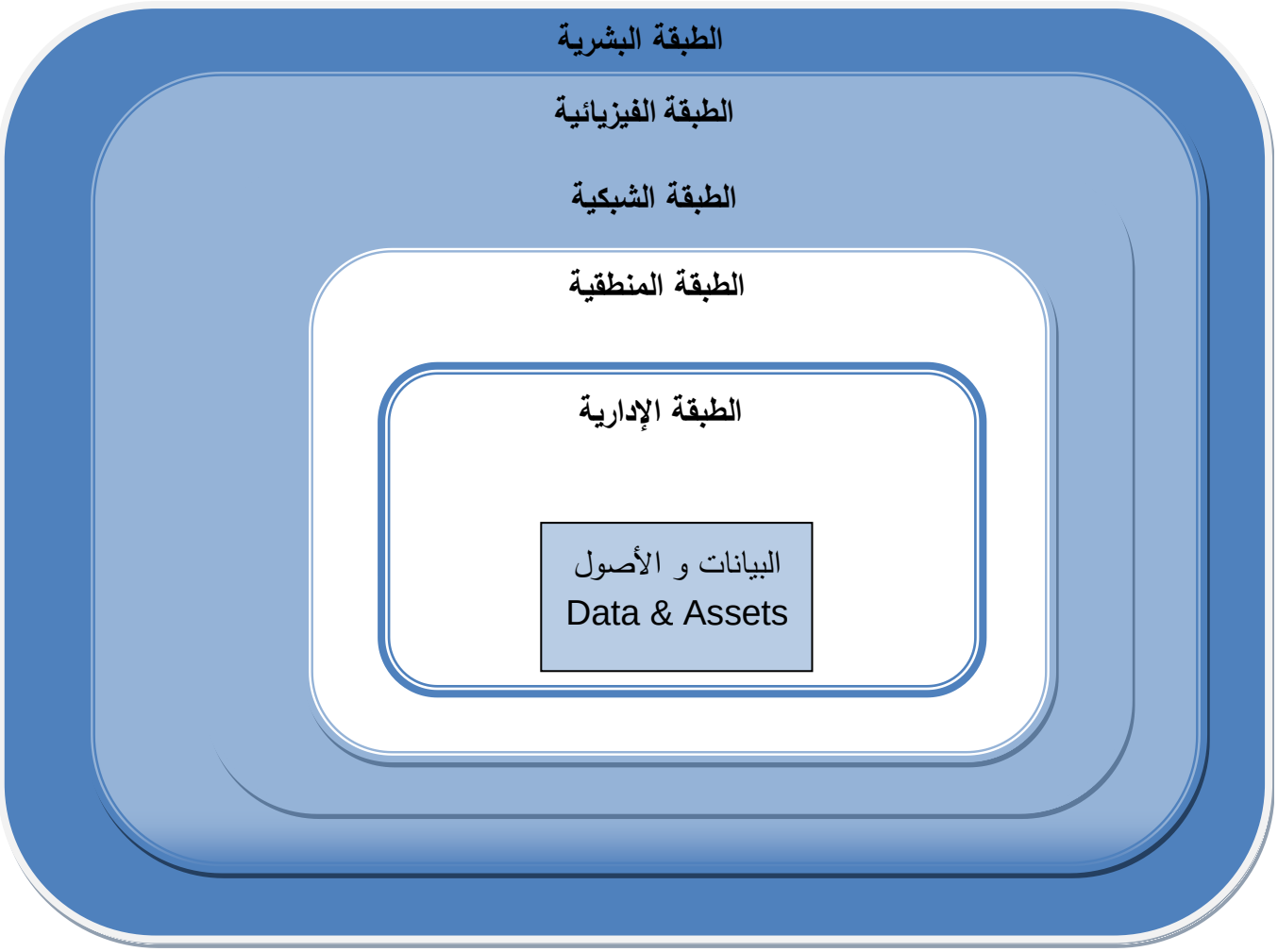
1. تصميم نموذج جديد لأمن المعلومات و الشبكات، و تحليله و التحقق من مطابقته للمعايير العالمية.
2. يتضمن النموذج المقترح الإجراءات الواجب اتخاذها لتقييم و تطوير المستوى الأمني للمؤسسة.
3. تطوير معادلة جديدة للقياس الكمي لكافة العوامل المؤثرة في أمن المعلومات للمؤسسات بكافة أنواعها. و ذلك بهدف تحديد مستوى أمان المؤسسة كمياً.
4. تطوير برنامج حاسوبي مؤتمت لإجراء القياس و تطبيق المعادلة المقترحة.
5. تطبيق المعادلة – البرنامج المطور– على إحدى المؤسسات للتحقق من فعاليته و مطابقته لأهداف البحث.
6. تحليل النتائج و التطوير المستقبلي.

و يتضمن هذا الفصل النموذج المقترح و مكوناته و دراسته من النواحي التحليلية و التصميمية.

2.2 النموذج المقترح

قدمنا في الفصل الأول (الدراسات المرجعية) المعايير العالمية في مجال أمن المعلومات و أهم أوراق البحث المنشورة المتعلقة في مجال أمن المعلومات.

و بعد دراسة معمقة للمعايير ISO 27000 Series و إطار العمل CobiT4.1 و أدلة العمل الصادرة عن NIST. يمكننا الآن عرض النموذج.



الشكل 31 النموذج المقترح

يحقق النموذج المقترح الشروط التالية:

1. نموذج طبقي يسمح بتوزيع المكونات و المتحكمات الأمنية Security Controls المستنتجة من المعايير العالمية و من أوراق البحث و المراجع ذات الصلة. بحيث تعكس كل طبقة المكونات ذات الطبيعة المتشابهة و تعريفها بشكل واضح لتحقيق المستوى الأمني المطلوب. بالإضافة إلى تضمين طبقة خاصة بالناحية البشرية و التي تحيط بكافة الطبقات الأخرى و تتضمن متحكمات المنع أو الحد من تأثير الهندسة الاجتماعية.
2. بدوره يحيط النموذج المقترح بالبيانات و الأصول Data & Assets والتي يهدف في النهاية إلى تأمين الحماية لها و تأمين العمل ضمن بيئة مستقرة و تقديم خدمات آمنة و سريعة.

3. تضمين كافة مجالات أمن المعلومات و مكوناتها و المتحكمات الأمنية في كل مجال من المعايير ISO 27001,ISO 27002.
4. متطلبات أمن المعلومات في الأصالة Authenticity و السرية Confidentiality و السلامة Integrity. وغيرها.
5. تحقيق المعايير الدولية في مجال أمن المعلومات و الشبكات و بخاصة:

a) ISO/IEC 27001.
b) ISO/IEC 27002.
c) ISO/IEC 13335-1:2004.
d) ISO/IEC TR 13335-3:2004.
e) ISO/IEC 15408-1:1999.
f) اعتماد إطار العمل NIST SP800-53 rev1:2008، كخطوات عملية لتطبيق السياسات الأمنية للمؤسسات الكبيرة و تقييمها.

و الذي يضمن فعالية النموذج المقترح و كفاءته للتطبيق و تحقيق الهدف منه.

6. أهداف المؤسسات في بيئة عمل مستقرة من الناحية الأمنية، بالإضافة إلى حماية بياناتها و أصولها.
7. قابلية قياس Measure كل عنصر من عناصر الطبقات.
8. إمكانية تطوير معادلة جديدة تتضمن كافة عناصر الطبقات المقترحة و تسمح بالقياس الكمي لمستوى أمن المعلومات في المؤسسة المدروسة.

3.2 طبقات النموذج المقترح و مكوناته و المتحكمات الأمنية في كل طبقة

تتضمن كل طبقة عدة مجالات أمنية و يحتوي كل مجال مجموعة من المتحكمات. و التي يمكن تعريفها كما يلي:

المجال Security Domain: و هو عنوان يتضمن مجموعة الأدوات ذات الطابع المتشابه و التي تحقق غاية محددة ضمن المجال المشترك.

المتحكمات Security Controls: و تكون تحت عنوان –مجال– واحد و تتضمن أدوات للتغلب على المخاطر. مثل السياسات و الإجراءات و التعليمات و غيرها.

أمن المعلومات: سنستخدم هذا المصطلح للدلالة على أمن المعلومات و الشبكات و مكافحة الهندسة الاجتماعية.

و بعد دراسة كافة المتحكمات، وجدنا أنها يمكن أن توزع كما يلي:

1. **الطبقة البشرية Human Layer**
   - السياسات الأمنية لمنع الهندسة الاجتماعية.
   - توزيع المهام التقنية Divide and Conquer.
   - برامج التوعية و التدريب (المناعة الذاتية).
   - الرقابة على العاملين و وسائل الاتصال بهم.
   - التفتيش المفاجئ.
   - الاختبارات.
2. **الطبقة الفيزيائية Physical Layer**
   - دخول الأفراد للمؤسسة بشكل عام و للأماكن المحظورة الخاصة بالتجهيزات الحاسوبية و الشبكية و تجهيزات أمن المعلومات.
   - تأمين التجهيزات الحاسوبية و الأمنية في أماكن محمية.
   - تأمين الأبنية و منشآت المؤسسة من الدخول غير المسموح و من الكوارث الطبيعية.
   - مراقبة أي محاولة للدخول غير المسموح.
   - تأمين البيئة المحيطة بالتجهيزات كدرجة الحرارة و الرطوبة و الغبار و غيرها. بالإضافة إلى استخدام أجهزة عدم انقطاع التيار الكهربائي UPS و مولدات الطاقة الاحتياطية.
3. **الطبقة الشبكية Network Layer**
   - البنية التحتية – الشبكات و أدواتها– بما فيها الإعدادات لهذه التجهيزات و خطوط الاتصال و الشبكات الداخلية.
   - التجهيزات الأمنية الشبكية و إعداداتها. مثل جدار الحماية Firewalls، و أجهزة منع/كشف الاختراق Intrusion Detection/Prevention Systems.
   - التشفير الشبكي أي استخدام أجهزة تشفير خاصة بالشبكات و تعمل على تشفير البيانات الداخلة و الخارجة للشبكة.
4. **الطبقة المنطقية Logical Layer**
   - السياسات الأمنية الخاصة بالنواحي التقنية للمنظومات الالكترونية. مثل آليات التحكم بالولوج للموارد – حواسيب أو برامج أو قواعد بيانات أو غيرها– Access Control Mechanisms.

- إدارة الموارد و كلمات السر.
- طرق التعريف و الأصالة Identification and Authentication Methods. و نعني بها ما يُستخدم تقنياً للدخول للموارد مثل اسم دخول و كلمة سر، أو بطاقة تعريف كبطاقة الصراف الآلي، أو بصمة دخول أو غيرها من طرق الدخول للموارد.
- البرامج الأمنية و إعداداتها. مثل برامج مضاد الفيروسات، و استخدام بروتوكولات التشفير في التطبيقات و المواقع الالكترونية مثل HTTPS.
- إدارة استمرارية العمل Business Continuity Management. بما فيها Disaster Recovery.

5. **الطبقة الإدارية Administrative Layer**

- السياسات الإدارية. سياسات إدارة المؤسسة فيما يخص أمن المعلومات.
- القوانين و الأنظمة.
- الإجراءات و دلائل العمل.
- إدارة المخاطر.
- أمن الموارد البشرية و قواعد التوظيف و التعاقد المؤقت و شروطه.
- التدريب و التأهيل المعلوماتي و خاصة التوعية من النواحي الأمنية.

1.3.2 الآلية المتبعة لتحديد المجالات و المتحكمات في كل مجال

بما أن جميع الأدوات و الإجراءات الأمنية وضعت بشكل عام لحماية و تأمين البيانات و الموارد من المخاطر الداخلية و الخارجية Risks. كان لابد من تبني آلية لتحديد المخاطر، و بالتالي تعريف المتحكم Security Control الذي يقابله و الذي يهدف إلى منع حدوث الخطر –إن أمكن– و معالجته في حال حصوله و التقليل من ضرره المحتمل. و في هذا الإطار سنسرد بعض المصطلحات المتعلقة بالمخاطر:

الأصول Assets: و هي موارد المؤسسة من أفراد و أنظمة معلوماتية و قواعد البيانات و بنية تحتية شبكية و الخدمات و المواقع الإلكترونية و غيره. و التي تمثل كل المكونات التي تستخدمها و تستثمرها المؤسسة، و التي تحتاج المؤسسة لحمايتها.

نقطة الضعف Vulnerability: و هي ضعف أو خطأ في البرامج أو الأجهزة أو الإجراءات مما يسمح للمهاجم بالدخول غير المشروع أو تخريب متعمد للمنظومة المعلوماتية أو لجزء منها. و كمثال

على نقاط الضعف أي خدمة Service متاحة و غير مستخدمة، أو بوابة Port مفتوحة و غير محمية بجدار حماية.

التهديد Threat: أي احتمال يتهدد الأنظمة المعلوماتية، و الذي ينشأ بسبب وجود نقاط ضعف. و مكون التهديد Threat Agent يستغل مثلاً البوابة المفتوحة للدخول للنظام و الحصول على معلومات غير مصرح له بها أو تخريب جزء أو كل النظام. من الممكن أن يكون مكون التهديد برنامج virus يتسلل للمنظومة.

الخطر Risk: هو احتمال أن يتمكن مكون التهديد من استغلال نقطة ضعف ما و التأثير المحتمل لذلك على النظام المخترق و على عمل المؤسسة بشكل عام.

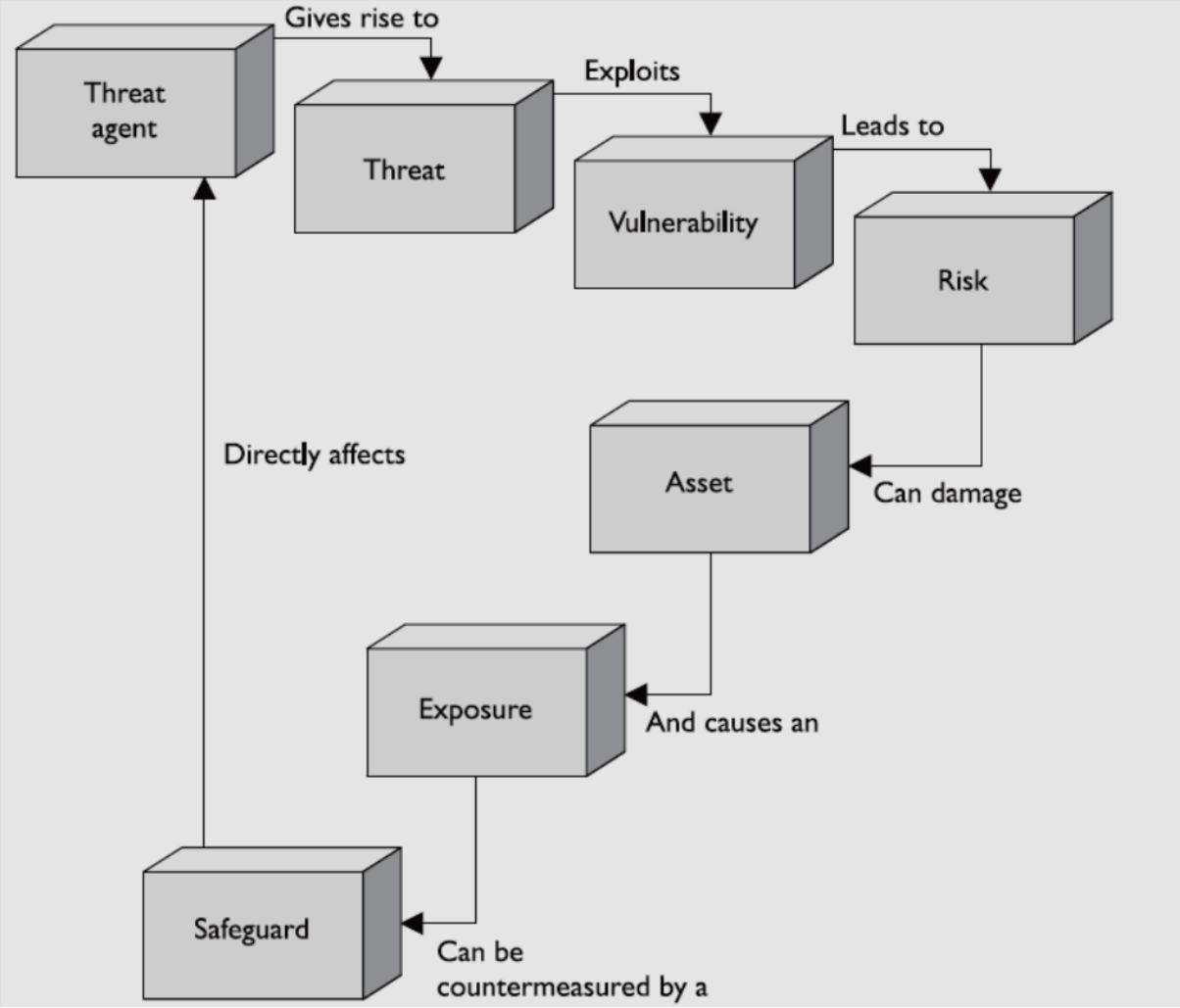
التعرض للخطر Exposure: هي حالة التعرض للخسارة أو فقدان معلومات بسبب مكون التهديد. و السبب الأساسي هو و جود نقاط ضعف. مثال: استخدام كلمات سر ضعيفة يعرض المستخدم لكشف كلمة السر الخاصة به و استخدامها من قبل المهاجم.

المتحكم Control أو الإجراء المضاد Countermeasure أو الإجراء الوقائي Safeguard: الآلية التي تستخدم لدرء الخطر. مثال: إغلاق كافة البوابات غير المستخدمة في جدار الحماية, أو استخدام كلمات سر قوية و تغييرها بشكل دوري.

الهندسة الاجتماعية Social Engineering: تُعَّرف الهندسة الاجتماعية بالطريقة التي تُستخدم للحصول على المعلومات من الأشخاص بطريقة الإقناع و الخداع لإقناعهم بأن المعتدي هو شخص آخر يحق له الحصول على المعلومات و ذلك دون استخدام أية تقنية من خلال التجهيزات الأمنية.

و يوضح الشكل 32 العلاقة بين مكونات الأمن و آلية استنتاج المتحكمات.

و سنقوم بشرح كل مجال و المجالات الفرعية المنبثقة عنها، و توصيف المتحكمات فيها.



الشكل 32 العلاقة بين مكونات الأمن و آلية استنتاج المتحكمات

2.3.2 المجالات المعرفة ضمن كل طبقة و المتحكمات

1. متحكمات الطبقة البشرية Human Layer و المجالات التي تتضمنها

يمكن تصنيف المتحكمات المتعلقة بالنواحي البشرية أي المستخدمين و العاملين في المؤسسة في المجالات التالية:

أ – السياسات المضادة للهندسة الاجتماعية

تتضمن هذه السياسات إجراءات احترازية Precautions و توصيات تهدف إلى التقليل من مخاطر الهندسة الاجتماعية من خلال المتحكمات التالية.

السياسات المضادة للهندسة الاجتماعية (المتحكمات)
دعم الإدارة المادي و المعنوي لمكافحة الهندسة الاجتماعية و إدراك مخاطرها
تأكيد الإدارة و التزامها بالعاملين لديها و بخاصة في الأماكن الحساسة و توطيد إحساسهم بالانتماء للمؤسسة و ضمان مستقبلهم
وجود برنامج خاص و مستقل عن برامج أمن المعلومات و الشبكات متخصص بالهندسة الاجتماعية و طرق مكافحتها
وجود كادر بشري متخصص بالهندسة الاجتماعية مرتبط مباشرة بالإدارة
عدم وجود أية معلومات هامة يمكن استغلالها من قبل المهاجمين على الموقع الالكتروني للمؤسسة مثل: أسماء و أرقام هواتف أو البريد الالكتروني لكافة مدراء المؤسسة و الاكتفاء بالمعلومات الخاصة بالمكاتب المسموح لها بالتعامل مع الزبائن و الجهات الخارجية. • في حال ضرورة وجود معلومات عن بعض المدراء يمكن وضع صفاتهم دون أسمائهم مثل: SalesManager@Companymail.xxx
عدم استخدام أرقام هواتف متسلسلة لكافة هواتف المؤسسة مما يسهل للمهاجم استنتاج أرقام الهواتف غير المعلن عنها
تنبيه المدراء و المسؤولين الهامين باستخدام أجهزة خلوي غير متطورة لتخزين أرقام الهواتف الهامة للشخصيات الحساسة. و ذلك كون أجهزة الخلوي الحديثة مثل iPhone و iPad و غيرها تحوي برامج تجسس.

إلزام جميع العاملين و بخاصة المدراء منهم بتوقيع استمارات دورية تتضمن: حسابات البريد الالكتروني الخاصة بهم خارج المؤسسة • حساباتهم على مواقع التواصل الاجتماعي – دون كلمات السر– • عدم استخدام حساباتهم البريدية خارج المؤسسة لنشاطات تخص المؤسسة • الالتزام بعدم إعطاء معلومات عن المؤسسة مهما بدت بسيطة و عامة • الإبلاغ الفوري عن أي اتصال مشبوه أو رسالة الكترونية أو برنامج يحاول الحصول على معلومات عن المؤسسة أو الأفراد
العزل الفيزيائي الكامل لشبكة المؤسسة عن الشبكة الموصلة بالانترنت و استخدام حواسيب منفصلة للدخول لكلا الشبكتين
وصل جميع خطوط الهاتف الخاصة بالمؤسسة بمقاسم مركزية قابلة لتسجيل المكالمات
تسجيل و مراجعة كافة المكالمات الهاتفية الواردة لأقسام الدعم الفني و خدمة الزبائن و المبيعات
التأكيد على التعاون بين فريق أمن المعلومات و الشبكات و فريق مكافحة الهندسة الاجتماعية لتسجيل البريد النافل Spam أو أية محاولة اختراق على المعدات الأمنية
التأكيد على عدم ترك وثائق هامة أو معلومات على مكاتب العاملين
التأكيد على استخدام آلات تلف الأوراق و المستندات قبل رميها في سلال المهملات
التأكد من قيام شركات التنظيف أو المستخدمين المسؤولين عن ذلك من ترحيل كافة المهملات
التأكد من أن عمليات تنظيف المكاتب و بخاصة مكاتب المدراء تتم بوجود بعض الموظفين أو المدراء أنفسهم
التأكد من إتلاف التجهيزات الحاسوبية و الشبكية القديمة بعد تفرغها من كافة المعلومات
ربط أنظمة الدخول للبنية و نظام الإجازات –الذاتية و الإدارية– بنظام السماح بالولوج للأنظمة العاملة في المؤسسة لمنع حسابات الأشخاص في حال الغياب أو الإجازة من الولوج و التحقق ممن يستخدم هذه الحسابات في حال غياب أصحابها
عدم السماح بالولوج إلى الأنظمة خارج أوقات الدوام الرسمي و منع دخول العاملين إلى مباني المؤسسة خارج أوقات الدوام الرسمي دون إذن مبرر من مدرائهم

توزيع المهام لضمان عدم احتكار فريق واحد للمهام الخاصة بأمن المعلومات و الشبكات و مكافحة الهندسة الاجتماعية: • فريق خاص بأمن المعلومات: يراقب العمل على الأنظمة و البرامج ضمن المؤسسة و تطبيق سياسة أمن المعلومات من نواحي صلاحيات المستخدمين و البرامج المفعلة على حواسيبهم و نشاطاتهم على تلك البرامج و الأنظمة و النسخ الاحتياطي و ملفات الرقابة Auditing logs على المخدمات و الحواسيب • فريق خاص بأمن الشبكات: يراقب العمل على التجهيزات الشبكية و السياسات الأمنية عليها و عمل التجهيزات الأمنية Firewalls أو IPS/IDS أو منظومات التشفير • فريق خاص بمكافحة الهندسة الاجتماعية: متخصص بالهندسة الاجتماعية و يقوم بمراقبة عمل الفريقين السابقين بالإضافة إلى التأكد من الإجراءات الخاصة بالهندسة الاجتماعية
مراقبة العاملين المتذمرين أو اللامبالين أو المهمِلين و إبعادهم عن الأماكن الحساسة و محاولة حل مشاكلهم و توعيتهم
التأكد – وخاصة في المؤسسات أو الأقسام الحساسة– من تفتيش العاملين عند الدخول و الخروج و عدم وجود أدوات تخزين معلومات Flash Memory أو CDs أو External Hard أو غيرها غير مصرح لهم بإدخالها أو إخراجها
التأكد قبل تسريح أي عامل و بخاصة التقنيين و الفنيين و المدراء من توفر كافة المعلومات عن المهام الموكلة إليه و مخاطر استبداله و وجود بديل و كفاءة البديل و تغيير كافة كلمات السر الخاصة بالعامل القديم و صلاحياته على التجهيزات و الأنظمة

ب –**برامج التوعية و التدريب**

يجب أن يقوم فريق مكافحة الهندسة الاجتماعية بالتعاون مع فرق أمن المعلومات و الشبكات بإجراء برامج توعية وتدريب دورية لكافة العاملين حول أمن المعلومات و الهندسة الاجتماعية، و التي تعتبر من أهم الوسائل لمنع تسريب المعلومات.

برامج التوعية و التدريب –المناعة الذاتية– (المتحكمات)
ضرورة التقيد بتعليمات الإدارة بالحفاظ على سرية المعلومات مهما كانت مع ذكر حوادث هامة حدثت و تحدث في مؤسسات أخرى
التأكيد على عدم وضع أسماء حساباتهم و كلمات السر على أوراق أو مستندات أو إعطائها لزملائهم
التوعية لحقيقة مواقع التواصل الاجتماعي و المحادثات Chat و ضرورة توخي الحذر في معلوماتهم الشخصية عليها و ما يكتبونه: • عدم استخدام الاسم الحقيقي و مكان العمل و أرقام الهواتف الحقيقية أو رقم بطاقة الائتمان أو حساباتهم المصرفية • عدم وضع أية معلومات عن المؤسسة التي يعملون فيها • التأكيد و بالوثائق على أن مواقع التواصل الاجتماعي و غيرها تتبع لحكومات و أجهزة استخبارات قد تستغلهم للضرر بهم أو بمؤسساتهم أو بأوطانهم • عدم تنزيل أي صور أو برامج مجانية تعرض عليهم و استخدامها على حواسب المؤسسة
التوعية لأساليب الهندسة الاجتماعية و استغلالها للنواحي الإنسانية لديهم مع الأمثلة الواقعية و العملية
التأكد – وبخاصة للمدراء – من زوارهم و المعلومات التي يحاولون الحصول عليها
التوعية عن البرامج الضارة التي يمكن أن تنصب على حواسيبهم من خلال تحميل الصور أو مقاطع الفيديو
التوعية لتقنيات Phishing و الخداع وطرق التحقق من المواقع المرسلة في البريد الالكتروني
التوعية لعدم ترك حواسيبهم بوضع التشغيل عند مغادرتهم مكان عملهم و حتى لفترة قصيرة
أن تتضمن برامج التوعية حقائق و أمثلة عملية لتجعل من برامج التدريب مهمة و مرغوبة من قبل العاملين و يجب أن تعتمد على الصور و غيرها لجذب المتلقي
التعريف بعدد من المواقع الآمنة و الموثوقة و التي تهم العاملين و أسرهم
التدريب على المعلومات المسموح إعطاؤها للمتصلين و في الرسائل الالكترونية و غيرها

التأكيد على ضرورة إعلام المعنيين في المؤسسة بأي اتصال هاتفي أو رسالة الكترونية تتضمن طلب لمعلومات هامة أو خاصة و حتى لو كانت على بريدهم الشخصي و ذلك لتقديم المساعدة
التأكد من عمل برامج مكافحة الفيروسات على أجهزتم في المؤسسة و حتى في المنزل و أهميتها
التوعية للقوانين و الأنظمة و العقوبات في حال تسريب المعلومات

ت -**الرقابة على العاملين و وسائل الاتصال و التفتيش المفاجئ**

بعد أن تم وضع سياسات أمنية فعالة في مجال مكافحة الهندسة الاجتماعية و برامج تدريب و توعية لرفع مستوى وعي و مناعة العاملين في المؤسسة للمخاطر. لابد من التحقق الدائم و التأكد من تنفيذ هذه السياسات و عدم وجود ثغرات أو أشخاص تشكل خطراً على المؤسسة.

الرقابة على العاملين و وسائل الاتصال و التفتيش المفاجئ (المتحكمات)
مراجعة التسجيلات الخاصة بالاتصالات الهاتفية للدعم الفني و خدمة الزبائن و الأقسام المخولة بتلقي الاتصالات من خارج المؤسسة و ذلك باستخدام Content Filtering لكلمات مفتاحية أو الاختيار العشوائي لبعض الاتصالات
مراقبة الرسائل البريدية الواردة للمؤسسة و بخاصة البريد النافل Spam و محاولة تحديد مصادرها
مراقبة الرسائل البريدية الصادرة عن المؤسسة و تحليل عينة منها للتحقق من عدم إرسال معلومات خاصة فيها و استخدام Content Filtering لكلمات مفتاحية في حال كان عدد البريد المرسل كبيراً
مراقبة نشاطات العاملين في المؤسسة على الأنظمة و البرامج و الذين سبق أن قدموا بعض المعلومات و التي قد تكون غير ضارة و غير المصرح لهم بتقديمها. أو الأشخاص المهملين الذين تسببوا ببعض الحوادث غير الضارة في عملهم
التفتيش المفاجئ للبرامج الموجودة على الحواسيب و التحقق من عدم وجود صور شخصية أو صور لخلفية الشاشة أو فيديو أو غيرها
التفتيش المفاجئ لسطح مكاتب العاملين و التأكد من عدم وجود وثائق أو أوراق تحوي معلومات هامة و غير محفوظة بشكل جيد
التفتيش المفاجئ لسلال المهملات و محتوياتها

التفتيش المفاجئ لقوائم العاملين على رأس عملهم و الغائبين و أماكن تواجد العاملين أثناء الدوام و وضع تجهيزاتهم الحاسوبية في حال مغادرتهم لمكاتبهم من حيث بقائها بوضعية التشغيل و كذلك وضع البرامج و الأنظمة التي تم الولوج إليها

ث -**الاختبارات الذكية**

يجب أن يقوم فريق مكافحة الهندسة الاجتماعية بإجراء اختبارات من نوع خاص – بحسب نوع المؤسسة و طبيعة عملها و المخاطر التي تهددها-. و تكون متممة لبرامج التوعية و دليلاً على نجاحها. تتضمن المتحكمات التالية:

الاختبارات الذكية (المتحكمات)
الاتصال من هاتف خارج المؤسسة –Private– بخدمة الزبائن أو الدعم الفني أو الأقسام المخول لها بالاتصال بخارج المؤسسة و عينة من بقية العاملين، و محاولة استدراجهم لإعطاء معلومات هامة عن المؤسسة – تمثيل دور المهاجم– و تسجيل النتائج و دراستها
إرسال رسائل الكترونية تحوي وصلات Links تؤدي إلى تحميل برامج أو صور غير ضارة و التحقق من تجاوب العاملين معها
البحث غير المباشر – دون علم الشخص المعني– في سلال المهملات لمعرفة نوعية الوثائق المهمة و مدى خطورتها
الدخول لمواقع التواصل الاجتماعي بأسماء وهمية و التواصل مع بعض العاملين – من خلال بريدهم الالكتروني الخاص – لمعرفة جزء من نشاطاتهم على هذه المواقع و لتوفير بدائل عن صفحات و مواقع أخرى
محاولة سرقة – أو الحصول– على بعض أدوات النسخ الاحتياطي المهملة و مراقبة رد فعل المسؤول عنها و مدرائه و تعديل سياسة النسخ الاحتياطي
التحقق من إجراءات الحماية الفيزيائية للدخول و الخروج للبناء

التحقق من أن السياسات الأمنية التي يضعها فريق أمن المعلومات والشبكات فعالة
محاولة الولوج لتجهيزات الحماية الشبكية Firewalls, IPS/IDS و غيرها و التحقق من عملها
التعاون مع فريق أمن المعلومات و الشبكات لتعديل الإعدادات و توعيتهم لوجود رقابة عليهم
تقديم تقارير دورية للإدارة عن نشاطاتهم و النصائح

ملاحظة: جميع المتحكمات في الطبقات اللاحقة تم استنتاجها من المعايير ISO 27K و ملحقاتها.

2. متحكمات الطبقة الإدارية Administrative Layer و المجالات التي تتضمنها

يمكن تصنيف المجالات في الطبقة الإدارية مع متحكماتها كما يلي:

أ – نظام إدارة أمن المعلومات ISMS

و هو نظام –برنامج موثق– تتبناه إدارة المؤسسة لتحقيق أمن المعلومات ضمن سياسات و إجراءات موثقة. يقوم بتطوير هذا النظام فرق أمن المعلومات و أمن الشبكات و مكافحة الهندسة الاجتماعية العاملة في المؤسسة، و تصادق عليه الإدارة ليتم تنفيذه و يتضمن سياسات و دلائل عمل المؤسسة في مجالات الأمن المختلفة. و من الأرجح أن يكون الجزء الأكبر من النظام مفروضاً من جهات حكومية أو رقابية [ISO/IEC 27001, 2005].

نظام إدارة أمن المعلومات (المتحكمات)
دعم الإدارة لبرنامج أمن المعلومات
عدم وجود أية أمور مستبعدة عن نظام إدارة أمن المعلومات
وجود سياسات و إجراءات للإدارة لتخصيص موارد لدعم أمن المعلومات من النواحي المالية أو تأمين كادر بشري متخصص
تناسب سياسات إدارة أمن المعلومات مع المواصفات العامة للمؤسسة و إستراتيجيتها في إدارة المخاطر
يجب أن تحقق سياسات إدارة أمن المعلومات كافة متطلبات الأعمال الخاصة بالمؤسسة، إضافةً إلى أية التزامات أو تشريعات قانونية متعلقة بأمن المعلومات

تضمن النظام لعوامل مفيدة وذات معنى لتقييم مخاطر أمن المعلومات تمت المصادقة عليها من قبل الإدارة
التزام المدراء حقيقةً بأمن المعلومات من خلال سلوكهم
التعريف الواضح بمتطلبات المهارة والتدريب والتوعية الضرورية لاختصاصيي أمن المعلومات وغيرهم مع تحديد الأدوار والمسؤوليات
وجود جدولة محددة للقيام بالمراجعة Auditing Review، مرة سنوياً على الأقل

ب –تقييم و معالجة المخاطر Risk Assessment and Treatment

يجب أن تتوفر خطة لمعالجة المخاطر و تقييمها بالمواصفات و المتحكمات التالية :

تقييم المخاطر و خطة مراجعتها (المتحكمات)
وجود طرق منهجية متبعة لتقييم المخاطر
أن تكون نتائج هذا التقييم قابلة للمقارنة وإعادة الإنتاج
تحديث طريقة تقييم المخاطر بناءً على ما سبق
تحديد العوامل الحرجة لمخاطر أمن المعلومات بشكل دقيق وقابل للتطبيق
تضمين التقييم جميع الأصول المعلوماتية الموجودة ضمن منظور إدارة أمن المعلومات
تحديد الأطراف المسؤولة (المالكة) عن الأصول المعلوماتية
وجود تحليل وتقييم كافٍ للتهديدات
وجود تحليل وتقييم كافٍ للثغرات وتأثيرها
وجود توثيق كافٍ لمختلف احتمالات المخاطر مع مراتب أو أولويات لها
توصيف علاج مناسب لكافة المخاطر المعرفة

وضع التغييرات ضمن الخطة
استخدام وتحديث خطة معالجة المخاطر بصورة استباقية فعالة كأداة لإدارة أمن المعلومات
قيام المؤسسة بمراجعة فعالة ووقائية لآلية تطبيق نظام إدارة أمن المعلومات للتأكد من أن طرق التحكم الأمنية المعرفة في خطة معالجة المخاطر والسياسات و...الخ

ت –تنظيم أمن المعلومات Organizing Information Security

يتضمن هذا المجال قسمين. أحدهما يتعلق بالتنظيم الداخلي و الآخر بالتنظيم مع الأطراف الخارجية العاملة في المؤسسة.

- **التنظيم الداخلي**
  - التزام الإدارة بأمن المعلومات
  - تنسيق جهود أمن المعلومات
  - توزيع المسؤوليات
  - عملية التفويض في سياق أمن المعلومات
  - اتفاقات السرية
  - الاتصال مع السلطات المخولة
  - الاتصال مع المجموعات الخاصة المهتمة
  - التدقيق المستقل لأمن المعلومات
- **الأطراف الخارجية**
  - تعريف المخاطر المتعلقة
  - مواجهة التحديات الأمنية حين التعامل مع الزبائن
  - مواجهة التحديات الأمنية في الاتفاقات مع أطراف ثالثة

فحص نظام إدارة أمن المعلومات داخلياً (المتحكمات)
وجود خطط داخلية لفحص إدارة أمن المعلومات
مسؤوليات إدارة عملية الفحص الداخلية موكلة رسمياً إلى مدققي تكنولوجيا معلومات مدربين ومختصين في ذلك. وهم الفرق الأمنية الثلاث.
مدى استجابة نظام إدارة أمن المعلومات إلى المخاطر المعرفة والمتغيرة بصورة ملحوظة
المسؤوليات الداخلية وآليات التواصل
يجب أن يتم تعريف و تفعيل دور المناصب التالية في فرق أمن المعلومات و الشبكات و مكافحة الهندسة الاجتماعية: مدير من الصف الأول مسؤول عن تكنولوجيا المعلومات وإدارة أمنها. أخصائيو أمن معلومات، مدراء أنظمة معلومات. مدير أمن للشؤون الفيزيائية في الموقع وأعضاء ارتباط المرافق. عضو ارتباط الموارد البشرية من أجل الأمور المتعلقة مثل الأفعال التأديبية والتدريب. فريق متخصص بالهندسة الاجتماعية. مدراء أنظمة وشبكات، تصميم الهيكل الأمني، وغيرهم من أخصائيي تكنولوجيا المعلومات.
يجب أن تعطي الإدارة دفعاً (قوة دفع) ودعماً قوياً لإدارة أمن المعلومات
توفر منتدى خاص لمناقشة سياسات إدارة أمن المعلومات والمخاطر وغيرها من القضايا المتعلقة مكون من مدراء الصف الأول
تعريف الأدوار والمسؤوليات بوضوح وتعيين الأفراد المؤهلين للقيام بها
تنسيق وتعاون كافٍ على مستوى الوحدة الاقتصادية، الوحدات فيما بينها، ومع المقر الرئيسي أيضاً

وجود عملية تدفق المعلومات (مثلاً رفع تقارير الحوادث) فعالة على أرض الواقع
الأطراف المعنية الخارجية
يتم تضمين الاتصالات والتواصل التابعة للأطراف المعنية في العقود بصورة غير مباشرة (الطرف الثالث) ضمن عملية تحليل المخاطر
وجود فرد أو أفراد مسؤولين عن ضمان أن كافة الروابط مع الأطراف الثالثة المعنية قد تم تعريفها وتقييم المخاطر المتعلقة بها
وجود ترتيبات لإدارة أمن المعلومات على أرض الواقع تراجع بانتظام طرق الاتصال مع الأطراف الثالثة وتقارنها مع المتطلبات
وجود عقود رسمية تغطي الروابط مع الأطراف الثالثة: ملكية ومسؤولية المسائل المتعلقة بإدارة أمن المعلومات المتطلبات القانونية حماية الأنظمة والشبكات والمعطيات من الناحية المنطقية والفيزيائية وحق المؤسسة بالتدقيق عليها إجراءات التحكم المتعلقة بالأصول، ومدى توافرية الخدمات في حالة الكوارث، وطرق إعلام الإدارة بالحوادث الأمنية قيام كادر الطرف الثالث بالتصريح الأمني رسمياً
عقود نقل الأعمال لأطراف خارجية تتضمن القضايا السابقة بشكل وافٍ

ث –الموارد البشرية و أمن المعلومات Human Resources and Information Security

و يتضمن كل ما يتعلق بالعاملين في المؤسسة:

- قبل التوظيف
  - الأدوار والمسؤوليات
  - شروط وبنود التوظيف
- خلال فترة التوظيف
  - مسؤوليات الإدارة
  - التوعية والتعليم والتدريب
  - عملية الانضباط
- انتهاء التوظيف أو تغيير الوظيفة

- مسؤوليات إنهاء التوظيف
- استرجاع الأصول
- إلغاء حقوق الدخول

متطلبات الأمن من جهة الموارد البشرية (المتحكمات)
يجب أن تكون وظائف أمن المعلومات و العقوبات و المسؤوليات معرفة بصورة واضحة في التوصيف الوظيفي و بنود وشروط التوظيف...إلخ، بالنسبة للكادر الخاص بأمن المعلومات. ومدراء الشبكات/الأنظمة، والمدراء والمستخدمين بصورة عامة
سياسات وإجراءات مناسبة للموارد البشرية حين انتهاك مبادئ أمن المعلومات
عمليات اختيار معمقة لكل من الكادر/المدراء وتحديداً للأدوار أو المواقع الحساسة
يتلقى الكوادر و مدراؤهم بانتظام تدريباً مناسباً على أمن المعلومات بما في ذلك الوظائف و المسؤوليات، و إجراءات الدخول ...الخ. و ذلك يجب أن يكون متضمناً في سياق التدريب العام على أنظمة تكنولوجيا المعلومات
إجراءات أو إرشادات تتعلق بعناصر أمن المعلومات في حالات من مثل ترك العمل أو تغيير التوظيف

ج – الامتثال Compliance

- **المتطلبات القانونية والامتثال**

- تعريف التشريعات القابلة للتطبيق
- حقوق الملكية الفكرية
- حماية سجلات المنظمة
- حماية البيانات وخصوصية المعلومات الشخصية
- منع سوء استخدام وسائل معالجة المعلومات
- تشريعات وسائل التحكم بالتشفير

- **السياسات والمعايير الأمنية والامتثال، والتأكد من الامتثال فنياً**
  - السياسات والمعايير الأمنية والامتثال
  - التأكد من الامتثال فنياً
- **مهمة تدقيق أنظمة المعلومات**
  - وسائل تحكم تدقيق أنظمة المعلومات
  - حماية أدوات تدقيق أنظمة المعلومات

الامتثال (المتحكمات)
خضوع المؤسسة تحت أية التزامات قانونية تتعلق بحماية البيانات والخصوصية (القوانين المحلية أو الدولية)
يجب أن تأخذ ترتيبات الأرشفة/التخزين احتمال تلف الوسائط بعين الاعتبار
توفر وسائط تخزين مناسبة ذات عمر طويل تستخدم من أجل التخزين طويل الأمد
يجب أن يعامل أي استخدام لمرافق تكنولوجيا المعلومات لأغراض لا تتعلق بالأعمال أو غير مصرح لها وبدون موافقة الإدارة على أنه خرق لأمن المعلومات
يجب أن تظهر رسائل تحذير للمستخدمين غير المصرح لهم
يضمن المدراء أن جميع الإجراءات الأمنية الواقعة ضمن نطاق مسؤوليتهم تطبق بصورة صحيحة للحصول على الالتزام المطلوب بسياسات ومعايير الأمن

3. متحكمات الطبقة المنطقية و المجالات التي تتضمنها

و تتضمن النواحي التقنية –ما عدا الشبكية– و تتضمن المجالات التالية:

أ – السياسة الأمنية Security Policy

- وثائق سياسة أمن المعلومات
- مراجعة سياسة أمن المعلومات

سياسات أمن المعلومات العامة (المتحكمات)
تبادل وفهم وقبول السياسات المتعلقة بما يلي: معايير الأمن الفيزيائية للحواسب وكافة ملحقاتها. الإجراءات الخاصة بالموارد البشرية والمتعلقة بالتحكم في النفاذ واستخدام خدمات تكنولوجيا المعلومات (أسماء مستخدمين وكلمات عبور، إجراءات تأديبية ...الخ). إرشادات للمستخدمين تتعلق بقضايا تراخيص برامج الحواسب، صد الفيروسات ...الخ).
أن تكون هذه السياسات منطقية وقابلة للتطبيق
تتكامل هذه السياسات مع أدوات تحكم مناسبة وكفوءة
تغطي هذه السياسات جميع الجوانب الأساسية المتعلقة بالحواسب والاتصالات
السياسات الأمنية الفنية
أن تكون سياسات الأمن الفنية مطبقة عموماً
إغلاق جميع الخدمات Services غير المستخدمة
إغلاق الواجهات غير المستخدمة
عدم استخدام أي من التطبيقات لبروتوكول telnet من أجل ممارسة أية أنشطة إدارية من مثل عمليات النسخ الاحتياطي Backup أو التهيئة Formatting
تظهر كلمات المرور بشكل مشفر أينما وجدت
تنسجم كلمات المرور مع مستوى التعقيد المطلوب والمعرف في السياسات
إلزام المستخدمين بتغيير كلمات المرور دورياً

وجود إجراءات موثقة من أجل إنشاء الحسابات للمستخدمين الجدد
يمتلك كل مدير نظام حساب فريدUnique ID خاص به
تتبع عمليات دخول – خروج مدراء الأنظمة والأوامر المنفذة من قبلهم Log File
إنشاء الحسابات بشكل تؤمن فيه أدنى سماحيات ممكنة من أجل إنجاز مهام المستخدمين المطلوبة فقط (قاعدة الحد الأدنى من الامتيازات/ السماحيات)
تغيير الإعدادات المسبقة التعريف Default Settings على كامل التجهيزات والأنظمة
تفعيل مخدم بروتوكول الوقت NTP Server لضمان تزامن الساعات على كافة التجهيزات
تتم عملية النسخ الاحتياطي لملفات التهيئة بصورة متكررة و دورية
نقل النسخ الاحتياطية إلى موقع خارجي/موقع مواجهة الكوارث Disaster Recovery Site
استخدام آليات أمن وحماية معينة على أنظمة التشغيل الموجودة حيث يتم تخزين ملفات التهيئة من أجل تحديد الدخول إلى هذه الملفات (مثلاً: عدم السماح بالنفاذ إلى التجهيزة دون كلمة مرور)
عدم استخدام بروتوكول TFTP لنقل ملفات التهيئة الشبكية في حال استخدامه يجب: العملية محصورة بعناوين حقيقية محددة يتم إيقاف الخدمة خارج أوقات استخدامها
إجراءات موثقة لعمليات النسخ الاحتياطي لملفات التهيئة للبرامج
توثيق كافة التغييرات والتحديثات لأنظمة التشغيل و البرامج بطريقة تسمح بمراجعتها
وجود تجهيزات احتياطية بحالة جاهزة استعداداً للطوارئ
توثيق وتجريب إجراءات مواجهة الكوارث البرمجية لأنظمة التشغيل و البرامج
تسجيل كافة محاولات الوصول إلى أي منفذ أو بروتوكول أو خدمة محجوبة
مراقبة انشغالية المعالجات /الذواكر /مساحات التخزين

ضرورة وجود مخدم خاص لحفظ ملفات الدخول محمٍ وذو سماحية دخول محدودة جداً
توثيق ومتابعة إجراءات تدقيق الدخول حسب ملفات الدخول الصادرة عن مختلف التجهيزات والأنظمة
أن تعتمد التقارير والتحاليل على رسائل النظام ورسائل ملفات الدخول
وجود سياسة واضحة و فعالة عند حدوث أي خرق أو نشاط غير مصرح به
أن يكون مهندسو الشبكات /الأنظمة /التطبيقات /الخدمات على اطلاع بآخر الثغرات التي قد تصيب مجالاتهم

ب – إدارة أمن الأصول المعلوماتية

- مسؤولية الأصول
  - مخزون الأصول
  - ملكية الأصول
  - الاستخدام المقبول للأصول
- تصنيف المعلومات
  - إرشادات عامة
  - عنونة ومعاملة المعلومات

إدارة أمن الأصول المعلوماتية (المتحكمات)
وجود ترتيبات تتعلق بإنشاء وصيانة مخزون الأصول المعلوماتية
وجود قوانين تحكم تطبيق الأنظمة الجديدة
وجود بطاقة تعريف الأصل المعلوماتي على كل الحواسيب

ضرورة أن تكون جميع كوابل الكهرباء والبيانات معنونة بوضوح، وجميع مخططات الأسلاك محفوظة بالكامل مع التعديلات التي تطرأ عليها.
يجب أن يتوافق تصنيف المعلومات على متطلبات الأعمال من نواحي السرية و الإتاحية
استخدام الاختصارات المناسبة في الوثائق والصيغ والتقارير والشارات و وسائط النسخ الاحتياطي ونقل الملفات
الوعي الكافي لدى الكادر لمتطلبات الأمن المقابلة لمعاملة المواد الحساسة و الخطيرة من النواحي الصحية و البيئية

ت – إدارة عمليات التشغيل

- الإجراءات التشغيلية والمسؤوليات
  - إجراءات تشغيل موثقة
  - إدارة التغيير
  - فصل المهام
  - الفصل بين وسائل التطوير والاختبار والتشغيل
- إدارة تسليم خدمات الأطراف العقدية الثالثة
  - تسليم الخدمات
  - مراقبة ومراجعة خدمات الطرف العقدي الثالث
  - إدارة تغيير خدمات الطرف العقدي الثالث
- تخطيط النظام والقبول
  - إدارة القدرات
  - قبول النظام
- الحماية مقابل الرمز الخبيث والنقال
  - وسائل التحكم ضد الرمز الخبيث

- وسائل التحكم ضد الرمز النقال
- النسخ الاحتياطي
  - النسخ الاحتياطي للمعلومات
- التعامل مع الوسائط
  - إدارة الوسائط القابلة للإزالة
  - تصريف الوسائط
  - إجراءات التعامل مع المعلومات
  - أمن نظام التوثيق
- تبادل المعلومات
  - سياسات وإجراءات تبادل المعطيات
  - اتفاقات التبادل
  - نقل الوسائط الفيزيائية
  - الرسائل الإلكترونية
  - أنظمة معلومات العمال
- خدمات التجارة الالكترونية
  - التجارة الإلكترونية
  - تبادل المعاملات الكترونياً وبالزمن الحقيقي
  - إتاحة المعلومات للجميع
- المراقبة
  - التفحص
  - استخدام نظام مراقبة
  - حماية معلومات ملفات الدخول
  - ملفات تسجيل إدارية وفنية
  - ملفات الأخطاء
  - التزامن بالنسبة للوقت

إدارة عمليات التشغيل والاتصالات (المتحكمات)
وجود مجموعة كاملة من إجراءات الأمن المتعلقة بعمليات تشغيل تكنولوجيا المعلومات عموماً
وجود مجموعة كاملة من إجراءات الأمن المتعلقة بإدارة الأنظمة والشبكة
وجود مجموعة كاملة من إجراءات الأمن المتعلقة بإدارة الحوادث
وجود مجموعة كاملة من إجراءات الأمن المتعلقة بإدارة أمن تكنولوجيا المعلومات
مراجعة الإجراءات السابقة و تحديثها بشكل مستمر
تكليف الأفراد المسؤولين عن إدارة الأنظمة بمسؤوليات متناسبة مع كفاءاتهم و قدراتهم
وجود اختبارات قبول وتخطيط للسعات يتضمن استخدام /مشغولية المعالج، حجم القرص، سعة الشبكة ...الخ.
اجراء كامل اختبارات القبول قبل استقدام أنظمة جديدة و البدء باستثمارها
تحديث إجراءات الاستعادة حتى تستوعب الأنظمة الجديدة والمتقادمة
يتم باستمرار وضمن تواتر معين فحص الحواسب القائمة بذاتها–غير المتصلة بالشبكة– والمحمولة ضد الفيروسات
تخفيض مستويات الإصابة بالفيروسات للحدود الدنيا (الوضع تحت السيطرة شبه التامة)
امتلاك المدراء والكادر معرفةً كافية حول إجراءات الحماية من البرامج الخبيثة
وجود حماية كافية ضد الهجمات مثل أحصنة طروادة، الديدان، البرامج التجسسية، البرامج المتطفلة ...الخ
توثيق وتجريب استراتيجيات وإجراءات النسخ الاحتياطي

يجب أن تغطي هذه الاستراتيجيات البيانات، البرامج، ملفات النظام، ملفات البارامترات ...الخ لكامل الأنظمة بما فيها المخدمات، الحواسب، أنظمة الهاتف وشبكته، أنظمة إدارة الشبكات والنظم، الأنظمة القائمة بذاتها والمحمولة، أنظمة التحكم ...الخ
القيام بالنسخ الاحتياطي بتواتر ونوع مناسب من حيث زمن الاستعادة
وسائط النسخ الاحتياطي محمية ضد الفقد، السرقة، الضرر، الحرائق بحالتي التخزين محلياً أو في مكان آخر
جميع وسائط النسخ الاحتياطي المدونة في الإجراءات والسجلات موجودة فعلياً و تطبق على أرض الواقع
توثيق إجراءات إدارة الشبكة المتعلقة بعناصر الأمن
تغطية الأوجه المختلفة لأمن المعلومات مثل الترتيبات الأمنية للاتصال مع الطرف الثالث بصورة كافية
تسجيل محدث وكامل لكل أشرطة النسخ الاحتياطي، الأقراص القابلة للإزالة، الأقراص الممغنطة ...الخ
التأكد من وجود نسختين مؤرشفتين من البيانات قبل محي النسخة الأصلية
التحقق و إعادة شد الأشرطة المؤرشفة خلال تواتر زمني معين
الحفاظ على سرية البيانات المخزنة بوسائل تحكم مناسبة
وجود وسائل تحكم أمنية مناسبة لتبادل المعلومات
وجود ترتيبات أمنية مناسبة من أجل الإنترنت والإنترانت والأنظمة المتعلقة
استخدام بروتوكول التصفح المشفر https عند استخدام التطبيقات العاملة على أساس الويب Web Applications وذلك لحماية البيانات الحساسة حين توجيهها بين المتصفح ومخدم الويب
مراقبة الدخول على الأنظمة الرئيسية ورفع تقارير الحوادث الأمنية
وجود عملية قائمة تتعلق بالمراجعة والاستجابة المناسبة للإنذارات الأمنية الداخلي منها والخارجي
متابعة ملفات الدخول والتقارير باعتماد مبادئ المسؤولية والمحاسبة

ث – التحكم بالنفاذ Access Control

- التحكم بالوصول ومتطلبات العمل
  - سياسة التحكم بالنفاذ
- إدارة دخول المستخدم
  - تسجيل المستخدم
  - إدارة الامتيازات
  - إدارة كلمة عبور المستخدم
  - مراجعة حقوق دخول المستخدم
- مسؤوليات المستخدم
  - كلمة العبور
  - إهمال معدات المستخدم
  - سياسة الشاشة وسطح المكتب الناصعين
  - التحكم بالاتصال الشبكي
  - التحكم بالتوجيه الشبكي
- التحكم بالنفاذ إلى أنظمة التشغيل
  - إجراءات تسجيل الدخول الأمنية
  - تعريف وتصريح المستخدم
  - نظام إدارة كلمات العبور
  - استخدام أدوات النظام
  - انتهاء زمن الجلسة
  - حدود مدة الاتصال
- التحكم بالنفاذ إلى التطبيقات والمعلومات
  - قيود الوصول إلى المعلومات
  - عزل الأنظمة الحساسة
- الحواسب النقالة والعمل عن بعد

- الحواسب النقالة والاتصالات
- العمل عن بعد

التحكم بالنفاذ (المتحكمات)
التصديق والتوثيق الجيد لمتطلبات الأعمال المتعلقة بالتحكم بالنفاذ من قبل مالكي (المسؤولين عن) الأصول المعلوماتية
التضمين الجيد لمتطلبات الأعمال من أجل التحكم بالنفاذ في المواصفات الفنية الخاصة بتصميم نظام الأمن المتبع
يجب أن تكون حقوق النفاذ محدودة قدر المستطاع
مراجعة وتعديل حقوق النفاذ بانتظام
إيلاء الإدارة اهتماماً خاصاً لوسائل التحكم في النفاذ و الحسابات المتعلقة بمستخدمي النظام و قواعد البيانات و التطبيقات ذوي الامتيازات (كامل السماحيات) و مدراء الشبكات
توثيق إساءة استخدام تلك الامتيازات و تصنيفها و التحقق من عدم تكرارها
وجود وسائل التحكم بكلمات المرور
متابعة فريق أمن المعلومات بانتظام و التدقيق لكشف كلمات العبور الضعيفة وتوعية/تدريب المستخدمين أمنياً
قيام الأفراد المخولين بحد الدخول إلى التطبيقات/الخدمات بفاعلية
قيام العقد الشبكية بالتحقق وتأسيس مناطق أمنية مختلفة باستخدام جدران الحماية، منع الدخول ...الخ
تطبيق تقنية إلغاء الجلسة Session Timeout بسبب نفاذ الوقت على الحواسب، الشبكات، التطبيقات، أنظمة التشغيل

وجود وسائل تحكم بالنفاذ مناسبة، من ضمنها مثلاً استخدام بطاقات التعريف أو البصمة الشخصية أو Single Sign On SSO، بما يضمن التحقق من المستخدم Authentication، باستخدام الوسائل المؤتمتة، التشفير ...الخ
وجود وسائل تحكم أمنية متعلقة بالتجوال Mobile Users، المستخدمين المنزليين (الدخول البعيد)، الحواسب النقالة، وسائل التخزين المتحركة، الشبكات الافتراضية الخاصة ...الخ
الحفاظ و التحكم بالأنظمة المحمولة

ج – اكتساب وتطوير وصيانة أنظمة المعلومات

- المتطلبات الأمنية لأنظمة المعلومات
  - تحديد وتحليل المتطلبات الأمنية
- عملية التصحيح في التطبيقات
  - التحقق من البيانات المدخلة
  - التحكم بالمعالجة الداخلية
  - صحة الرسائل
  - التحقق من البيانات المخرجة
- أمن أنظمة الملفات
  - التحكم في برامج التشغيل
  - حماية بيانات اختبار النظام
  - التحكم بالوصول إلى مصدر ترميز البرامج
- عملية تطوير ودعم الأمن
  - إجراءات التحكم بالتغيير
  - مراجعة التطبيقات فنياً بعد تغيير نظام التشغيل
  - تقييد التغيير لحزمة البرامج
  - تسرب المعلومات

- البرامج المطورة خارج المنظمة

- إدارة الثغرات الفنية
  - التحكم في الثغرات الفنية

اكتساب، تطوير، صيانة أنظمة المعلومات (المتحكمات)
إمكانية أن تتطلب التغيرات –إضافة برامج أو تطويرها– القيام بمراجعة أمنية/تقييم المخاطر وحتى إعادة ترخيص الأنظمة في حال الحاجة
استخدام طرق رسمية منهجية بانتظام لتحديث أو تغيير الأنظمة المعلوماتية
تطبيق وسائل تحكم مناسبة من أجل البيانات مثل التحقق من صلاحية الإدخالات والمعالجة، التشفير، رسالة التحقق ...الخ
تطبيق سياسات رسمية تعنى باستخدام وسائل التحكم السرية
يجب أن تشمل الإجراءات: تحديد المعلومات التي يجب حمايتها حسب المبادئ العامة. المعايير الواجبة التطبيق لضمان فعالية تنفيذ وسائل التحكم السرية. القيام بتحديد مستوى الحماية الواجب تطبيقه. إدارة مفاتيح السرية بما فيها استرجاع المعلومات في حال ضياع أو تضرر أو انكشاف المفاتيح. التوافق مع أية متطلبات موثقة.
وجود وسائل تحكم كافية لعزل بيئة التطوير عن التجريب و عن الإنتاج
يستند قبول التغييرات على تأكيد المختصين أن التغيرات/التجديدات لا تعطل العمليات التشغيلية الأخرى
توثيق التغيرات وذكر مبررات القيام بها وتصديقها من الإدارة
حماية بيانات الاختبارات بحد ذاتها من الكشف

يجب أن تعالج إجراءات التحكم مواضيع التغيرات الهامة في الأنظمة الحاسوبية ووسائل الاتصالات
وجود عمليات مناسبة تعنى بمراجعة مخزون الأنظمة و توضيح الثغرات الأمنية المتعلقة بها
تقييم الرقع البرمجية Software Patches (البرمجيات اللاحقة لمعالجة ثغرات البرامج المنصبة) من حيث قابلية تطبيقها ومخاطرها قبل تنفيذها
أن تكون عمليات التطبيق الطارئة للرقع البرمجية مدركة وسهلة بصورة مقبولة

ح – إدارة حوادث أمن المعلومات

- رفع الحوادث ونقاط الضعف المعلوماتية الأمنية
  - رفع الحوادث المعلوماتية الأمنية
  - رفع نقاط الضعف الأمنية
- إدارة حوادث أمن المعلومات وتحسينها
  - المسؤوليات والإجراءات
  - التعلم من الحوادث المعلوماتية الأمنية
  - جمع الأدلة

إدارة حوادث أمن المعلومات (المتحكمات)
يتمتع القائمون على رفع تقارير الحوادث الأمنية ونقاط الضعف بالوعي الكافي لسير عمليات معالجة هذه المهام. والأهم من ذلك أن يتقنوا استخدمها فعلياً
الالتزام بالسياسات واللوائح والإرشادات على أرض الواقع
وجود معالجة ناضجة نسبياً لإدارة الحوادث، التقييم/التحقيق، الفعل التصحيحي، والأجزاء الأخرى لإدارة الحوادث الأمنية وتعزيز فرص الحماية
تجري وبصورة متواصلة عملية التعلم من الحوادث Learn From Previews Incidents و الدعم في معرفة المخاطر ووسائل التحكم الأمنية بناءً على إدارة الحوادث

خ – إدارة استمرارية العمل Business Continuity

إدارة استمرارية العمل (المتحكمات)
تصميم أنظمة تكنولوجيا المعلومات، الشبكات ...الخ، لتؤمن إتاحية Availability عالية تدعم معالجة الأعمال الأكثر حرجاً وأهميةً
تفهم الأطراف المعنية للمخاطر التي تواجهها المؤسسة في حال توقف العمل على الأنظمة المعلوماتية
تعريف دقيق للعمليات الحرجة بالنسبة للأعمال والأصول المعلوماتية المرتبطة بها وتأثير الحوادث المحتمل عليها
وجود خطط مناسبة للمحافظة على عمليات التشغيل أو استعادتها عند حصول حوادث ضمن إطار زمني محدد
اعتماد وسائل تحكم مانعة و كاشفة و مصححة تُناسب أعمال استعادة العمل
يجب أن تأخذ هذه الخطط بعين الاعتبار التعريفات والاتفاقات المتعلقة بالمسؤوليات، الخسائر المقبولة، إجراءات تنفيذ المعالجة والاستعادة، توثيق الإجراءات، الاختبارات والتجارب المنتظمة
اعتماد إطار عمل وحيد و متناسق لتخطيط استمرارية العمل
يضمن هذا الإطار متانة هذه الخطط و يعرف الأولويات للاختبار والصيانة
الوعي لدى أعضاء إدارة الحوادث/الأزمات و فرق المعالجة وغيرهم من المعنيين، بهذه الخطط ويدركون تماماً أدوارهم ومسؤولياتهم

4. متحكمات الطبقة الشبكية و المجالات التي تتضمنها

تشمل الطبقة الشبكية كل ما يتعلق بالشبكات و خطوط الاتصال و المعدات الشبكية و التجهيزات الأمنية الشبكية بالإضافة إلى الإعدادات Configurations على هذه التجهيزات.

- التحكم بالوصول إلى الشبكة
  - سياسة استخدام الخدمات الشبكية
  - التصريح للاتصال الخارجي
  - تعريف المعدات في الشبكات
  - حماية منفذ التشخيص والتهيئة عن بعد
  - تقسيم الشبكات
- إدارة أمن الشبكة
  - وسائل التحكم الشبكية
  - أمن شبكة الخدمات
- وسائل التحكم بالتشفير
  - سياسات استخدام التحكم بالتشفير
  - إدارة المفاتيح

الطبقة الشبكية (المتحكمات)
التحكم بالوصول للشبكة بأمان مثل استخدام Access Control List على مبدلات الشبكة
عدم السماح بالدخول للتجهيزات الشبكية من مبدلات و موجهات ...الخ إلا لفريق الشبكات
التأكد من عدم الدخول لمنافذ التهيئة للتجهيزات الشبكية إلا للمعنيين
استخدام معايير الأمن الفيزيائية للتجهيزات الشبكية و خطوط الاتصال وكافة ملحقاتها
تقسيم الشبكات الداخلية LANs إلى عدة شبكات افتراضية VLANs و ذلك لحصر كافة التجهيزات الشبكية و تجهيزات أمن الشبكات في أقسام خاصة
تصميم الشبكات بحيث تؤمن إتاحية Availability عالية تدعم استمرار عمل الشبكات. من حيث تواجد تجهيزات شبكية احتياطية
توفر خطوط اتصال احتياطية
وجود إجراءات واضحة و موثقة لنقل الاتصال للتجهيزات الشبكية و الخطوط الاحتياطية

مراقبة عمل التجهيزات الشبكية من موجهات Routers و مبدلات Switches و موديمات و غيرها و التحقق من أدائها
وجود فريق عمل متخصص بأمن التجهيزات الشبكية
توثيق محاولات الدخول للتجهيزات الشبكية
وجود تجهيزات خاصة بأمن الشبكات مثل Firewalls و أجهزة كشف/منع الاختراق IPS/IDS
التحقق من عدم استخدام الإعدادات المصنعية Default Settings
استخدام سياسات Rules فعالة على جدار الحماية لإغلاق البوابات غير المستخدمة
استخدام إعدادات فعالة على أجهزة كشف/منع الاختراق IPS/IDS
مراجعة و توثيق التقارير المولدة على أجهزة الحماية الشبكية
استخدام المناطق المعزولة و بعدة مستويات لحماية المخدمات الأساسية و قواعد البيانات DMZ
استخدام التشفير على جدار الحماية أو بأجهزة شبكية متخصصة بالتشفير لضمان سلامة البيانات المتبادلة عبر خطوط الاتصال
استخدام خوارزميات تشفير موثوقة و مقبولة عالمياً مثل AES و Diffie-Hellman و خوارزميات PKI Infrastructure مثل RSA
إدارة مفاتيح التشفير من خلال نظام موثوق و فعال مثل استخدام الشهادات الرقمية Digital Certificates
ضمان نقل المفاتيح الخاصة بآلية سرية و مضمونة
ضمان تخزين المفاتيح السرية الخاصة و الشهادات الرقمية في أماكن آمنة
أن تكون المفاتيح المستخدمة للتشفير بأطوال غير قابلة للكشف
استخدام تقنيات VPN لدخول المستخدمين عبر الشبكة الانترنت

5. متحكمات الطبقة الفيزيائية

و تتضمن كل ما يتعلق بالمباني و البيئة المحيطة بالتجهيزات و العاملين و دخول الأفراد للمباني و لأماكن تواجد المخدمات و التجهيزات الشبكية:

- المناطق الأمنية
  - محيط الأمن الفيزيائي
  - وسائل التحكم بالمدخل الفيزيائي
  - تأمين الغرف والمكاتب والمرافق
  - الحماية من التهديدات الفيزيائية الداخلية والخارجية
  - العمل في المناطق الأمنية
  - أماكن الدخول والتسليم والتحميل العامة
- أمن المعدات
  - وضع وحماية المعدات
  - الأدوات الداعمة
  - أمن الكبلات
  - صيانة المعدات
  - أمن المعدات خارج المصرف
  - أمن المعدات المنسقة أو المعاد استخدامها
  - ترحيل الملكية

متطلبات الأمن من الناحية البيئية والفيزيائية (المتحكمات)
وجود آليات دقيقة لدخول العاملين/الضيوف للمباني
التحقق من أن الضيوف قد دخلوا فقط للأماكن المصرح لهم بالدخول إليها
وضع وسائل فعالة و دقيقة لتقليل احتمالات الكوارث أو تكاليف الحلول الوقائية

أن يكون البناء مبنياً مع الأخذ بعين الاعتبار الأمن من الناحية الفيزيائية، مثلاً جدران متراصفة، أبواب سميكة صلبة ...الخ
تطبيق أنظمة مناسبة للتحكم بالدخول والإجراءات المقابلة لها
وجود إجراءات حماية فيزيائية مناسبة للكبلات الخارجية، علب القواطع، مبرد المكيفات، اللواقط، مداخل التهوية...الخ ضد الأضرار غير المتعمدة أو الدخول عنوة
وجود وسائل حماية/تحكم تتعلق بالحرائق أو الدخان مثل الأسلاك ومواد البناء المقاومة للحريق–قليلة إصدار الدخان–
عم السماح بالتدخين في أماكن العمل و وضع إشارات عدم التدخين بوضوح
فحص وصيانة أنظمة الإنذار ضد الحرائق والقفل بصورة منتظمة من قبل أخصائيين
وجود توعية كافية حول إجراءات الإخلاء عند حدوث الحريق
وجود ما يكفي من وحدات عدم انقطاع التيار الكهربائي تغطي سعاتها كافة التجهيزات الحاسوبية الأساسية والمحيطية وتفرعاتها
وجود مولدة كهربائية احتياطية ذات سعة كافية
توفر طاقة تبريدية كافية لمعالجة الحمل الحراري
وجود ما يكفي من القطع الاحتياطية أو المحمولة المتاحة لدعم المرونة والصيانة الدورية دون تأثر الخدمة
توافر حساسات حرارية تدعم القراءة من بعيد وإنذارات زيادة درجة الحرارة إضافةً إلى إجراءات الطوارئ
وجود نظام منع وكشف وإنذار بعيد حول تسرب المياه وطوفانها
المحافظة على شروط نظافة غرف التجهيزات و الاتصالات
وجود معالجة خاصة لتجنب الغبار

تثبيت كافة الهياكل المعدنية المكشوفة وربطها إلى نقطة تأريض لأغراض السلامة وتقليل الكهرباء الساكنة
التأكد من عمل قواطع الإضاءة، عوازل الكبلات، قواطع الطاقة الكهربائية ...الخ
تشغيل وصيانة كافة التجهيزات الفيزيائية واختبارها تحت الحمل على أساس المواصفات الفنية التي حددتها الجهة الصانعة
وجود عملية مصرحة إدارياً لزوم نقل الأصول المعلوماتية من موقع إلى آخر
وجود عمليات آمنة من أجل مسح البيانات الحساسة والشخصية كاملةً من وسائط التخزين الثابتة أو القابلة للإزالة قبل التصرف بها لغرض إتلافها أو نقلها

و بعد استعراض المكونات الأساسية للنموذج المقترح يمكن تقديمه كما في الشكل 33:

الشكل 33 النموذج المقترح و المجالات التي تحويها كل طبقة

4.2 الدراسة التحليلية

تم بناء النموذج المقترح على عدة مبادئ:

1. يؤمن النموذج المقترح الحماية القصوى للمعلومات و الأصول بحيث أُحيطت بكل متطلبات الحماية.
2. خمس طبقات أمنية تعكس الحاجة لتجميع المتحكمات الأمنية في مجالات متشابهة من حيث النوعية و الهدف و تسهل فهمها و تنفيذها.
3. في كل طبقة تم تعريف مجالات محددة تحوي متحكمات قابلة للتنفيذ. بمجموع 18 مجالاً أمنياً.
4. تحيط الطبقات ببعضها بحسب أهميتها و مدى تأثيرها على أمن المعلومات.
5. يمكن تنفيذ النموذج المقترح من الأعلى للأدنى و بالعكس، على أن يتم الالتزام بكافة المجالات ضمن الطبقة.
6. بُني النموذج على اعتبار المؤسسة التي سيطبق عليها تقدم خدمات إلكترونية شبكية سواءً عن طريق الانترنت أو الشبكة الداخلية للمؤسسة Intranet أو Extranet[1].

1.4.2 الفرق المسؤولة عن أمن المعلومات و الشبكات و الهندسة الاجتماعية

1. فريق خاص بأمن المعلومات: يراقب العمل على الأنظمة و البرامج ضمن المؤسسة و تطبيق سياسة أمن المعلومات من نواحي صلاحيات المستخدمين و البرامج المفعلة على حواسيبهم و نشاطاتهم على تلك البرامج و الأنظمة و النسخ الاحتياطي و ملفات الرقابة Auditing logs على المخدمات و الحواسيب.
2. فريق خاص بأمن الشبكات: يراقب العمل على التجهيزات الشبكية و السياسات الأمنية عليها و عمل التجهيزات الأمنية Firewalls أو IPS/IDS أو منظومات التشفير.
3. فريق خاص بمكافحة الهندسة الاجتماعية: متخصص بالهندسة الاجتماعية و يقوم بمراقبة عمل الفريقين السابقين بالإضافة إلى التأكد من الإجراءات الخاصة بالهندسة الاجتماعية.

الهدف من توزيع العاملين في مجال أمن المؤسسة على ثلاث فرق هو توزيع المهام الأمنية و عدم احتكارها من قبل جهة واحدة و ضمان عدة جهات للرقابة بالإضافة إلى ضمان تدريب و تأهيل كل فريق

[1] Intranet: شبكة المؤسسة التي لا يسمح بالنفاذ إليها لغير العاملين في المؤسسة، أما Extranet: فهي شبكة المؤسسة التي يسمح بالنفاذ لبعض خدماتها للزبائن و الشركاء فقط [Stallings W. B., 2008].

على المهام الموكلة إليه كتخصص يمكن من خلاله تحسين قدراتهم و عدم تشتيتها في عدة مجالات متباعدة من حيث طبيعة العمل و التجهيزات عن بعضها و لكنها تصب في نفس الهدف و هو حماية و ضمان عدم اختراق المنظومات الالكترونية العاملة في المؤسسة.
و يجب أن نؤكد هنا أن جميع فرق العمل الثلاث المذكورة يجب أن تتبع إدارياً و تقنياً لمنصب إداري رفيع – مثل معاون مدير عام لشؤون أمن المعلومات– Chief Information Officer CIO.

2.4.2 الكفاءات المطلوبة في فرق العمل

1. فريق أمن المعلومات: اختصاص في إدارة البنية التحتية للمجال/المجالات المعرفة للمؤسسة Domain[2] و إدارة السياسة الأمنية لصلاحيات المستخدمين و الأجهزة المسموح باستخدامها –مثل ...USB Flash Disk, CD Rom, – و يمكن أن يحمل العاملون في هذا المجال شهادة MCITP أو RHCE أو التدريب الخاص بمنظومة المجال المستخدم. كما يختص العاملون بتحليل ملفات الرقابة على أنظمة التشغيل Log Files و الأنظمة الالكترونية المستخدمة. بالإضافة إلى الإدارة و الرقابة لنظام Antivirus المستخدم و تحديثه، كما يملك هذا الفريق القدرة اللازمة لتحليل البرامج الضارة و مكافحتها، و يمكن أن يخضع هذا الفريق لدورات أمن المعلومات مثل CISSP أو CEH أو غيرها.
2. فريق أمن الشبكات: تتضمن منظومة أمن الشبكات عدة تجهيزات أمنية متطورة و بحاجة لتفرغ و تخصص مثل Firewalls و IPS/IDS و منظومات التشفير. بالإضافة إلى التجهيزات الشبكية كالموجهات و المبدلات. و التي يتطلب عملها إلى متخصصين و مراقبة دائمة.
3. فريق مكافحة الهندسة الاجتماعية: يضم مجموعة من التقنيين المتخصصين في الهندسة الاجتماعية و طرق مكافحتها الالكترونية و غير تقنيين متخصصين في علم النفس و مدربين على مخاطر الهندسة الاجتماعية و طرق مكافحتها من النواحي الإنسانية.

و نؤكد على ضرورة تعاون الفرق الثلاثة لضمان الحصول على نتائج ملموسة و فعالة في حماية المؤسسة.

[2] المجال: هو الاسم الالكتروني للمؤسسة و الذي تُضم إليه كافة التجهيزات الحاسوبية العاملة في المؤسسة مثل: Company.com

3.4.2 الطبقة البشرية

اعتبرنا أن الطبقة البشرية تحيط بكافة الطبقات الأخرى و هي الأكثر أهمية و ذلك للأسباب التالية:

1. الإنسان هو العامل الحاسم في أي منظومة فلا فائدة من التجهيزات ما لم يكن المسؤول عنها يمتلك الكفاءة المطلوبة لتشغيل و مراقبة التجهيزات.
2. إن كافة التجهيزات الأمنية وضعت لحماية الشبكات و المعلومات من الخطر الخارجي. فماذا عن المستخدمين داخل المؤسسة ؟ و الذين يسمح لهم بالدخول للأنظمة المعلوماتية –لأداء أعمالهم– من خلف تجهيزات الحماية و لو تم ذلك بصلاحيات محدودة، فذلك يشكل الخطر الأكبر على المعلومات من خلال التسريب/التخريب المقصود أو غير المقصود.
3. حماية المؤسسة من الداخل هي حجر الأساس لتأمين الحماية الشاملة للمؤسسة.
4. تتضمن الطبقة الأمنية البشرية أربعة مجالات تضمن تحقيق الهدف منها من خلال:

- **السياسات المضادة للهندسة الاجتماعية**

الإجراءات الداخلية الواجب اتخاذها لضمان مناعة العاملين و السياسات الداخلية من الاختراق.

- **برامج التوعية و التدريب**

تضمن المناعة الحقيقية و التوعية للعاملين من الهندسة الاجتماعية و مخاطرها.

- **الرقابة على العاملين و وسائل الاتصال و التفتيش المفاجئ**

بعد التدريب و التوعية لا بد من إجراءات فعالة للرقابة العملية على العاملين و وسائل الاتصال بهم من خارج المؤسسة.

- **الاختبارات الذكية**

وهي مجموعة اختبارات من نوع خاص تحاكي محاولات الاختراق التي قد يقوم بها المهاجمون من خارج المؤسسة، و تسمح بالنتيجة باتخاذ إجراءات مضادة.

4.4.2 الطبقة الفيزيائية

بعد أن تم التحصين الداخلي للمؤسسة من خلال الطبقة البشرية. ينتقل النموذج للطبقة الثانية من الحماية و هي الطبقة الفيزيائية و التي تتضمن آليات و إجراءات الحماية للأبنية و البيئة المحيطة بالمستخدمين و التجهيزات الحاسوبية و ملحقاتها، و ضمان عمل الأشخاص و التجهيزات في بيئة محمية فيزيائياً.

5.4.2 الطبقة الشبكية

بعد أن تم تأمين الحماية البيئية و الفيزيائية لأماكن العمل و التجهيزات. تعتبر البنية التحتية الشبكية العصب الأساسي للعمل في أي مؤسسة لأنها الوسيلة و المعبر للوصول إلى الخدمات الالكترونية الموجودة على مخدمات المؤسسة. و بالتالي كان موقع هذه الطبقة قبل طبقة الخدمات الالكترونية – المنطقية– . و يعتبر أمن الشبكات و الذي يؤدي إلى سهولة وسرعة استخدام التجهيزات الشبكية للوصول إلى المخدمات التي تخدم المنظومات الالكترونية العاملة في المؤسسة – كالبرامج و غيرها– أهم المراحل لتسهيل العمل و ضمانه. و يمكن تشبيه هذه الطبقة بالطرق الواصلة بين المدن و داخل المدن لتسهيل وصول الناس إلى أعمالهم، فبقدر ما هي ميسرة و ذات سعات مناسبة و مراقبة من قبل الجهات المعنية، يتم الوصول الآمن و السريع لمباشرة العمل.

تتضمن هذه الطبقة أمن تجهيزات الربط الشبكي من موجهات و مبدلات و غيرها و تجهيزات الحماية الأمنية مثل Firewalls و IPS/IDS و منظومات التشفير. بما يشمل الإعدادات المفعلة على هذه التجهيزات و مراقبتها. و المسؤول عن هذه الطبقة هو فريق أمن الشبكات.

6.4.2 الطبقة المنطقية

بعد تأمين الطرق المؤدية –الشبكات– إلى التجهيزات الحاسوبية و المخدمات التي تشغل المنظومات الالكترونية العاملة في المؤسسة، نصل إلى الطبقة المنطقية التي تقدم الخدمات الالكترونية المباشرة للمستخدمين داخل المؤسسة مثل البرامج الداخلية و للمستخدمين خارج المؤسسة –الزبائن– مثل الموقع الالكتروني و الخدمات الالكترونية الموجهة لخارج المؤسسة، مثل خدمات الدفع الالكتروني و غيرها.

تتضمن هذه الطبقة كل ما يتعلق بأمن الخدمات المنطقية التي تقدمها المؤسسة من خلال المجالات التالية:

- **السياسة الأمنية Security Policy**
- **إدارة أمن الأصول المعلوماتية**
- **إدارة عمليات التشغيل**
- **التحكم بالوصول Access Control**
- **اكتساب وتطوير وصيانة أنظمة المعلومات**
- **إدارة حوادث أمن المعلومات**
- **إدارة استمرارية العمل**

و التي تضمن من خلال تطبيق المتحكمات المعرفة في كل مجال تقديم خدمات آمنة و سريعة و محمية و مراقبة. يشرف على عمل هذه الطبقة فريق أمن المعلومات.

7.4.2 الطبقة الإدارية

بعد أن تم تأمين الخدمات التي تقدمها المنظومات الالكترونية العاملة في المؤسسة نصل إلى الطبقة الأخيرة وهي الطبقة الإدارية.

تتضمن هذه الطبقة الإجراءات و البرامج الإدارية الداعمة لأمن المعلومات و الشبكات و التي يجب أن تشرف عليها و تدعمها إدارة المؤسسة بشكل مباشر. و تبدأ بتفهم الإدارة للمواضيع الخاصة بأمن المعلومات و الشبكات و الدعم المادي و المعنوي لذلك.

- **نظام إدارة أمن المعلومات**

  و هو برنامج تصادق عليه الإدارة و تتبناه، و يتضمن تعريف المسؤوليات و آليات العمل.

- **تقييم و معالجة المخاطر**

  تحديد المخاطر و تعريفها و آليات مكافحتها.

- **تنظيم أمن المعلومات**

  الآليات المتبعة للتنظيم الداخلي لأمن المؤسسة.

- **الموارد البشرية و أمن المعلومات**

  كل ما يتعلق بالعاملين في المؤسسة من إجراءات توظيف و تسريح و غيرها.

- **الامتثال**

  امتثال المؤسسة للقوانين و المعايير داخل البلدان التي تعمل بها أو المعايير الدولية الطامحة للحصول عليها لتعزيز مكانتها و اكتساب أسواق و زبائن جدد.

5.2 كيف يحقق النموذج المقترح متطلبات أمن المعلومات التقنية

يحقق النموذج المطور متطلبات أمن المعلومات التالية:

1. الفعالية Effectiveness: و تتحقق بكون المعلومات مرتبطة و مفيدة لعمل المؤسسة، و متوفرة عند الحاجة إليها و بالصيغة و الشكل المناسب للمؤسسة. و بما أن النموذج يتضمن المتحكمات الأمنية على شكل طبقات و في كل طبقة مجال/مجالات أمنية، سهل هذا الأمر تطبيق النموذج بفعالية كون كل طبقة مستقلة و يمكن التقيد بالمتحكمات الموجودة فيها أو في مجال من المجالات

ضمن الطبقة الواحدة بغض النظر عن الطبقات الأخرى. و بالتالي يمكن تقسيم الإجراءات إلى مراحل و متابعة كل مرحلة على حده.

2. الكفاءة Efficiency: الاستخدام الأمثل و في أقصى حدوده للأنظمة المعلوماتية للاستفادة القصوى من مصادر المعلومات و بشكل اقتصادي لموارد المؤسسة. و هذا ما تضمنه المتحكمات في الطبقات الخمس.
3. السرية Confidentiality: حماية المعلومات من الوصول إليها لغير المصرح لهم. تضمنه الطبقة الشبكية من استخدام التشفير و الطبقة المنطقية من التحكم بالوصول.
4. السلامة Integrity: سلامة المعلومات و دقتها. تضمنه الطبقة الشبكية من استخدام التشفير.
5. الاتاحية Availability: توفر المعلومات عند الحاجة إليها الآن و في المستقبل. و هذا ما تضمنه الطبقة المنطقية في استمرارية العمل، و الطبقة الشبكية في توافر خطوط الاتصال الاحتياطية و المعدات الشبكية الاحتياطية.
6. الامتثال Compliance: امتثال المعلومات و أنظمة المعلومات للقوانين و الأنظمة الحاكمة داخل و خارج المؤسسة. تضمنه الطبقة الإدارية.
7. الموثوقية Reliability: إمداد الإدارة بالمعلومات المناسبة التي تساعدها على اتخاذ القرارات الصائبة. و هذا ما تضمنه الطبقة المنطقية و الشبكية و البشرية في المراجعات و التقارير الأمنية و الرقابة الدائمة.

6.2 مقارنة النموذج المقترح مع المعايير ISO 27001 & 27002

يحدد المعيار ISO 27001 متطلبات تأسيس و تطبيق و مراجعة و مراقبة و تحسين توثيق نظام إدارة أمن المعلومات، في إطار سياسة المؤسسات لمعالجة المخاطر. و كل ذلك متضمن في الطبقة الإدارية، ضمن المجالين –نظام إدارة أمن المعلومات و إدارة المخاطر–.

و يحتوي المعيار ISO 27002 [ISO/IEC 27002, 2005] على 11 مجالاً أمنياً و عدداً من المتحكمات في كل مجال. و يبين الجدول 11 تضمن النموذج المقترح للمعيار ISO 27002

النموذج المقترح	ISO27002
الطبقة المنطقية و الطبقة الشبكية	السياسة الأمنية.
الطبقة المنطقية	تنظيم أمن المعلومات.
الطبقة الإدارية	إدارة الأصول.

الطبقة الإدارية	أمن الموارد البشرية.
الطبقة الفيزيائية	أمن البيئة المحيطة.
الطبقة المنطقية و الطبقة الشبكية	إدارة الاتصالات و التشغيل.
الطبقة المنطقية و الطبقة الشبكية	التحكم بالوصول للموارد.
الطبقة الإدارية	امتلاك الأنظمة المعلوماتية.
الطبقة المنطقية	إدارة حوادث أمن المعلومات.
الطبقة المنطقية	إدارة استمرارية العمل.
الطبقة الإدارية	الامتثال.

جدول 11 مقارنة بين النموذج المقترح و المعيار ISO27002

إضافة إلى شمول النموذج المقترح للمعايير ISO27001 و ISO27002. يعتبر وجود الطبقة البشرية إضافة هامة للنواحي غير المعرفة في المعايير العالمية المذكورة في مجال مكافحة الهندسة الاجتماعية. و بالتالي يقدم النموذج المقترح بنية متكاملة لتحقيق أمن المعلومات و الشبكات و الحماية المثلى للمؤسسات و خدماتها و بياناتها.

7.2 خلاصة الفصل الثاني

تضمن الفصل الثاني عرض النموذج المقترح لأمن المعلومات و الشبكات و تحليل أقسامه من الطبقات الخمس و محتوياتها من مجالات أمنية و متحكمات Security Controls. و تحليل آلية اعتماد المتحكمات. كما تم تحليل تطابق النموذج مع المعايير العالمية و متطلبات أمن المعلومات العالمية.

كما تضمن الفصل شرحاً لأهمية الهندسة الاجتماعية Social Engineering و طرق الحماية من نتائجها، و أهمية توزيع المهام الأمنية على ثلاث فرق عمل لضمان الوثوقية و السيطرة الكاملة على الحوادث الأمنية و معالجتها.

الفصل الثالث (تطبيق النموذج المقترح و القياس الرقمي)

1.3 مقدمة

نهدف في هذا الفصل إلى التحقق من فعالية النموذج المقترح، من خلال وضع آلية لتطبيقه على أرض الواقع و تقييمه من أطراف خارجية ذات علاقة بأمن المعلومات و الشبكات. بالإضافة إلى تقديم دراسة تحليلية معمقة لواقع أمن المعلومات في العينة المدروسة والخطوات الواجب اتخاذها لتحسين مستوى أمن المعلومات فيها، مما يجعل البحث ذا فائدة عملية و تطبيقية و ليس من الناحية النظرية فقط. و في سياق سعينا لتطبيق النموذج المقترح. وجدنا أنه من الأفضل القيام بما يلي:

1. طباعة النموذج المقترح على شكل وثيقة ورقية أو إلكترونية و تحويلها إلى استطلاع Survey على شكل استعلام Questionnaire. لتحديد مدى تطابق المؤسسة المدروسة مع المتحكمات الواردة في النموذج[3].
2. تطبيق الاستطلاع على عدد من المؤسسات و دراسة النتائج و تحليل الفجوة بين واقع تلك المؤسسات و النموذج المقترح و المعايير الدولية ISO 27K.
3. إعداد النتائج على شكل تقارير و تحليلها و تسليمها للمؤسسات المدروسة.

و من خلال السعي لإجراء الاستطلاع في سوريا. وجدنا الحقائق التالية:

1. لا يمكن مقارنة نتائج الاستطلاع بين مؤسسات من طبيعة عمل مختلفة و ذلك للأسباب التالية:

أ – إن ما يعتبر هاماً جداً لبعض المؤسسات، لا يشكل أهمية تذكر لمؤسسات أخرى. مثال: المؤسسات المالية التي تستخدم خدمات الدفع الالكتروني على موقعها و ما يسبب لها توقف أو تضرر الموقع الالكتروني من خسائر مادية آنية و مستقبلية بخسارة زبائنها، لا يشكل أهمية لمؤسسات أخرى لا تعتمد على خدمات الموقع الالكتروني، و لا يمثل لها الموقع الالكتروني سوى نافذة للتعرف على الشركة. مثال آخر: توقف عمل الموجه الرئيسي أو المخدم الرئيسي في المصارف – والتي تعمل في بيئة مخدمات مركزية– يعتبر أمراً كارثياً و يؤدي إلى شل خدمات المصرف بشكل كامل. أما بالنسبة لبعض المؤسسات فهذا لا يؤثر مباشرة على عملها، و لا يعتبر كارثياً، و ذلك لعدم اعتمادها على المنظومات المؤتمة بشكل أساسي.

[3] يحتوي الملحق (1) الاستطلاع الذي تم إجراءه لعدد من المؤسسات

ب –تحاول جميع المؤسسات الامتثال للقوانين المحلية، و لكنها لا تسعى بالضرورة للحصول على شهادات عالمية أو لتطبيق معايير عالمية –لا يشملها القانون الحالي– و ذلك لعدم توجهها لزبائن خارجيين أو للربط مع منظومات خارج القطر. و بالتالي لا تهتم لكثير من المجالات الموجودة في النموذج المقترح. في حين تهتم المصارف و شركات تحويل الأموال و غيرها بالمعايير العالمية لأمن المعلومات و ذلك لحاجتها للربط الشبكي مع شركات أو مصارف خارجية تتطلب هذه المعايير أو يشجع امتثال المؤسسات المحلية لهذه المعايير إمكانية التعامل معها من الخارج.

2. عدم وجود قوانين و أنظمة محلية تلزم جميع المؤسسات بمعايير وطنية لأمن المعلومات.
3. عدم إدراك إدارة معظم المؤسسات لأهمية أمن المعلومات وتخصيص دعم مادي و إداري له.
4. صعوبة التجاوب مع الاستطلاعات ذات البنود الدقيقة و المتعلقة بصلب عمل مديريات المعلوماتية و بخاصة أمن المعلومات و خصوصاً لكثرة المتحكمات و طول الاستطلاع. ونذكر هنا أننا اضطررنا لإعادة الاستطلاع عدة مرات في بعض المؤسسات و ذلك لشرح الكثير من النقاط و أهميتها، مما استغرق وقتاً طويلاً لتجميع البيانات.
5. وجدنا بأن نسبة كبيرة من مدراء المعلوماتية في المؤسسات و بخاصة الحكومية، من غير المختصين في المعلوماتية وذلك لكون الاختصاص حديثاً نسبياً في سوريا.
6. و بالنتيجة رأينا أن طريقة الاستطلاع الورقي أو الالكتروني التقليدية غير فعالة بالشكل المطلوب و يجب إيجاد طريقة أسرع و أكثر تقبلاً و فعالية.
7. ضرورة تقديم النتائج بشكل كمي –رقمي– للإشارة إلى مستوى أمن المعلومات لدى المؤسسة المدروسة و تسهيل المقارنة بين الواقع الحالي و المستوى الذي يجب أن يكون عليه ليحقق الأمان المطلوب. بالإضافة إلى فوائد القياس الكمي التي سنعرضها لاحقاً.

2.3 الآلية المتبعة لتطبيق النموذج

للأسباب السابقة و في إطار السعي لتعزيز النموذج المقترح لأمن المعلومات فقد اعتمدنا في تطبيق النموذج و التحقق من فاعليته على الخطوات التالية:

1. تطبيق الاستطلاع المطور بحسب النموذج المقترح على مؤسسات من طابع واحد. و تم اختيار المؤسسات المالية بما فيها المصارف و مؤسسات تقدم خدمات مالية. و ذلك كون هذه المؤسسات تستخدم أو تخطط لاستخدام منظومات مؤتمتة و خدمات إلكترونية و خصوصاً بعد دخول القطاع

الخاص المحلي و الأجنبي إلى السوق السورية. وكذلك ليكون تطبيق النموذج و تحليل النتائج و المقارنة ذات فائدة للبحث و للمؤسسات نفسها و للقطاع المالي في سوريا بشكل عام.

2. تطوير معادلة جديدة لقياس مستوى أمن المعلومات في أي مؤسسة بشكل عام و تطبيقه على المؤسسات المالية في سوريا.
3. اعتماد آلية تحميل Weighting كل متحكم أمني في النموذج المقترح لقيمة كمية، على مشاركة مسؤولي أمن المعلومات في المؤسسات المالية المدروسة للتقييم، بالإضافة إلى تقييمنا الخاص للمتحكم و ذلك للتأكد من فعاليته و توسيع قاعدة المشاركة في القيمة الكمية المقترحة لكل متحكم.
4. تطوير نظام مؤتمت يحتوي على النموذج المقترح و متحكماته و يعطي النتائج بحسب المعادلة المقترحة.
5. تطبيق النتائج على مؤسسة/مؤسسات مالية لم تدخل في الاستطلاع. و التأكد من النموذج المقترح و المعادلة المطورة.
6. تحليل النتائج و توثيقها في أوراق بحث و تقديمها للتحكيم في مجلات علمية محكمة للتحقق من صحة النتائج.

1.2.3 الاستطلاعات و نتائجها

يوضح الملحق (1)، الاستطلاعات التي تمت على أربع مؤسسات مالية في سورية. وقد تم تحليل نتائج هذه الاستطلاعات و تبيان نقاط التطابق و التباعد مع النموذج المقترح، بالإضافة إلى الخطوات الواجب اتخاذها من قبل المؤسسات المدروسة للتطابق مع النموذج و بالتالي مع المعايير العالمية. ومن ثم تم تسليم التقارير للمؤسسات المعنية.

و من أجل التحقق من العمل الذي تم تطويره –النموذج و الاستطلاعات المبنية عليه–، قمنا بإعداد ورقة بحث بعنوان " **تحليل الهوة القائمة بين الواقع و المعايير العالمية لأمن المعلومات في المؤسسات المالية في سورية** ". وتم قبولها للنشر في مجلة جامعة تشرين للأبحاث و الدراسات العلمية بالكتاب رقم 320 تاريخ 2011/2/20. مما يثبت أهمية و فعالية النموذج المقترح.

1.1.2.3 نتائج الاستطلاعات و التوصيات

فيما يتعلق بالنموذج المقترح، أكد جميع المشاركين في الاستطلاع أهميته و فعاليته و تضمنه لمتطلبات أمن المعلومات العالمية.

وجدنا في نهاية هذه الدراسة و التي أُعطيت نتائجها للمؤسسات المعنية, وجود هوة كبيرة – تتفاوت درجتها بين مؤسسة و أخرى– بين الواقع الملموس و متطلبات أمن المعلومات العالمية, و أن المطلوب

عمله كثير خصوصاً في غياب (أو قلة) المحددات و المعايير الوطنية من الجهات المختصة مثل المصرف المركزي ومجلس النقد و التسليف و وزارة الاتصالات و التقانة أو غيرهم من الجهات العليا ذات العلاقة.

كما وجدنا أن المواضيع الخاصة بأمن المعلومات و السياسات الأمنية تتعلق إلى حد كبير بشخص و كفاءة رأس الهرم الإداري و مدير المعلوماتية –التقنية– في تلك المؤسسات.

مع الأخذ في الاعتبار أنه لا يمكن لأي إستراتيجية معلوماتية أمنية أن تحقق مناعة تامة ضد أي هجوم، إلا أن اختيار الضوابط المناسبة و إعداد الاستجابة للحوادث والتخطيط بعناية لإدارة التغيير بصورة مسبقة وما إلى ذلك، يحمل معه المزيد من النجاح في مقاومة العاصفة الأمنية الكبيرة القادمة، وبالتالي في حماية العمل مما قد يحدث.

إن أمن المعلومات هو عملية مستمرة ، وينبغي إعادة النظر في كل بند بانتظام، وتصحيحه وربما تغييره بقدر ما تتطلب عوامل دفع العمل، تتلخص بعض التوصيات على النحو التالي :

1. لا يمكن تطبيق أمن المعلومات دون دعم الإدارة.
2. يجب معاملة أمن المعلومات في إطار حماية أصول العمل وليس كمسألة فنية فقط.
3. يعتبر توعية وتدريب الكادر من العوامل الحاسمة، وعليه فيجب على إدارة المؤسسات المالية السورية بذل كل الجهود من أجل نشر مفهوم أمن المعلومات وأهميته.
4. يتعلق نظام إدارة أمن المعلومات أساساً بتحديد نطاقه و تشخيص المفاهيم و المنهجيات و إجراءات التصحيح و التنظيم، بالإضافة إلى التوثيق والاستعراض والإشراف.
5. بدءاً من تعريف مجال أمن المعلومات، ينبغي على المؤسسات المالية السورية المضي في خطوات صغيرة ولكن مستقرة ومستمرة. ونقترح القضايا الفنية البحتة كنقطة بداية.

2.2.3 تطوير معادلة جديدة لقياس مستوى أمن المعلومات

إن السعي لتطوير معادلة جديدة لقياس أمن المعلومات في المؤسسات مبنياً على النموذج الأمني المقترح، قد أدى لفتح باب جديد للبحث عن القياس الكمي و طرقه و الأبحاث السابقة بهذا الخصوص. قبل الخوض بتطوير معادلة جديدة لقياس مستوى أمن المعلومات مبنياً على النموذج المقترح. لابد من سرد فوائد القياس الكمي لأمن المعلومات و توضيح تحليلي للدراسات السابقة في القياس الكمي.

1.2.2.3 فوائد القياس الكمي

يقدم برنامج القياس الكمي فوائد عديدة للمؤسسات و أهمها:

1. تعزيز المحاسبة Increase Accountability: يمكن لقياس أمن المعلومات تعزيز إمكانيات الإدارة لتقييم و محاسبة نظام أمن المعلومات المستخدم في المؤسسة من خلال تقييم متحكمات أمن المعلومات و تحديد الخلل فيها، كما يمكن من خلال عملية جمع المعلومات و تحليل واقع أمن المعلومات في المؤسسة تسهيل تعريف المسؤوليات و الأشخاص المسؤولين عن هذه الإجرائيات و بالتالي التحكم بها و تعديلها بما يخدم تحسين المحاسبة.
2. تحسين فاعلية نظام أمن المعلومات Improve Information Security Effectiveness: يتيح برنامج قياس أمن المعلومات للمؤسسات متابعة التطور الحاصل لنظام أمن المعلومات و الحصول على معلومات رقمية –كمية– عن تحسين قدرة النظام المعلوماتي للوصول لأهداف المؤسسة و استراتيجياتها. كما يؤمن تحديد فاعلية البرامج و الإجراءات و السياسات المطبقة في المؤسسة، و خاصة عند حصول حوادث أمنية كمحاولات الاختراق و تعطل البرامج أو انهيار التجهيزات الصلبة Hardware.
3. الامتثال Compliance: يمكن للمؤسسات التحقق من امتثال المؤسسة للقوانين و الأنظمة و القواعد التي تخضع لها المؤسسة، عن طريق تنفيذ برنامج قياس أمن المعلومات. كما يساعد البرنامج تقارير المؤسسة السنوية و مدى تطابقها مع القوانين الناظمة للرقابة الحكومية.
4. تزويد المؤسسة بدخل كمي لدعم قرارات تخصيص الموارد Resource Allocation Decisions: تجبر الضغوط المالية و شروط السوق الحكومات و المؤسسات لتخفيض ميزانياتها. و في مثل هذه البيئة، يصعب تبرير الإنفاق على أنظمة أمن المعلومات، و التي يجب أن تطرح كداعم لنظام إدارة المخاطر. و يمكن للقياس الكمي للمخاطر المساعدة في دعم القرار بتخصيص الأموال الضرورية لنظام المخاطر و أمن المعلومات.

2.2.2.3 تحليل و نقد الدراسات السابقة للقياس الكمي

قمنا في الفصل الأول بعرض الدراسات و البحوث السابقة في مجال قياس أمن المعلومات. و بعد دراسة معمقة لهذه الأبحاث نلخص هذه الأبحاث و محدوديتها لغرض بحثنا في الجدول 12.

البحث	ملخص	الفوائد/المحدودية
دليل العمل التقني لاختبار و تقييم أمن المعلومات للباحث Karen Scarfone عام 2008	تقدم ورقة البحث نموذجاً لإجراء قياس كمي لأمن المعلومات	تساهم هذه الورقة بتحديد نقاط عملية لتقييم متحكمات أمن المعلومات و لم تحدد قيم كمية أو أولوليات للقياس

Security Measurement في عام 2005 للباحث John Murdoch	نموذج يسمح بتطوير آلية عملية لقياس أمن المعلومات	من الفوائد المستقاة من الورقة السابقة هي الآلية المقترحة لتطوير القياسات و تعريف مجالات أمن المعلومات و متطلبات القياس. أما فيما يخص البحث الذي نقوم به، لم نجد قياسات عملية –كمية– مقترحة لكامل أو لجزء من دليل العمل المقترح
إطار عمل كمية لتقييم مكونات الأمن في الأنظمة المعلوماتية الموزعة. للباحث K. Bond في العام 2004	قيم الباحث معادلة سابقة للباحث Anderrson لقياس أمن المعلومات. و اقترح تطويرات عليها للأنظمة المعلوماتية الموزعة.	قدمت ورقة البحث السابقة آلية جديدة و فعالة لقياس مستوى أمن المعلومات كمياً. و عرفت بعض الخصائص الأمنية الواجب قياسها. و لكنها اقتصرت على أنظمة التشغيل الموزعة، و لم تشمل المؤسسات و الأنظمة المعلوماتية بشكل عام. كما لم تشمل الشبكات و قواعد البيانات و الأجهزة الأمنية كالجدار الناري و غيرها
أوراق البحث المنشورة من قبل المعهد الوطني للمعايير و التقانة في الولايات المتحدة NIST. و أهمها SP800-53A و SP800-55	ذكرت هذه الأوراق أهمية و فوائد القياس الكمي و مبادئه. بالإضافة إلى خطة عمل لتطوير خطة تقييم أمن المعلومات.	مفيدة في عملية تطوير نظام كمي لأمن المعلومات. و لكنها لم تذكر قياسات محددة أو معادلة للقياس

جدول 12 ملخص عن الأبحاث العالمية في مجال قياس أمن المعلومات و فوائدها و محدودياتها

3.2.3 آلية البحث المتبعة لتطوير معادلة جديدة للقياس الكمي

1. اعتماد النموذج المقترح لأمن المعلومات كأساس لبناء المعادلة الجديدة و المكون من خمس طبقات و 18 مجالاً أمنياً كما يلي:

I	Domain
1	Social Engineering Countermeasures and Policies
2	Awareness and Training Programs
3	Monitoring of Employees and Telecommunications and Unplanned Inspection
4	Intelligent Inspection
5	ISMS (information Security Management System)
6	Risk Assessment
7	Security Policy
8	Organization of Information Security
9	Network Security Administration
10	Asset Security Management
11	Human resources security
12	Physical security
13	Operations Management
14	Access Control
15	Information system acquisition, development and maintenance
16	Information security incident management
17	Business Continuity Management
18	Compliance

جدول 13 المجالات الأمنية ضمن النموذج المقترح

2. يحتوي كل مجال في الطبقة الأمنية المقابلة على مجموعة من المتحكمات، تم عرضها في الفصل السابق. و سنقوم باعتبار أن لكل مجال أمني قيمة كمية صحيحة 100، و تحميل كل متحكم ضمنه قيمة رقمية صحيحة بحيث يكون مجموع قيم المتحكمات في المجال الواحد يساوي 100.

3. حتى تكون نتائج القياس منطقية و أكثر واقعية و تعكس أهمية هذا المتحكم، قمنا بمشاركة القائمين على أمن المعلومات في المؤسسات المالية الأربع التي أجرينا عليها البحث السابق بتحديد القيمة الرقمية لكل متحكم من خلال استطلاع أجريناه معهم و هو موضح بالملحق (2).
4. اقتراح المعادلة الجديدة للقياس الكمي كما يلي:

بحيث:

- L : القيمة النهائية لمستوى أمن المعلومات في المؤسسة المدروسة
- n : عدد المجالات ضمن النموذج المقترح
- V_i : القيمة النهائية للمجال وهي مجموع قيم المتحكمات فيه، تتراوح القيمة من 0 إلى 100

$$V_i = \sum_{j=1}^{k} Cj$$

حيث Cj تمثل القيمة الرقمية لكل متحكم في المجال V_i. و عدد المتحكمات k.

- α_i : عامل يعكس أهمية المجال
- β_i : (من أجل التطوير مستقبلاً) بحيث يمكن اعتبار أهمية المجال غير خطية
- m : من أجل الحصول على قيمة نهائية لمستوى أمن المعلومات من 100 يجب التقسيم على العوامل المضافة

5. لغرض البحث اعتمدنا الفرضيات التالية:

1. We will consider $\beta_i = 1\ for\ all\ i$. β_i Could be for future development.
2. n =18, the number of domains.
3. m = $\sum_{i=1}^{18} \alpha_i$, where α_i are collected from the survey. Which reflects the importance of each domain. Table 14 shows the average values of α_i and calculation of m.

I	Domain	α_i
1	Social Engineering Countermeasures and Policies	5

2	Awareness and Training Programs	5
3	Monitoring of Employees and Telecommunications and Unplanned Inspection	4
4	Intelligent Inspection	4
5	ISMS (information Security Management System)	2
6	Risk Assessment	1
7	Security Policy	2
8	Organization of Information Security	2
9	Network Security Administration	5
10	Asset Management	2
11	Human resources security	5
12	Physical and Environmental security	4
13	Operations Management	2
14	Access Control	4
15	Information system acquisition, development and maintenance	3
16	Information security incident management	3
17	Business Continuity Management	2
18	Compliance	3

جدول 14 calculation of m

وهنا افترضنا أن أهمية المجال تقدم برقم صحيح من 1 إلى 5، بالتالي تصبح قيمة m=58.

6. و بعد اعتماد الفرضيات السابقة تصبح المعادلة:

7. للتحقق من المعادلة المطورة و تسهيل استخدامها قمنا بأتمتة المعادلة عن طريق تطوير برنامج[4] خاص يقوم بطرح المتحكمات على شكل أسئلة و من ثم احتساب النتائج باستخدام المعادلة المقترحة بعد اختصارها لتشمل 14 مجالاً من المجال 5 إلى المجال 18 في الجدول 14، و ذلك لتسهيل التنفيذ و ليشمل الطبقات الأربع في النموذج المتضمنة للمعايير ISO 27K. و بتطبيق ذلك على إحدى المؤسسات المالية من خارج المؤسسات الأربع المدروسة، و تقديم تقرير يوضح قياس مستوى أمن المعلومات لديهم في كل مجال من النموذج الأمني المقترح و المجموع العام. بالإضافة إلى

[4] يوضح الملحق 3 شرح عن البرنامج المطور

المقترحات و الآليات اللازمة لتطوير المستوى الأمني. كما طلبنا رأيهم في النتائج التي حصلنا عليها وفق المعادلة فكانت كما في الجدول 15:

Domain	Bank feedback (%)
ISMS (information Security Management System)	85
Risk Assessment	90
Security Policy	83
Organization of Information Security	88
Network Security Administration	92
Asset Management	82
Human resources security	91
Physical and Environmental security	95
Communication and Operations Management	80
Access Control	87
Information system acquisition, development and maintenance	83
Information security incident management	88
Business Continuity Management	89
Compliance	90
Average Acceptance 87%	

جدول 15 مقارنة النموذج المقترح مع عينة مدروسة

و بالتالي حصلت آلية الاحتساب المقترحة على 87% كنسبة قبول بالمقارنة مع توقعات المؤسسة المدروسة لتقييم المتحكمات و المجالات ضمن النموذج المقترح.

8. بغرض التحقق من العمل الذي قمنا به و من فعالية المعادلة و آلية القياس المقترح، قمنا بإعداد ورقة بحث باللغة الانكليزية بعنوان:

" A Novel Approach to Design Quantitative Method for ICT Security Assessment" و التي تم تقديمها لمجلة جامعة دمشق للعلوم الهندسية و تم قبولها للنشر بالكتاب رقم 20146/ص تاريخ 2011/7/6، مما يعزز النموذج المقترح و المعادلة المطورة.

3.3 خلاصة الفصل الثالث

تضمن الفصل الثالث آلية تطبيق النموذج المقترح و مبررات استخدام هذه الآلية:

1. تحويل النموذج المقترح إلى مجموعة من الاستطلاعات الورقية و تنفيذها على أربعة مؤسسات مالية في سورية.
2. دراسة نتائج هذه الدراسة و تحليل الفجوة بين واقع المؤسسات المالية و النموذج المقترح.
3. بيّنا في الفصل ضرورة تحويل الاستطلاع الورقي إلى الكتروني لتسهيل الدراسة وتسريع النتائج و استجابة الجهات المدروسة معها.
4. أشار الفصل إلى أهمية أن تكون النتائج رقمية، مما أضاف للأطروحة بعداً جديداً بدراسة آليات القياس الكمي لمستوى أمن المعلومات.
5. قدم الفصل مناقشة لعدة أوراق بحث عالمية في مجال القياس الكمي لأمن المعلومات و نقاط القوة و الضعف فيها، كما قدم شرح لأهمية القياس الكمي لأمن المعلومات و فق المراجع العالمية.
6. استنتاج معادلة جديدة للقياس الكمي لأمن المعلومات و شرح عواملها.
7. تطوير برنامج حاسوبي يؤتمت النموذج المقترح و المعادلة المبنية للقياس الكمي و تطبيقه على إحدى المؤسسات المالية خارج العينة السابقة.
8. تحليل نتائج التطبيق و مطابقها للمعايير العالمية.
9. نشر أوراق بحث تتضمن الدراسات السابقة في مجلات علمية محكمة.

الفصل الرابع (تحليل النتائج و الآفاق المستقبلية)

1.4 تحليل النتائج (خلاصة البحث)

قدم البحث نموذجاً جديداً لكافة النواحي المحيطة بأمن المعلومات و الشبكات و مكافحة الهندسة الاجتماعية و تضمن المعايير العالمية المعتمدة في هذا المجال، بالإضافة إلى دراسة جديدة لجميع نواحي الهندسة الاجتماعية التي لم تشملها المعايير العالمية. و التي تشكل خطراً حقيقياً يهدد المؤسسات التي تقدم خدمات إلكترونية و المؤسسات التي لا تقدم خدمات إلكترونية.

و يمكن تلخيص النقاط الأساسية في البحث كالتالي:

1. قدم البحث نموذجاً مقترحاً لأمن المعلومات و الشبكات مبنياً على مبدأ الطبقات ويحقق ما يلي:
   أ – تعكس كل طبقة مجموعة من المتطلبات الأساسية لأمن المعلومات و الشبكات و مكافحة الهندسة الاجتماعية المرتبطة مع بعضها لتحقق مستوى أمنياً عالياً قابلاً للتطبيق في كل طبقة أو مجال ضمن الطبقة على حده، مما يسهل تنفيذه و تحقيق الفائدة منه في تقييم مستوى أمن المعلومات و تحسين هذا المستوى.
   ب –يعكس كل مجال أمني جميع المتحكمات التي يجب توافرها و المتشابهة من حيث الطبيعة و الهدف.
   ت –اعتماد المعايير الدولية في أمن المعلومات و الشبكات في بناء النموذج المقترح و أهمها ISO27K Series.
   ث –اعتماد أوراق البحث و المعايير العالمية في بناء آليات تنفيذ المتحكمات في كل طبقة و أهمها: ISO 13335 و ISO 15408 و NIST SP800 و CobiT Framework.
   ج – تعريف جديد لآلية إدارة أمن المعلومات من خلال اعتماد ثلاث فرق عمل لإدارة كافة نواحي أمن المعلومات و الشبكات و الهندسة الاجتماعية. بما يتيح توزيع المهام و الإدارة الفعالة لأمن المعلومات.
   ح – فعالية النموذج و قابلية تنفيذه على جميع المؤسسات.
2. تطبيق النموذج المقترح على عينة من المؤسسات السورية ذات الطبيعة المتشابهة (مالية بما فيها مصارف)، و ذلك من خلال ما يلي:
   أ – إجراء استطلاعات مبنية على النموذج المقترح.
   ب –تحليل المستوى الأمني للمؤسسات المدروسة بناءً على الاستطلاعات و تحديد الهوة بين واقعها و النموذج الأمني.

ت –تحديد الإجراءات العملية لتجاوز الإشكالات المكتشفة و تحسين مستوى أمن المعلومات والشبكات للمؤسسات المدروسة.

ث –تطوير معادلة جديدة خاصة بالنموذج المقترح تهدف للقياس الكمي لمستوى أمن المعلومات و الشبكات في أي مؤسسة بشكل عام و تطبيقه على المؤسسات المالية في سورية.

ج –تطوير برنامج خاص يؤتمت المعادلة المبنية على النموذج المقترح مما يسهل تنفيذه و تعديله لاحقاً.

3. تم إعداد ورقتي بحث تشملان النموذج المقترح و الاستطلاعات و الدراسات التحليلية و النتائج، بالإضافة إلى المعادلة المقترحة، و تقديمها لمجلات علمية محكمة للتحقق من البحث بشكل عام، و من فعالية و شمول البحث للمعايير العالمية. و اعتبار قبول أوراق البحث للنشر دليلاً على نضج البحث و كفاءته.
4. تضمن البحث دراسات معمقة لواقع أمن المعلومات و الشبكات في المؤسسات المالية في سورية و شمل جميع النقاط التي تشكل عوائق أمام تطور هذا المجال في تلك المؤسسات بما فيها العوائق الاجتماعية و الإدارية و القانونية. و توضح الملاحق (أوراق البحث) هذه النقاط.
5. أكد البحث على أهمية الهندسة الاجتماعية و خطرها في أيامنا هذه و خصوصاً بعد الانتشار السريع و غير المراقب لمواقع التواصل الاجتماعي و وسائل الاتصال الحديثة، بالإضافة إلى ازدياد الاعتماد على الخدمات الالكترونية و قواعد البيانات المركزية و احتكار الدول الغربية لهذه التقنيات و استغلالها لأغراضهم الخاصة.
6. ركز البحث على أهمية الإنسان في أي منظومة عمل و ضرورة اعتباره الحلقة الأضعف في سلسلة الحماية وضرورة التوعية و المناعة الداخلية للمؤسسات.

2.4 الآفاق المستقبلية

1. يمكن تطوير النموذج المقترح من خلال تعديل الطبقات و إضافة طبقات جديدة أو مجالات ضمن الطبقات تعكس التطور التقني و الخدمات الجديدة التي ستظهر على شبكات الحواسيب.
2. تطوير النموذج ليلائم المخاطر الأمنية الجديدة و تطوير متحكمات لمكافحتها.
3. تعديل النموذج المقترح عن طريق اختصاره ليشمل مؤسسات صغيرة و بالتالي يتم اختصار المتحكمات و المجالات في طبقات النموذج.

4. تعديل أو تطوير المعادلة المقترحة للقياس الكمي بما يعكس أهمية كل طبقة أو مجال ضمن الطبقة. حيث تم اعتماد معادلة خطية و يمكن أن تطور لتكون غير خطية. مثل دراسة العامل β_i في المعادلة المقترحة.
5. استخدام المعادلة المقترحة و تطويرها لأغراض محددة مثل قياس أداء أنظمة التشغيل أو قواعد البيانات أو البرامج المطورة محلياً.
6. دراسة العوامل غير التقنية المعيقة لتطور أمن المعلومات و الشبكات في سورية من خلال اقتراحات لتطوير القوانين و الأنظمة و اعتماد التوقيع الالكتروني و الشهادات الرقمية. و تأهيل كوادر خاصة بأمن المعلومات مع برامج تدريب مستمرة لضمان كفاءة العاملين و إطلاعهم على التطورات الحاصلة في مجال أمن المعلومات و الشبكات و خصوصاً مع الازدياد السريع للخدمات الالكترونية و أتمتة الأعمال و خاصة في المؤسسات الحكومية.
7. إجراء دراسات وأبحاث خاصة بالهندسة الاجتماعية و مخاطرها و طرق مكافحتها.
8. إجراء دراسات خاصة بمواقع التواصل الاجتماعي و طرق الحماية من مخاطرها.
9. أبحاث حول سيطرة الدول المتقدمة على شبكات الانترنت و خدماتها و احتكارها لتقنيات الحماية و طرق تطوير تقنيات محلية لأمن المعلومات.

الفصل الخامس(الملاحق)

الملحق (1) الاستطلاع رقم -1-

واقع أمن المعلومات في المؤسسة المدروسة

استطلاع لتحديد درجة التقارب /التباعد عن متطلبات أمن المعلومات

للمؤسسات المالية في سورية

بإشراف: الأستاذ الدكتور غسان فلوح

المشرف المساعد: الأستاذ الدكتور نور بك باشا بن إدريس

إعداد: المهندس وسيم أحمد

Information Security in place

Questionnaire to determine how close/ far it is from Security Requirements

Introduction

Implementation of ISO Standards is demanded many requirements; in addition to a high level of auditing and checking. A new Information Security Model has been developed to asses information security. This Questionnaire built upon that model.

This report includes a wide range of questions that aim to determine gaps between ISO 27K and the organization reality, to follow systemic assessment, and to define logical objectives that well define the project scope and framework to develop a practical, systemic and scientific transformation plan.

Objectives

They could be summarized by;

1. Defining gaps;
2. Prioritizing;
3. Scoping and preparing action plan;
4. Acting in logical and real framework-basis.

Very Important

1. Top management should take this questionnaire seriously and empathize employees to answer it in a time constrain;
2. All internal parties, who are involved in IT, should participate;
3. These questions relay on ISO 27K main parts which will be under depth auditing;
4. Every single question will be targeted for farther investigation by the authorities via gathering, studying and matching random samples.
5. Please give this questionnaire the needed time and effort, be accurate as far as possible, and comment whenever it helps.

المقدمة

تفترض معايير الجودة العالمية مجموعة من المتطلبات مع آليات تدقيق وتمحيص حول مدى توافق ما هو موجود مع المعايير المطلوبة. تم تطوير نموذج لأمن المعلومات يتضمن المعايير الدولية ISO 27K series، و وضع هذا الاستطلاع بناءً على مكونات النموذج المقترح.

يحتوي هذا التقرير على مجموعة واسعة من الأسئلة تهدف إلى تحديد الفجوة بين المعايير والواقع، و إتباع منهج علمي لتقييمها، ومن ثم التحديد العقلاني لما هو قابل للوصول إلى مستوى المعايير المطلوبة وما يعتبر في المرحلة الحالية سابقاً لأوانه، مما يساعد على وضع المنظور وإطار العمل المناسبين لبناء خطة منهجية وعملية وعلمية تساعد على نقل ما تم تحديده ضمن هذا المنظور إلى مستوى معايير الجودة العالمية.

النتائج المرجوة

تتلخص أهداف هذا التقرير بالنقاط التالية:

1. تعريف الفجوة بين القائم والمطلوب.
2. تحديد أولويات البدء.
3. تحديد منظور خطة الاستعداد لتطبيق المعايير العالمية.
4. تحديد إطار العمل بصورة عقلانية وواقعية.

ملاحظات هامة جداً

1. يجب أن يساهم مدراء الصف الأول مباشرةً في الإجابة على هذا الاستطلاع وفي دعم التعاطي معه بصورة جدية وضمن إطار زمني محدد.
2. يجب أن تشارك جميع الأطراف المعنية بتكنولوجيا المعلومات في الإجابة على هذا الاستطلاع.
3. اعتمد وضع هذه الأسئلة على محاور التدقيق المطلوبة للحصول على معايير الجودة 27K.
4. كل سؤال من الأسئلة الواردة أدناه تقوم الجهة المدققة والمخولة بإعطاء شهادة الأيزو 27000 بفحصه وتمحيصه عن طريق جمع النماذج العشوائية المختلفة ودراستها ومطابقتها.
5. الرجاء إعطاء الوقت والجهد الكافيين والتزام الدقة في الإجابات، ولا بد هنا من التركيز على أهمية تسجيل كافة الملاحظات التي تنجم عن هذه الأسئلة.

Questionnaire: Implementation of Information Security

استطلاع: تطبيق أمن المعلومات

Item No.	Notes	Findings النتائج			Questions	الأسئلة
		Partially Applied	N لا	Y نعم		
			Information security management system (ISMS) 6 Controls			**نظام إدارة أمن المعلومات**
1		☐	☐	☐	Is there any evidence that management genuinely understands and supports the ISMS?	هل يوجد دلائل ملموسة تؤكد أن الإدارة حقيقةً تستوعب وتدعم هذا النظام؟
2		☐	☐	☐	Is there any exclusion from ISMS scope?	هل يوجد أية أمور مستبعدة عن نظام إدارة أمن المعلومات؟
3		☐	☐	☐	If yes; are there justified reasons for excluding any elements?	في حال الإجابة نعم، هل هنالك أسباب منطقية وراء استبعادها؟
4		☐	☐	☐	Does organization's ISM Policy adequately reflect the organization's general characteristics and its strategic risk management approach?	هل تتناسب سياسات إدارة أمن المعلومات مع المواصفات العامة للمؤسسة و إستراتيجيته في إدارة المخاطر؟
5		☐	☐	☐	Does ISM incorporate the organization's business requirements plus any legal or regulatory obligations for information security?	هل تحقق سياسات إدارة أمن المعلومات كافة متطلبات الأعمال الخاصة بالمؤسسة، إضافةً إلى أية التزامات أو تشريعات قانونية متعلقة بأمن المعلومات؟

Item No.	Notes	Findings النتائج			Questions	الأسئلة
		Partially Applied	N لا	Y نعم		
6		☐	☐	☐	Has it been formally approved by management and set meaningful criteria for evaluating information security risks?	هل تتضمن عوامل مفيدة وذات معنى لتقييم مخاطر أمن المعلومات تمت المصادقة عليها من قبل الإدارة؟
			Risk Assessment (14 Controls)			**1-تقييم المخاطر**
1		☐	☐	☐	Is there any systemic risk assessment method(s)?	هل هناك طرق منهجية متبعة لتقييم المخاطر؟
2		☐	☐	☐	Are the results of risk assessments comparable and reproducible?	هل نتائج هذا التقييم قابلة للمقارنة وإعادة الإنتاج؟
3		☐	☐	☐	Is the risk assessment method updated as a result?	هل يتم تحديث طريقة تقييم المخاطر بناءً على ما سبق؟
4		☐	☐	☐	Is the definition of criteria sensible and practicable in relation to information security risks?	هل تم تحديد العوامل الحرجة لمخاطر أمن المعلومات بشكل دقيق وقابل للتطبيق؟
5		☐	☐	☐	Are all relevant in-scope information assets included?	هل تم تضمين التقييم جميع الأصول المعلوماتية الموجودة ضمن منظور إدارة أمن المعلومات؟
6		☐	☐	☐	Are responsible owners identified for all the information assets?	هل تم تحديد الأطراف المسؤولة (المالكة) عن الأصول المعلوماتية؟
7		☐	☐	☐	Is there an adequate analysis/evaluation of threats?	هل يوجد تحليل وتقييم كافٍ للتهديدات؟

Item No.	Notes	Findings النتائج			Questions	الأسئلة
		Partially Applied	N لا	Y نعم		
8		☐	☐	☐	Is there an adequate analysis/evaluation of vulnerabilities and impacts?	هل يوجد تحليل وتقييم كافي للثغرات وتأثيرها؟
9		☐	☐	☐	Is there an adequate documentation of risk scenarios plus the prioritization or ranking of risks?	هل يوجد توثيق كافٍ لمختلف احتمالات المخاطر مع مراتب أو أولويات لها؟
			Risk Treatment Plan			**1-1-خطة معالجة المخاطر**
10		☐	☐	☐	Are appropriate "treatments" specified for all identified risks?	هل تم توصيف علاج مناسب لكافة المخاطر المعرفة؟
11		☐	☐	☐	Are changes suitably fitted in the plan?	هل يتم وضع التغييرات ضمن الخطة؟
12		☐	☐	☐	Is the Risk Treatment Plan being used and updated proactively as an information security management tool?	هل تم استخدام وتحديث خطة معالجة المخاطر بصورة استباقية فعالة كأدة لإدارة أمن المعلومات؟
13		☐	☐	☐	Are defined controls objectives and selected controls satisfied?	هل تعتبر أهداف التحكم وأنواع التحكم المعرفة على مستوى جيد؟

Item No.	Notes	Findings النتائج			Questions	الأسئلة
		Partially Applied	N لا	Y نعم		
14		☐	☐	☐	Is the organization effectively and proactively reviewing the implementation of the ISMS to ensure that the security controls identified in the Risk Treatment Plan, policies, etc. are actually implemented and are in fact in operation?	هل تقوم المؤسسة بمراجعة فعالة ووقائية لآلية تطبيق نظام إدارة أمن المعلومات للتأكد من أن طرق التحكم الأمنية المعرفة في خطة معالجة المخاطر والسياسات و...الخ، مطبقة حقاً وهي تعمل؟
			Management responsibility (9 Controls)			**2-مسؤولية الإدارة**
1		☐	☐	☐	Are there enough resources allocated to the ISMS in terms of budget, manpower etc?	هل هنالك موارد كافية مخصصة لنظام إدارة المعلومات من حيث الميزانية، القوة العاملة...الخ؟
2		☐	☐	☐	Are sufficient funds allocated by management to address information security issues in a reasonable timescale and to a suitable level of quality?	هل خصصت الإدارة تمويلاً كافياً من أجل مواجهة ومعالجة قضايا أمن المعلومات ضمن حدود الوقت والجودة المطلوبين؟
3		☐	☐	☐	Do the top managers seriously commit to information security in their behavior?	هل يلتزم المدراء حقيقةً بأمن المعلومات من خلال مسلكيتهم؟

Item No.	Notes	Findings النتائج			Questions	الأسئلة
		Partially Applied	N لا	Y نعم		
4		☐	☐	☐	Are necessary competencies and training/awareness requirements for information security professionals and others with specific roles and responsibilities explicitly identified?	هل تم التعريف الواضح بمتطلبات المهارة والتدريب والتوعية الضرورية لاختصاصيي أمن المعلومات وغيرهم مع تحديد الأدوار والمسؤوليات؟
5		☐	☐	☐	Is there a scheduled reviewing, at last once a year?	هل هنالك جدولة محددة للقيام بالمراجعة، مرة سنوياً على الأقل؟
6		☐	☐	☐	Does management play an active part and is fully engaged in the review/s?	هل تلعب الإدارة دوراً فعالاً وحقيقياً الاهتمام في عمليات المراجعة؟
			Internal ISMS audits			**2-1-فحص نظام إدارة أمن المعلومات داخلياً**
7		☐	☐	☐	Is there any internal audits plan?	هل هنالك أي خطط داخلية لفحص إدارة أمن المعلومات؟
8		☐	☐	☐	If yes, are responsibilities for conducting ISMS internal audits formally assigned to competent, adequately trained IT auditors?	في حال كان الجواب نعم، هل مسؤوليات إدارة عملية الفحص الداخلية موكلة رسمياً إلى مدققي تكنولوجيا معلومات مدربين ومختصين في ذلك؟
9		☐	☐	☐	Does ISMS changes in response to the identification of significantly changed risks?	هل يستجيب نظام إدارة أمن المعلومات إلى المخاطر المعرفة والمتغيرة بصورة ملحوظة؟

Item No.	Notes	Findings النتائج			Questions	الأسئلة
		Partially Applied	N لا	Y نعم		
			Information security policy (15 Controls)			**3- سياسات أمن المعلومات**
1		☐	☐	☐	Are the policies communicated, understood and accepted? • Standards for physical security of the computer and telecommunications installation and associated facilities; • HR procedures governing access to and use of IT services (usernames and passwords, disciplinary procedures); • End user guidelines covering PC software licensing and virus prevention, etc?	هل يتم تبادل وفهم وقبول السياسات المتعلقة؟ • معايير الأمن المادية للحواسب والاتصالات وكافة ملحقاتها. • الإجراءات الخاصة بالموارد البشرية والمتعلقة بالتحكم في الدخول إلى واستخدام خدمات تكنولوجيا المعلومات (أسماء مستخدمين وكلمات عبور، إجراءات تأديبية ...الخ). • إرشادات للمستخدمين تتعلق بقضايا تراخيص برامج الحواسب، صد الفيروسات ...إلخ).
2		☐	☐	☐	Are they reasonable and workable?	هل هذه السياسات منطقية وقابلة للتطبيق؟
3		☐	☐	☐	Do they incorporate suitable and sufficient controls?	هل تتكامل هذه السياسات مع أدوات تحكم مناسبة وكفء؟

Item No.	Notes	Findings النتائج			Questions	الأسئلة
		Partially Applied	N لا	Y نعم		
4		☐	☐	☐	Do they cover all essential computing and telecommunication services?	هل تغطي هذه السياسات جميع الجوانب الأساسية المتعلقة بالحواسب والاتصالات؟
			Internal Responsibilities and Communications			**3-1-المسؤوليات الداخلية وآليات التواصل**
5		☐	☐ ☐ ☐ ☐ ☐	☐ ☐ ☐ ☐ ☐	Are the following positions well defined and activated: • Senior manager responsible for IT and ISM; • Information security professionals; Security administrators; • Site/physical security manager and Facilities contacts; • HR contact for HR matters such as disciplinary action and training; • Systems and network managers, security architects and other IT professionals.	هل تم تعريف وتفعيل دور المناصب التالية: • مدير من الصف الأول مسؤول عن تكنولوجيا المعلومات وإدارة أمنها. • أخصائيو أمن معلومات، مدراء أنظمة معلومات. • مدير أمن للشؤون المادية في الموقع وأعضاء ارتباط المرافق. • عضو ارتباط الموارد البشرية من أجل الأمور المتعلقة مثل الأفعال التأديبية والتدريب. • مدراء أنظمة وشبكات، تصميم الهيكل الأمني، وغيرهم من أخصائيي تكنولوجيا المعلومات.
6		☐	☐	☐	Is ISM given sufficient emphasis (is there a 'driving force'?) and management support?	هل تعطي الإدارة دفعاً (قوة دفع) ودعماً قوياً لإدارة أمن المعلومات؟

Item No.	Notes	Findings النتائج			Questions	الأسئلة
		Partially Applied	N لا	Y نعم		
7		☐	☐	☐	Is there a senior management forum to discuss ISM policies, risks and issues?	هل هنالك منتدى خاص لمناقشة سياسات إدارة أمن المعلومات والمخاطر وغيرها من القضايا المتعلقة مكون من مدراء الصف الأول؟
8		☐	☐	☐	Are roles and responsibilities clearly defined and assigned to skilled individuals?	هل تم تعريف الأدوار والمسؤوليات بوضوح وتعيين الأفراد المؤهلين للقيام بها؟
9		☐	☐	☐	Is there sufficient co-ordination within the BU (business unit), between BUs and with HQ?	هل هنالك تنسيق وتعاون كافٍ على مستوى الوحدة الاقتصادية، الوحدات فيما بينها، ومع المقر الرئيسي أيضاً؟
10		☐	☐	☐	Are the information flows (like incident reporting) operating effectively in practice?	هل تعتبر عملية تدفق المعلومات (مثلاً رفع تقارير الحوادث) فعالة على أرض الواقع؟
			External Parties			**3-2-الأطراف المعنية الخارجية**
11		☐	☐	☐	Is there a risk analysis process in place for 3rd -party communications and connections?	هل يتم تضمين الاتصالات والتواصل التابعة للأطراف المعنية في العقود بصورة غير مباشرة (الطرف الثالث) ضمن عملية تحليل المخاطر؟
12		☐	☐	☐	Is there any individual who has responsibility for ensuring that all 3-party links are in fact identified and risk assessed?	هل هنالك أي فرد مسؤول عن ضمان أن كافة الروابط مع الأطراف الثالثة المعنية قد تم تعريفها وتقييم المخاطر المتعلقة بها؟
13		☐	☐	☐	Are ISM arrangements in operation on 3-party connections routinely reviewed against the requirements?	هل من ترتيبات لإدارة أمن المعلومات على أرض الواقع تراجع بانتظام طرق الاتصال مع الأطراف الثالثة وتقارنها مع المتطلبات؟

Item No.	Notes	Findings النتائج			Questions	الأسئلة
		Partially Applied	N لا	Y نعم		
14		☐	☐ ☐ ☐ ☐ ☐	☐ ☐ ☐ ☐ ☐	Are there formal contracts covering 3rd party links? • Ownership and responsibility for ISM issues? • Legal requirements? • Protection of systems, networks and data via physical, logical and the right of audit by the organization? • Procedural controls business assets, availability of services in the event of disasters, management notification for security incidents? • Security clearance of staff?	هل هنالك عقود رسمية تغطي الروابط مع الأطراف الثالثة: • ملكية ومسؤولية المسائل المتعلقة بإدارة أمن المعلومات؟ • المتطلبات القانونية؟ • حماية الأنظمة والشبكات والمعطيات من الناحية المنطقية والمادية وحق المؤسسة بالتدقيق عليها؟ • إجراءات التحكم المتعلقة بالأصول، ومدى إتاحية الخدمات في حالة الكوارث، وطرق إعلام الإدارة بالحوادث الأمنية؟ • قيام كادر الطرف الثالث بالتصريح الأمني رسمياً؟
15		☐	☐	☐	Does the outsourcing contract adequately address the previous issues?	هل عقود نقل الأعمال لأطراف خارجية تتضمن القضايا السابقة بشكل وافٍ؟
			Information Asset Management (7 Controls)			**4-إدارة الأصول المعلوماتية**
1		☐	☐	☐	Are there any arrangements to establish and maintain an inventory of information assets?	هل هنالك أية ترتيبات تتعلق بإنشاء وصيانة مخزن الأصول المعلوماتية؟

Item No.	Notes	Findings النتائج			Questions	الأسئلة
		Partially Applied	N لا	Y نعم		
2		☐	☐	☐	Is there a 'registration process' for new application systems?	هل هنالك قوانين تحكم تطبيق الأنظمة الجديدة؟
3		☐	☐	☐	Are there asset tags on all PCs, network equipment, etc?	هل هنالك بطاقة تعريف الأصل المعلوماتي على كل حاسب و تجهيزة شبكية...الخ؟
4		☐	☐	☐	Are power and data cables clearly labeled and are wiring diagrams kept complete and up-to-date?	هل جميع كبلات الكهرباء والبيانات معنونة بوضوح، وجميع مخططات الأسلاك محفوظة بالكامل وبأحدث نسخها؟
5		☐	☐	☐	Is Information classification in place, covering business requirements for confidentiality, integrity and availability	هل يشتمل تصنيف المعلومات القائم على متطلبات الأعمال من أجل السرية والصحة والإتاحية؟
6		☐	☐	☐	Are appropriate markings used on documents, forms, reports, screens, backup media, emails, file transfers?	هل تستخدم تأشيرات مناسبة في الوثائق والصيغ والتقارير والشارات و وسائط النسخ الاحتياطي ونقل الملفات؟
7		☐	☐	☐	Is staff made aware of the corresponding security requirements for handling sensitive materials?	هل يعي الكادر متطلبات الأمن المقابلة لتدابير المواد الحساسة؟
			Human Resources Security (5 Controls)			**5-متطلبات الأمن من جهة الموارد البشرية**

Item No.	Notes	Findings النتائج			Questions	الأسئلة
		Partially Applied	N لا	Y نعم		
1		☐	☐	☐	Are information security roles, disciplinary actions and responsibilities defined in job descriptions, terms and conditions of employment etc. for specific IT security staff, system/network managers, managers and end users in general?	هل وظائف أمن المعلومات والأفعال التأديبية والمسؤوليات معرفة بصورة واضحة في التوصيف الوظيفي و وبنود وشروط التوظيف...الخ، بالنسبة للكادر الخاص بأمن المعلومات ومدراء الشبكات/الأنظمة، والمدراء والمستخدمين بصورة عامة؟
2		☐	☐	☐	Are there appropriate HR policies and procedures that transgress IT security rules?	هل هنالك سياسات وإجراءات مناسبة للموارد البشرية حين انتهاك مبادئ أمن تكنولوجيا المعلومات؟
3		☐	☐	☐	Are there enhanced screening processes for staff/managers in particularly sensitive roles or sites?	هل هنالك عمليات اختيار معمقة من أجل الكادر/ المدراء وتحديداً للأدوار أو المواقع الحساسة؟
4		☐	☐	☐	Do end staff and their managers routinely receive appropriate training on information security including roles and responsibilities, login procedures etc., within the context of general IT systems training?	هل يتلقى الكوادر ومدرائهم بانتظام تدريباً مناسباً على أمن المعلومات بما في ذلك الوظائف والمسؤوليات، إجراءات الدخول ...إلخ متضمناً في مجرى التدريب العام على أنظمة تكنولوجيا المعلومات؟
5		☐	☐	☐	Are there any procedures and/or guidelines relating to information security elements in the cases of termination or change of employment?	هل هنالك أية إجراءات أو/و إرشادات تتعلق بعناصر أمن المعلومات في حالات من مثل ترك العمل أو تغيير التوظيف؟

Item No.	Notes	Findings النتائج			Questions	الأسئلة
		Partially Applied	N لا	Y نعم		
			Physical and Environmental Security (23 Controls)			**6-متطلبات الأمن من الناحية البيئية والمادية**
1		☐	☐	☐	Are discreet facilities sited to minimize disaster potential or cost of protective countermeasures?	هل تم وضع وسائل حكيمة لتقليل احتمالات الكوارث أو تكاليف الحلول الوقائية؟
2		☐	☐	☐	Is the construction physically sound e.g. walls go "slab-to-slab", thick solid doors, etc?	هل البناء يوحي بالأمن من الناحية المادية، مثلاً جدران متراصفة، أبواب سميكة صلبة ...الخ؟
3		☐	☐	☐	Are suitable access control systems employed with matching procedures?	هل تطبق أنظمة مناسبة للتحكم بالدخول والإجراءات المقابلة لها؟
4		☐	☐	☐	Is there appropriate physical protection for external cables, junction boxes, air conditioner chillers, microwave dishes, air inlets etc. against accidental damage or deliberate interference?	هل هنالك إجراءات حماية مادية مناسبة للكبلات الخارجية، علب القواطع، مبرد المكيفات، اللواقط، مداخل التهوية...الخ ضد الأضرار غير المتعمدة أو الدخول عنوة؟
5		☐	☐	☐	Is there any protection/control of fire and smoke, e.g. fire-resistant/low-smoke construction materials, wiring, etc?	هل هناك أية وسائل حماية/ تحكم تتعلق بالحرائق أو الدخان مثل الأسلاك ومواد البناء المقاومة للحريق/ قليلة إصدار الدخان؟
6		☐	☐	☐	Is there any evidence of smoking?	هل يوجد تدخين في المكان؟
7		☐	☐	☐	Are no-smoking signs displayed?	هل توضع إشارات عدم التدخين بوضوح؟

Item No.	Notes	Findings النتائج			Questions	الأسئلة
		Partially Applied	N لا	Y نعم		
8		☐	☐	☐	Are fire systems and interlocks regularly inspected and maintained inspections by professionals?	هل يتم فحص وصيانة أنظمة الإنذار ضد الحرائق والقفل بصورة منتظمة من قبل أخصائيين؟
9		☐	☐	☐	Is there enough awareness of fire evacuation procedures?	هل يوجد توعية كافية حول إجراءات الإخلاء عند حدوث الحريق؟
10		☐	☐	☐	Is there an adequate UPS capacity to support all essential computer equipment and peripherals, and all such equipment?	هل هنالك ما يكفي من وحدات عدم انقطاع التيار الكهربائي تغطي سعاتها كافة التجهيزات الحاسوبية الأساسية والمحيطية وتفرعاتها؟
11		☐	☐	☐	Is there an adequate Back-up generator capacity?	هل هنالك مولدة كهربائية احتياطية ذات سعة كافية؟
12		☐	☐	☐	Is there adequate A/C capacity to support heat load?	هل هنالك طاقة تبريدية كافية لمعالجة الحمل الحراري؟
13		☐	☐	☐	Are there adequate redundant/spare units or portables available to improve resilience and permit maintenance without affecting service?	هل هنالك ما يكفي من القطع الاحتياطية أو المحمولة المتاحة لدعم المرونة والصيانة الدورية دون تأثر الخدمة؟
14		☐	☐	☐	Is temperature sensing with remote-reading over-temperature alarms and incident procedures available?	هل تتوفر حساسات حرارية تدعم القراءة من بعيد وإنذارات زيادة درجة الحرارة إضافةً إلى إجراءات الطوارئ؟
15		☐	☐	☐	Is water/flood protection with detection and remote alarms applied?	هل يوجد نظام منع وكشف وإنذار بعيد حول تسرب المياه وطوفانها؟

Item No.	Notes	Findings النتائج			Questions	الأسئلة
		Partially Applied	N لا	Y نعم		
16		☐	☐	☐	Are computer and telecommunications rooms maintained in clean condition?	هل يتم المحافظة على شروط نظافة غرف التجهيزات و الاتصالات؟
17		☐	☐	☐	Is there a special treatment for dust avoidance?	هل توجد معالجة خاصة لتجنب الغبار؟
18		☐	☐	☐	Is all exposed metalwork earth bonded to a common safety earth point for both safety and static reduction reasons?	هل تم تثبيت كافة الهياكل المعدنية الكشوفة وربطها إلى نقطة تأريض لأغراض السلامة وتقليل الكهرباء الساكنة؟
19		☐	☐	☐	Are lightning conductors, cable isolators, and fuses etc, mounted where applicable?	هل تم رفع كافة قواطع الإضاءة، عوازل الكبلات، قواطع الطاقة الكهربائية ...إلخ حين توفر الإمكانية؟
20		☐	☐	☐	Are all physical equipments operated and maintained as per manufacturer's specifications and tested on-load regularly?	هل يتم تشغبل وصيانة كافة التجهيزات المادية واختبارها تحت الحمل على أساس المواصفات الفنية التي حددتها الجهة الصانعة؟
21		☐	☐	☐	Are all physical controls following major changes?	هل تتبع كافة وسائل التحكم المادية التغيرات الكبيرة؟
22		☐	☐	☐	Is there any management authorization process for removal of information assets from site?	هل يوجد عملية مصرحة إدارياً لزوم إزالة الأصول المعلوماتية من موقع ما؟

Item No.	Notes	Findings النتائج			Questions	الأسئلة
		Partially Applied	N لا	Y نعم		
23		☐	☐	☐	Are there any secure disposal processes to erase sensitive corporate and personal site data fully from removable or fixed media before disposal?	هل هنالك أية عمليات آمنة من أجل مسح البيانات الحساسة والشخصية كاملةً من وسائط التخزين الثابتة أو القابلة للإزالة قبل التصرف بها؟
			Communications and Operations Management (31 Controls)			**7-إدارة عمليات التشغيل والاتصالات**
1		☐	☐	☐	Is there a full set of security procedures in place relating to general IT operations?	هل يوجد في واقع الحال مجموعة كاملة من إجراءات الأمن المتعلقة بعمليات تشغيل تكنولوجيا المعلومات عموماً؟
2		☐	☐	☐	Is there a full set of security procedures in place relating to systems and network management?	هل يوجد في واقع الحال مجموعة كاملة من إجراءات الأمن المتعلقة بإدارة الأنظمة والشبكة؟
3		☐	☐	☐	Is there a full set of security procedures in place relating to incident management?	هل يوجد في واقع الحال مجموعة كاملة من إجراءات الأمن المتعلقة بإدارة الحوادث؟
4		☐	☐	☐	Is there a full set of security procedures in place relating to IT security admin?	هل يوجد في واقع الحال مجموعة كاملة من إجراءات الأمن المتعلقة بإدارة أمن تكنولوجيا المعلومات؟
5		☐	☐	☐	Is there a full set of security procedures in place relating to change management?	هل يوجد في واقع الحال مجموعة كاملة من إجراءات الأمن المتعلقة بإدارة التغيير؟
6		☐	☐	☐	Are the previous procedures reasonably well controlled?	هل يتم التحكم بالإجراءات السابقة بصورة جيدة من الناحية المنطقية؟

Item No.	Notes	Findings النتائج			Questions	الأسئلة
		Partially Applied	N لا	Y نعم		
7		☐	☐	☐	Are corresponding responsibilities assigned to individuals?	هل يتم تكليف الأفراد بمسؤوليات متناسبة معهم؟
8		☐	☐	☐	Are there acceptance tests and capacity planning including CPU usage, disk space, network capacity, etc?	هل يوجد اختبارات قبول وتخطيط للسعات يتضمن استخدام /مشغولية المعالج، حجم القرص، سعة الشبكة ...الخ.
9		☐	☐	☐	Are acceptance tests completed prior to the introduction of new systems onto the network?	هل تجرى كامل اختبارات القبول قبل استقدام أنظمة جديدة إلى الشبكة؟
10		☐	☐	☐	Are fallback arrangements updated to reflect new/retired systems?	هل يتم تحديث إجراءات الاستعادة حتى تستوعب الأنظمة الجديدة والمتقادمة؟
11		☐	☐	☐	Are there continuous/frequent virus-checks on all PCs including standalones/portables?	هل يتم باستمرار وضمن تواتر معين فحص الحواسب القائمة بذاتها منها والمحمولة ضد الفيروسات؟
12		☐	☐	☐	Are infection levels minimized (is the situation broadly under control)?	هل تم تخفيض مستويات الإصابة للحدود الدنيا (هل الوضع تحت السيطرة شبه التامة)؟
13		☐	☐	☐	Are staff and managers aware of the protection against malicious and mobile code procedures?	هل يمتلك المدراء والكادر معرفةً حول إجراءات الحماية من البرامج الخبيثة والنقالة؟
14		☐	☐	☐	Is there a sufficient protection against Trojans, worms, spyware, rootkits, etc?	هل يوجد حماية كافية ضد الهجمات مثل أحصنة طروادة، الديدان، البرامج التجسسية، البرامج المتطفلة ...الخ؟

Item No.	Notes	Findings النتائج			Questions	الأسئلة
		Partially Applied	N لا	Y نعم		
15		☐	☐	☐	Are backup strategies and procedures documented and tested?	هل تم توثيق وتجريب استراتيجيات وإجراءات النسخ الاحتياطي؟
16		☐	☐	☐	Do these strategies cover data, programs, system files, parameter files, etc, for all systems including servers, desktops, phone/network systems, system/network management systems, standalone/portable systems, control systems, etc?	هل تغطي هذه الاستراتيجيات البيانات، البرامج، ملفات النظام، ملفات البارامترات ...الخ لكامل الأنظمة بما فيها المخدمات، الحواسب، أنظمة الهاتف وشبكته، أنظمة إدارة الشبكات والنظم، الأنظمة القائمة بذاتها والمحمولة، أنظمة التحكم ...الخ؟
17		☐	☐	☐	Are backup frequencies and types appropriate?	هل يعتبر تواتر ونوع النسخ الاحتياطي مناسباً؟
18		☐	☐	☐	Are backup media protected against loss, theft, damage, fire including both on-site and off-site/remote storage?	هل وسائط النسخ الاحتياطي محمية ضد الفقد، السرقة، الضرر، الحرائق بحالتي التخزين محلياً أو في مكان آخر؟
19		☐	☐	☐	Do all backup media listed in the procedures/records actually exist?	هل جميع وسائط النسخ الاحتياطي المدونة في الإجراءات والسجلات موجودة حقاً؟
20		☐	☐	☐	Are security elements of network management procedures properly documented?	هل تم توثيق إجراءات إدارة الشبكة المتعلقة بعناصر الأمن؟

Item No.	Notes	Findings النتائج			Questions	الأسئلة
		Partially Applied	N لا	Y نعم		
21		☐	☐	☐	Are information security aspects such as security arrangements for 3rd-party connections adequately covered?	هل تم تغطية الأوجه المختلفة لأمن المعلومات مثل الترتيبات الأمنية للاتصال مع الطرف الثالث بصورة كافية؟
22		☐	☐	☐	Is there an up-to-date and complete asset register for tapes, removable disks, CDs etc?	هل هنالك تسجيل محدث وكامل لكل أشرطة النسخ الاحتياطي، الأقراص القابلة للإزالة، الأقراص الممغنطة الخ؟...
23		☐	☐	☐	Are archival media duplicated and verified prior to deletion of source data?	هل يتم التأكد من وجود نسختين مؤرشفتين من البيانات قبل محي النسخة الأصلية؟
24		☐	☐	☐	Are archive tapes periodically verified and re-tensioned?	هل يتم التحقق وإعادة شد الأشرطة المؤرشفة خلال تواتر زمني معين؟
25		☐	☐	☐	Are there appropriate controls to maintain confidentiality of stored data?	هل يتم الحفاظ على سرية البيانات المخزنة بوسائل تحكم مناسبة؟
26		☐	☐	☐	Are there suitable security controls for exchange of information?	هل يوجد وسائل تحكم أمنية مناسبة لتبادل المعلومات؟
27		☐	☐	☐	Are there any security arrangements for Internet, Intranet and related systems?	هل يوجد ترتيبات أمنية مناسبة من أجل الإنترنت و الإنترنت والأنظمة المتعلقة؟
28		☐	☐	☐	While using or providing Web-based applications; is there an enforced use of https, for example, to protect sensitive data en route between browser and Web server?	هل يتم مثلاً إلزام استخدام بروتوكول التصفح المشفر https عند استخدام أو توفير التطبيقات العاملة على أساس الويب وذلك لحماية البيانات الحساسة حين توجيهها بين المتصفح ومخدم الويب؟

Item No.	Notes	Findings النتائج			Questions	الأسئلة
		Partially Applied	N لا	Y نعم		
29		☐	☐	☐	Are main systems monitored for logging and reporting security incidents?	هل يتم مراقبة الدخول على الأنظمة الرئيسية ورفع تقارير الحوادث الأمنية؟
30		☐	☐	☐	Is there a process in place for reviewing and responding appropriately to internal or external security alerts?	هل توجد عملية قائمة تتعلق بالمراجعة والاستجابة المناسبة للإنذارات الأمنية الداخلي منها والخارجي؟
31		☐	☐	☐	Are the logs and reports followed-up with principles of responsibility and accountability?	هل تتم متابعة ملفات الدخول والتقارير باعتماد مبادئ المسؤولية والمحاسبة؟
			Access control (14 Controls)			**8-التحكم بالوصول والدخول**
1		☐	☐	☐	Are business requirements for access control properly documented and approved by information asset owners?	هل تم التصديق والتوثيق الجيد لمتطلبات الأعمال المتعلقة بالتحكم بالدخول من قبل مالكي (المسؤولين عن) الأصول المعلوماتية؟
2		☐	☐	☐	Are business requirements for access control (for breadth and depth of coverage) properly included in system security design specifications?	هل تم التضمين الجيد لمتطلبات الأعمال من أجل التحكم بالدخول (تغطية أفقية وعمودية) في المواصفات الفنية الخاصة بتصميم نظام الأمن؟
3		☐	☐	☐	Are access rights normally limited as far as practicable?	هل عادةً ما تكون حقوق الدخول محدودة قدر المستطاع؟

Item No.	Notes	Findings النتائج			Questions	الأسئلة
		Partially Applied	N لا	Y نعم		
4		☐	☐	☐	Are access rights regularly reviewed and modified as far as needed?	هل تتم مراجعة وتعديل حقوق الدخول بانتظام حسب الحاجة؟
5		☐	☐	☐	Is management pay special attention to access/account controls for the users of privileged system-, database- application- & network-managers?	هل تولي الإدارة اهتماماً خاصاً لوسائل التحكم في الدخول/ الحسابات المتعلقة بمستخدمي النظام، قواعد البيانات، التطبيقات ذوي الامتيازات (كامل السماحيات) ومدراء الشبكات؟
6		☐	☐	☐	Does the organization suffer from abuse of privileges? Is this case classified as a great potential?	هل تعاني المؤسسة من إساءة استخدام تلك الامتيازات؟ هل تصنف هذه الحالة ضمن الاحتمالات العالية؟
7		☐	☐	☐	Does the organization have password controls?	هل تمتلك المؤسسة وسائل التحكم بكلمات المرور؟
8		☐	☐	☐	Does anyone routinely check for weak passwords and follow-up with user security awareness/training?	هل يتابع أي فرد بانتظام التدقيق لكشف كلمات العبور الضعيفة وتوعية /تدريب المستخدم أمنياً؟
9		☐	☐	☐	Do authorized individuals effectively limit access to applications/services?	هل يقوم الأفراد المخولون بحد الدخول إلى التطبيقات /الخدمات بفاعلية؟
10		☐	☐	☐	Are network nodes authenticated and established distinct security domains using firewalls, key lock-out, etc?	هل تقوم العقد الشبكية بالتحقق وتأسيس مناطق أمنية مختلفة باستخدام جدران الحماية، منع الدخول ...الخ؟
11		☐	☐	☐	Are session timeouts implemented on the desktop, network, application or operating system levels?	هل تطبق تقنية إلغاء الجلسة بسبب نفاذ الوقت على الحواسب، الشبكات، التطبيقات، أنظمة التشغيل؟

Item No.	Notes	Findings النتائج			Questions	الأسئلة
		Partially Applied	N لا	Y نعم		
12		☐	☐	☐	Are suitable access controls in place, including the use of individual user identities, user authentication, automated access controls, encryption, etc?	هل توجد وسائل تحكم بالدخول مناسبة، من ضمنها مثلاً استخدام بطاقات التعريف، التحقق من المستخدم، الوسائل المؤتمتة، التشفير ...الخ؟
13		☐	☐	☐	Are there any security controls relating to mobile, home users (remote access), laptops, mobile storage devices, VPNs, etc?	هل توجد وسائل تحكم أمنية متعلقة بالجوال، المستخدمين المنزليين (الدخول البعيد)، الحواسب النقالة، وسائل التخزين المتحركة، الشبكات الافتراضية الخاصة ...الخ؟
14		☐	☐	☐	Are portable systems maintained and controlled?	هل يتم الحفاظ على والتحكم بالأنظمة المحمولة؟
	IS acquisition, development and maintenance (13 controls)					**9-اكتساب، إعداد، صيانة أنظمة المعلومات**
1		☐	☐	☐	Do changes trigger security reviews/risk assessments and, if necessary, re-certification of systems?	هل تستدعي التغيرات القيام بمراجعة أمنية /تقييم المخاطر وحتى إعادة ترخيص الأنظمة في حال الحاجة؟
2		☐	☐	☐	Are formal systemic methods used routinely?	هل يتم استخدام طرق رسمية منهجية بانتظام؟
3		☐	☐	☐	Are data controls such as input data validation, processing validation, encryption, message authentication etc, employed appropriately?	هل تطبق وسائل تحكم مناسبة من أجل البيانات مثل التحقق من صلاحية المدخلات والمعالجة، التشفير، رسالة التحقق ...الخ؟

Item No.	Notes	Findings النتائج			Questions	الأسئلة
		Partially Applied	N لا	Y نعم		
4		☐	☐	☐	Has a formal policy covering the use of cryptographic controls been implemented?	هل تم تطبيق سياسات رسمية تعنى باستخدام وسائل التحكم السرية؟
5		☐	☐ ☐ ☐ ☐ ☐	☐ ☐ ☐ ☐ ☐	If yes, is it covers: • The general principles under which business information should be protected; • Standards to be applied for the effective implementation of crypto; • A process to determine the level of protection to be applied; • Management of crypto keys, including recovery of information in the event of lost, damaged or compromised keys; • Alignment with any documented requirements.	في حال كانت الإجابة نعم، هل تشمل: • أي من معلومات الأعمال تستوجب حمايتها حسب المبادئ العامة. • المعايير الواجبة التطبيق لضمان فعالية تنفيذ وسائل التحكم السرية. • القيام بتحديد مستوى الحماية الواجب تطبيقه. • إدارة مفاتيح السرية بما فيها استرجاع المعلومات في حال ضياع أو تضرر أو انكشاف المفاتيح. • التماشي مع أية متطلبات موثقة.
6		☐	☐	☐	Are there adequate controls isolating development from testing from production environments?	هل توجد وسائل تحكم كافية لعزل بيئة التطوير عن التجريب عن الإنتاج؟

Item No.	Notes	Findings النتائج			Questions	الأسئلة
		Partially Applied	N لا	Y نعم		
7		☐	☐	☐	Are changes acceptances built on professional ensuring that new/changed cases do not disrupt other operations?	هل يستند قبول التغييرات على تأكيد المختصين أن التغيرات/ التجديدات لا تعطل العمليات التشغيلية الأخرى؟
8		☐	☐	☐	Are changes properly documented, justified and authorized by management?	هل يتم توثيق التغيرات وذكر مبررات القيام بها وتصديقها من الإدارة؟
9		☐	☐	☐	Are tested data derived and protected against disclosure?	هل يتم حماية بيانات الاختبارات بحد ذاتها من الكشف؟
10		☐	☐	☐	Do control procedures cover significant changes to computing and telecommunications equipment?	هل تعالج إجراءات التحكم مواضيع التغيرات الهامة في الأنظمة الحاسوبية ووسائل الاتصالات؟
11		☐	☐	☐	Are there suitable processes in place to review the inventory of systems and identify whether announced vulnerabilities are relevant?	هل يوجد عمليات مناسبة تعنى بمراجعة مخزون الأنظمة وهل تم الإعلان عن ثغرات أمنية متعلقة بها؟
12		☐	☐	☐	Are patches assessed for applicability and risks before being implemented?	هل تقيم الرقع البرمجية (البرمجيات اللاحقة لمعالجة ثغرات البرامج المنصبة) من حيث قابلية تطبيقها ومخاطرها قبل تنفيذها؟
13		☐	☐	☐	Are the processes for implementing urgent patches sufficiently slick and comprehensive?	هل عمليات التطبيق الطارئة للرقع البرمجية مدركة وسهلة بصورة مقبولة؟
			Information security incident management (4 Controls)			**10-إدارة حوادث أمن المعلومات**

Item No.	Notes	Findings النتائج			Questions	الأسئلة
		Partially Applied	N لا	Y نعم		
1			☐	☐	Are those who should be reporting security events and weaknesses aware of, and in fact use, the processes for reporting security events and weaknesses?	هل يتمتع القائمون على رفع تقارير الحوادث الأمنية ونقاط الضعف بالوعي الكافي لسير عمليات معالجة هذه المهام؟ والأهم من ذلك هل يستخدمونها فعلياً؟
2			☐	☐	Are the policies, procedures and guidelines followed in reality?	هل يتم الالتزام بالسياسات واللوائح والإرشادات على أرض الواقع؟
3			☐	☐	Does the organization have a relatively mature incident management process, evaluation/investigation, corrective action and the other parts for managing security incidents and improving protection opportunities in place?	هل لدى المؤسسة معالجة ناضجة نسبياً لإدارة الحوادث، التقييم/ التحقيق، الفعل التصحيحي، والأجزاء الأخرى لإدارة الحوادث الأمنية وتعزيز فرص الحماية؟
4			☐	☐	Is the organization proactively learning from incidents, improving risk knowledge and security controls accordingly?	هل تجري وبصورة متواصلة عملية التعلم من الحوادث والدعم في معرفة المخاطر ووسائل التحكم الأمنية بناءً على إدارة الحوادث؟
			Business Continuity Management (9 Controls)			**11-إدارة استمرارية العمل**
1		☐	☐	☐	Are suitable designs of 'high availability' employed for IT systems, networks, etc, which support critical business processes?	هل تم تصميم أنظمة تكنولوجيا المعلومات، الشبكات ...الخ، لتؤمن إتاحية عالية تدعم معالجة الأعمال الأكثر حرجاً وأهميةً؟

Item No.	Notes	Findings النتائج			Questions	الأسئلة
		Partially Applied	N لا	Y نعم		
2		☐	☐	☐	Are those who involved understanding the risks the organization is facing?	هل تتفهم الأطراف المعنية المخاطر التي تواجهها المؤسسة؟
3		☐	☐	☐	Are business critical, the associated assets and potential incident impacts correctly identified?	هل يوجد تعريف صحيح للعمليات الحرجة بالنسبة للأعمال والأصول المعلوماتية المرتبطة بها وتأثير الحوادث المحتمل؟
4		☐	☐	☐	Are suitable plans in place to maintain business operations or restore them within defined time frames?	هل يوجد خطط مناسبة للمحافظة على عمليات التشغيل أو استعادتها ضمن إطار زمني محدد؟
5		☐	☐	☐	Are suitable preventative, detective and corrective controls mandated?	هل تم اعتماد وسائل تحكم مانعة وكاشفة ومصححة تناسب الأعمال؟
6		☐	☐	☐	Do the plans take into account the identification and agreement of responsibilities, identification of acceptable loss, implementation of recovery and restoration procedure, documentation of procedure and regular testing/exercises?	هل تأخذ هذه الخطط بعين الاعتبار التعريفات والاتفاقات المتعلقة بالمسؤوليات، الخسائر المقبولة، إجراءات تنفيذ المعالجة والاستعادة، توثيق الإجراءات، الاختبارات والتجارب المنتظمة؟
7		☐	☐	☐	Is there a single coherent framework for business continuity planning?	هل يوجد إطار وحيد متناسق لتخطيط استمرارية العمل؟

Item No.	Notes	Findings النتائج			Questions	الأسئلة
		Partially Applied	N لا	Y نعم		
8		☐	☐	☐	If yes, does the framework ensure that all plans are consistent and identifies priorities for testing and maintenance?	في حال الإجابة نعم، هل يضمن هذا الإطار متانة هذه الخطط ويعرف الأولويات للاختبار والصيانة؟
9		☐	☐	☐	Are members of the crisis/incident management, recovery teams and other relevant staff aware of the plans and are clear on their personal roles and responsibilities?	هل يعي أعضاء إدارة الحوادث /الأزمات، فرق المعالجة، وغيرهم من المعنيين، بهذه الخطط ويدركون تماماً أدوارهم ومسؤولياتهم؟
			Compliance (36 Controls)			**12-فرض الالتزام والطاعة**
1		☐	☐	☐	Is the organization subject to specific legal obligations for data protection and privacy?	هل تقع المؤسسة تحت طائلة أية التزامات قانونية خاصة تتعلق بحماية البيانات والخصوصية؟
2		☐	☐	☐	Do the storage/archival arrangements take account of the possibility of media deterioration?	هل تأخذ ترتيبات الأرشفة /التخزين احتمال تلف الوسائط بعين الاعتبار؟
3		☐	☐	☐	Are appropriate long-life storage media used for long term storage?	هل هنالك وسائط تخزين مناسبة ذات عمر طويل تستخدم من أجل التخزين طويل الأمد؟
4		☐	☐	☐	Is the use of IT facilities for any non-business or unauthorized purpose, without management approval, treated as improper use?	هل يعامل أي استخدام لمرافق تكنولوجيا المعلومات لأغراض لا تتعلق بالأعمال أو غير مصرح بها وبدون موافقة الإدارة على أنه غير لائق؟

Item No.	Notes	Findings النتائج			Questions	الأسئلة
		Partially Applied	N لا	Y نعم		
5		☐	☐	☐	Is an appropriate warning message presented to unauthorized behaviors/users?	هل تظهر أية رسائل تحذير للمستخدمين غير المصرح لهم؟
6		☐	☐	☐	Do managers ensure that all security procedures within their area of responsibility are carried out correctly to achieve compliance with security policies and standards?	هل يضمن المدراء أن جميع الإجراءات الأمنية ضمن نطاق مسؤوليتهم تطبق بصورة صحيحة للحصول على الالتزام المطلوب بسياسات ومعايير الأمن؟
			Technical Security Policies (30 Controls)			**(يتبع) 3-3-السياسات الأمنية الفنية**
1		☐	☐	☐	Is a technical security policy in place?	هل سياسات الأمن الفنية مطبقة عموماً؟
2		☐	☐	☐	Are unused services disabled?	هل تم إغلاق جميع الخدمات غير المستخدمة؟
3		☐	☐	☐	Are unused interfaces disabled?	هل تم إغلاق الواجهات غير المستخدمة؟
4		☐	☐	☐	Do any applications use telnet to perform management activities such as backing up configuration?	هل تستخدم أي من التطبيقات الـtelnet من أجل ممارسة أية أنشطة إدارية من مثل نسخ احتياطي للتهيئة؟
5		☐	☐	☐	Do passwords appear in encrypted form wherever they viewed or appeared?	هل تظهر كلمات المرور بشكل مشفر أينما وجدت؟

Item No.	Notes	Findings النتائج			Questions	الأسئلة
		Partially Applied	N لا	Y نعم		
6		☐	☐	☐	Do the passwords meet with the required complexity as defined by the policy?	هل تنسجم كلمات المرور مع مستوى التعقيد المطلوب والمعرف في السياسات؟
7		☐	☐	☐	According to policy, Is there any enforcement to change passwords regularly?	عملاً بالسياسات، هل يوجد فرض لتغيير كلمات المرور دورياً؟
8		☐	☐ ☐	☐ ☐	Is authentication done through: • Locally configured usernames and passwords • TACACS+/ RADUIS/ Database server	هل تتم عملية التحقق من خلال: • أسماء مستخدمين وكلمات مرور مهيئة محلياً ضمن الجهاز نفسه. • مخدمات قواعد بيانات / TACACS+/RADUIS
9		☐	☐	☐	Is there a documented procedure for creation of users?	هل هنالك إجراءات موثقة من أجل إنشاء الحسابات؟
10		☐	☐	☐	Does each administrator have a unique account for himself/herself?	هل يمتلك كل مدير نظام حساب فريد خاص به؟
11		☐	☐	☐	Is there a login and logout tracking/command history?	هل يتم تتبع عمليات دخول – خروج مدراء الأنظمة والأوامر المنفذة؟
12		☐	☐	☐	Are all user accounts assigned the lowest privilege level that allows them to perform their duties? (Principle of Least Privilege)	هل تم إنشاء الحسابات بشكل تؤمن فيه أدنى سماحيات ممكنة من أجل إنجاز مهام المستخدمين المطلوبة؟ (قاعدة الحد الأدنى من الامتيازات/ السماحيات)

Item No.	Notes	Findings النتائج			Questions	الأسئلة
		Partially Applied	N لا	Y نعم		
13		☐	☐	☐	Are the default settings changed in all systems and equipments?	هل تم تغيير الإعدادات المسبقة التعريف على كامل التجهيزات والأنظمة؟
14		☐	☐	☐	Is the NTP server service used to synchronize the clocks of all equipments?	هل تم تفعيل مخدم بروتوكول الوقت لضمان تزامن الساعات على كافة التجهيزات؟
15		☐	☐	☐	Is configurations backed up done regularly?	هل تتم عملية النسخ الاحتياطي لملفات التهيئة بصورة متكررة؟
16		☐	☐	☐	Is the backup moved to an off-site/DR site?	هل تم نقل النسخ الإحتياطي إلى موقع خارجي /موقع مواجهة الكوارث؟
17		☐	☐	☐	On the system where the configuration files are stored, is the local operating system's security mechanisms used for restricting access to the files (i.e., the machine should be password enabled and prevent unauthorized individuals from accessing the machine.)?	هل تستخدم آليات أمن وحماية معينة على أنظمة التشغيل الموجودة حيث يتم تخزين ملفات التهيئة من أجل تحديد الدخول إلى هذه الملفات (عدم السماح بالدخول إلى التجهيزة دون كلمة مرور مثلاً)؟

Item No.	Notes	Findings النتائج			Questions	الأسئلة
		Partially Applied	N لا	Y نعم		
18		☐	☐ ☐ ☐	☐ ☐ ☐	Is the TFTP protocol used to transfer network configuration or image files? If yes, • Is the TFTP process restricted to certain addresses only? • Is the TFTP service disabled when not in use?	هل يستخدم بروتوكول TFTP لنقل ملفات التهيئة الشبكية؟ في حال نعم: • هل العملية محصورة بعناوين حقيقية محددة؟ • هل يتم إغلاق الخدمة خارج أوقات استخدامها؟
19		☐	☐	☐	Is there a documented procedure for backup of configuration files?	هل هنالك إجراءات موثقة لعمليات النسخ الاحتياطي لملفات التهيئة؟
20		☐	☐	☐	Are all changes and updates documented in a manner suitable for review according to a change management procedure?	هل تم توثيق كافة التغييرات والتحديثات بطريقة تسمح بمراجعتها بما يتوافق مع إجراءات إدارة التغيير؟
21		☐	☐	☐	Is there a redundant machine in cold standby or hot standby?	هل يوجد احتياطات عتادية بوضعية خامدة أو جاهزة؟
22		☐	☐	☐	Are disaster recovery procedures for the network documented and are they tested?	هل تم توثيق وتجريب إجراءات مواجهة الكوارث الشبكية؟
23		☐	☐	☐	Are all attempts to any port, protocol, or service that is denied logged?	هل تسجل كافة محاولات الوصول إلى أي منفذ أو بروتوكول أو خدمة محجوبة؟

Item No.	Notes	Findings النتائج			Questions	الأسئلة
		Partially Applied	N لا	Y نعم		
24		☐	☐	☐	Are all CPUs /memories / storages monitored?	هل تتم مراقبة انشغالية المعالجات /الذواكر /مساحات التخزين؟
25		☐	☐	☐	Is there a special logging server enabled and login restricted?	هل يوجد مخدم خاص لحفظ ملفات الدخول محمي وذو سماحية دخول محدودة جداً؟
26		☐	☐	☐	Are procedures for audit log review generated by different systems and machines documented and followed?	هل يتم توثيق ومتابعة إجراءات تدقيق الدخول حسب ملفات الدخول الصادرة عن مختلف التجهيزات والأنظمة؟
27		☐	☐	☐	Are all logs (covering administrator access /access control) reviewed?	هل تتم مراجعة كافة ملفات الدخول (بما فيها دخول مدير النظام/ التحكم بالدخول)؟
28		☐	☐	☐	Are reports and analyses carried out based on system and log messages?	هل تعتمد التقارير والتحاليل على رسائل النظام ورسائل ملفات الدخول؟
29		☐	☐	☐	What is the course of action to be followed if any malicious incident is noticed?	هل يوجد سلسلة فعل متبعة وفعالة حين ملاحظة أي حادث خرق(غير مصرح به)؟
30		☐	☐	☐	Are the network/ system /applications /services engineers aware of the latest vulnerabilities that could affect their domain of proficiency?	هل مهندسو الشبكات /الأنظمة /التطبيقات /الخدمات على إطلاع بآخر الثغرات التي قد تصيب مجالاتهم؟

في النهاية هل تعتقد بأن النموذج المقترح فعال و يحقق متطلبات أمن المعلومات (المعايير الدولية) ؟ يرجى التوضيح.

الإجابة:

نهاية الاستطلاع

الملحق (2) الاستطلاع رقم -2-

استطلاع لتقييم كمي لمتحكمات أمن المعلومات

Introduction

This survey aims to weight each control of the security domain with numerical value, which reflects its importance.

We have conducted a survey for assessing the gap between your company information security situation and a new security model. And we have divided the model to security domains.

Please assign an integer number for each control in such a way that the sum of control's weights for each domain is equal to 100.

المقدمة

يهدف هذا الاستطلاع إلى تحميل كل متحكم لأمن المعلومات بقيمة رقمية صحيحة تعكس أهميته في سياق أمن المعلومات و الشبكات لدى مؤسستكم.

قمنا سابقاً بإجراء استطلاع لتحديد واقع أمن المعلومات لدى مؤسستكم. و قد وزعنا المتحكمات على عدة مجالات بحسب الطبقة الأمنية التي تنتمي لها المجالات.

يرجى وضع قيمة رقمية صحيحة لكل متحكم بحيث يكون مجموع المتحكمات في كل مجال يساوي 100.

Questionnaire: Implementation of Information Security

استطلاع: تطبيق أمن المعلومات

Item No.	Weight					Notes	Findings			Questions	الأسئلة
	Average	Sample1	Sample2	Sample3	Sample4		Partially Applied	No	YES		
							-Information security management system (ISMS) 6 Controls				نظام إدارة أمن المعلومات
1	20	15	19	24	21		☐	☐	☐	Is there any evidence that management genuinely understands and supports the ISMS?	هل يوجد دلائل ملموسة تؤكد أن الإدارة حقيقةً تستوعب وتدعم هذا النظام؟
2	15	15	16	11	18		☐	☐	☐	Is there any exclusion from ISMS scope?	هل يوجد أية أمور مستبعدة عن نظام إدارة أمن المعلومات؟
3	10	8	10	9	13		☐	☐	☐	If yes; are there justified reasons for excluding any elements?	في حال الإجابة نعم، هل هنالك أسباب منطقية وراء استبعادها؟
4	15	12	13	17	16		☐	☐	☐	Does organization's ISM Policy adequately reflect the organization's general characteristics and its strategic risk management approach?	هل تتناسب سياسات إدارة أمن المعلومات مع المواصفات العامة للمصرف واستراتيجيته في إدارة المخاطر؟
5	20	25	21	17	20		☐	☐	☐	Does ISM incorporate the organization's business requirements plus any legal or regulatory obligations for information security?	هل تحقق سياسات إدارة أمن المعلومات كافة متطلبات الأعمال الخاصة بالمؤسسة، إضافةً إلى أية التزامات أو تشريعات قانونية متعلقة بأمن المعلومات؟

Item No.	Weight					Notes	Findings			Questions	الأسئلة
	Average	Sample1	Sample2	Sample3	Sample4		Partially Applied	No	YES		
6	20	25	21	22	12		☐	☐	☐	Has it been formally approved by management and set meaningful criteria for evaluating information security risks?	هل تتضمن عوامل مفيدة وذات معنى لتقييم مخاطر أمن المعلومات تمت المصادقة عليها من قبل الإدارة؟
										Risk Assessment (14 Controls)	**تقييم المخاطر**
1	10	13	10	9	8		☐	☐	☐	Is there any systemic risk assessment method(s)?	هل هناك طرق منهجية متبعة لتقييم المخاطر؟
2	6	5	5	7	7		☐	☐	☐	Are the results of risk assessments comparable and reproducible?	هل نتائج هذا التقييم قابلة للمقارنة وإعادة الإنتاج؟
3	7	6	8	8	6		☐	☐	☐	Is the risk assessment method updated as a result?	هل يتم تحديث طريقة تقييم المخاطر بناءً على ما سبق؟
4	9	4	10	12	10		☐	☐	☐	Is the definition of criteria sensible and practicable in relation to information security risks?	هل تم تحديد العوامل الحرجة لمخاطر أمن المعلومات بشكل دقيق وقابل للتطبيق؟
5	8	9	8	7	8		☐	☐	☐	Are all relevant in-scope information assets included?	هل تم تضمين التقييم جميع الأصول المعلوماتية الموجودة ضمن منظور إدارة أمن المعلومات؟
6	1	1	1	1	1		☐	☐	☐	Are responsible owners identified for all the information assets?	هل تم تحديد الأطراف المسؤولة (المالكة) عن الأصول المعلوماتية؟
7	6	4	5	6	9		☐	☐	☐	Is there an adequate analysis/evaluation of threats?	هل يوجد تحليلاً وتقييماً كافياً للتهديدات؟
8	6	7	8	4	5		☐	☐	☐	Is there an adequate analysis/evaluation of vulnerabilities and impacts?	هل يوجد تحليل وتقييم كافٍ للثغرات وتأثيرها؟

Item No.	Weight					Notes	Findings			Questions	الأسئلة
	Average	Sample1	Sample2	Sample3	Sample4		Partially Applied	No	YES		
9	5	9	3	2	6		☐	☐	☐	Is there an adequate documentation of risk scenarios plus the prioritization or ranking of risks?	هل يوجد توثيق كافٍ لمختلف احتمالات المخاطر مع مراتب أو أولويات لها؟
										- Risk Treatment Plan	**-خطة معالجة المخاطر**
10	10	12	8	11	9		☐	☐	☐	Are appropriate "treatments" specified for all identified risks?	هل تم توصيف علاج مناسب لكافة المخاطر المعرفة؟
11	6	4	5	7	8		☐	☐	☐	Are changes suitably fitted in the plan?	هل يتم وضع التغييرات ضمن الخطة؟
12	8	10	9	8	5		☐	☐	☐	Is the Risk Treatment Plan being used and updated proactively as an information security management tool?	هل تم استخدام وتحديث خطة معالجة المخاطر بصورة استباقية فعالة كأدة لإدارة أمن المعلومات؟
13	8	7	12	6	7		☐	☐	☐	Are defined controls objectives and selected controls satisfied?	هل تعتبر أهداف التحكم وأنواع التحكم المعرفة على مستوى جيد؟
14	10	9	8	12	11		☐	☐	☐	Is the organization effectively and proactively reviewing the implementation of the ISMS to ensure that the security controls identified in the Risk Treatment Plan, policies, etc. are actually implemented and are in fact in operation?	هل تقوم المؤسسة بمراجعة فعالة ووقائية لآلية تطبيق نظام إدارة أمن المعلومات للتأكد من أن طرق التحكم الأمنية المعرفة في خطة معالجة المخاطر والسياسات و...الخ، مطبقة حقاً وهي تعمل؟
							Management responsibility (9 Controls)				**مسؤولية الإدارة**

Item No.	Weight					Notes	Findings			Questions	الأسئلة
	Average	Sample1	Sample2	Sample3	Sample4		Partially Applied	No	YES		
1	20	17	23	22	19		☐	☐	☐	Are there enough resources allocated to the ISMS in terms of budget, manpower etc?	هل هنالك موارد كافية مخصصة لنظام إدارة المعلومات من حيث الميزانية، القوة العاملة...الخ؟
2	15	17	14	13	16		☐	☐	☐	Are sufficient funds allocated by management to address information security issues in a reasonable timescale and to a suitable level of quality?	هل خصصت الإدارة تمويلاً كافياً من أجل مواجهة ومعالجة قضايا أمن المعلومات ضمن حدود الوقت والجودة المطلوبين؟
3	6	9	6	4	5		☐	☐	☐	Do the top managers seriously commit to information security in their behavior?	هل يلتزم المدراء حقيقةً بأمن المعلومات من خلال مسلكيتهم؟
4	12	13	11	13	11		☐	☐	☐	Are necessary competencies and training/awareness requirements for information security professionals and others with specific roles and responsibilities explicitly identified?	هل تم التعريف الواضح بمتطلبات المهارة والتدريب والتوعية الضرورية لإختصاصيي أمن المعلومات وغيرهم مع تحديد الأدوار والمسؤوليات؟
5	10	8	12	11	9		☐	☐	☐	Is there a scheduled reviewing, at last once a year?	هل هنالك جدولة محددة للقيام بالمراجعة، مرة سنوياً على الأقل؟
6	6	5	4	5	10		☐	☐	☐	Does management play an active part and is fully engaged in the review/s?	هل تلعب الإدارة دوراً فعالاً وحقيقي الاهتمام في عمليات المراجعة؟
							- Internal ISMS audits				**-فحص نظام إدارة أمن المعلومات داخلياً**
7	8	7	6	10	8		☐	☐	☐	Is there any internal audits plan?	هل هنالك أي خطط داخلية لفحص إدارة أمن المعلومات؟

	Weight						Findings				
Item No.	Average	Sample1	Sample2	Sample3	Sample4	Notes	Partially Applied	No	YES	Questions	الأسئلة
8	8	9	7	6	10		☐	☐	☐	If yes, are responsibilities for conducting ISMS internal audits formally assigned to competent, adequately trained IT auditors?	في حال كان الجواب نعم، هل مسؤوليات إدارة عملية الفحص الداخلية موكلة رسمياً إلى مدققي تكنولوجيا معلومات مدربين ومختصين في ذلك؟
9	15	15	17	16	12		☐	☐	☐	Does ISMS changes in response to the identification of significantly changed risks?	هل يستجيب نظام إدارة أمن المعلومات إلى المخاطر المعرفة والمتغيرة بصورة ملحوظة؟
							Information security policy (15 Controls)				**سياسات أمن المعلومات**

Item No.	Weight					Notes	Findings			Questions	الأسئلة
	Average	Sample1	Sample2	Sample3	Sample4		Partially Applied	No	YES		
1	15	11	12	14	23		☐	☐	☐	Are the policies communicated, understood and accepted? • Standards for physical security of the computer and telecommunications installation and associated facilities; • HR procedures governing access to and use of IT services (usernames and passwords, disciplinary procedures); • End user guidelines covering PC software licensing and virus prevention, etc?	هل يتم تبادل وفهم وقبول السياسات المتعلقة؟ • معايير الأمن المادية للحواسب والاتصالات وكافة ملحقاتها. • الإجراءات الخاصة بالموارد البشرية والمتعلقة بالتحكم في الدخول إلى واستخدام خدمات تكنولوجيا المعلومات (أسماء مستخدمين وكلمات عبور، إجراءات تأديبية ...الخ). • إرشادات للمستخدمين تتعلق بقضايا تراخيص برامج الحواسب، صد الفيروسات ...إلخ).
2	8	9	10	6	7		☐	☐	☐	Are they reasonable and workable?	هل هذه السياسات منطقية وقابلة للتطبيق؟
3	5	3	4	8	5		☐	☐	☐	Do they incorporate suitable and sufficient controls?	هل تتكامل هذه السياسات مع أدوات تحكم مناسبة وكفء؟
4	8	7	10	6	5		☐	☐	☐	Do they cover all essential computing and telecommunication services?	هل تغطي هذه السياسات جميع الجوانب الأساسية المتعلقة بالحواسب والاتصالات؟

Item No.	Weight					Notes	Findings			Questions	الأسئلة
	Average	Sample1	Sample2	Sample3	Sample4		Partially Applied	No	YES		
							- Internal Responsibilities and Communications				**-المسؤوليات الداخلية وآليات التواصل**
5	4	5	7	2	2		☐	☐ ☐ ☐ ☐ ☐	☐ ☐ ☐ ☐ ☐	Are the following positions well defined and activated: • Senior manager responsible for IT and ISM; • Information security professionals; Security administrators; • Site/physical security manager and Facilities contacts; • HR contact for HR matters such as disciplinary action and training; • Systems and network managers, security architects and other IT professionals.	هل تم تعريف وتفعيل دور المناصب التالية: • مدير من الصف الأول مسؤول عن تكنولوجيا المعلومات وإدارة أمنها. • أخصائيو أمن معلومات، مدراء أنظمة معلومات. • مدير أمن للشؤون المادية في الموقع وأعضاء ارتباط المرافق. • عضو ارتباط الموارد البشرية من أجل الأمور المتعلقة مثل الأفعال التأديبية والتدريب. • مدراء أنظمة وشبكات، تصميم الهيكل الأمني، وغيرهم من أخصائيي تكنولوجيا المعلومات.
6	5	5	4	5	6		☐	☐	☐	Is ISM given sufficient emphasis (is there a 'driving force'?) and management support?	هل تعطي الإدارة دفعاً (قوة دفع) ودعماً قوياً لإدارة أمن المعلومات؟

Item No.	Weight					Notes	Findings			Questions	الأسئلة
	Average	Sample1	Sample2	Sample3	Sample4		Partially Applied	No	YES		
7	2	4	1	3	2		☐	☐	☐	Is there a senior management forum to discuss ISM policies, risks and issues?	هل هنالك منتدى خاص لمناقشة سياسات إدارة أمن المعلومات والمخاطر وغيرها من القضايا المتعلقة مكون من مدراء الصف الأول؟
8	8	9	6	7	10		☐	☐	☐	Are roles and responsibilities clearly defined and assigned to skilled individuals?	هل تم تعريف الأدوار والمسؤوليات بوضوح وتعيين الأفراد المؤهلين للقيام بها؟
9	3	2	2	3	5		☐	☐	☐	Is there sufficient co-ordination within the BU (business unit), between BUs and with HQ?	هل هنالك تنسيق وتعاون كافٍ على مستوى الوحدة الاقتصادية، الوحدات فيما بينها، ومع المقر الرئيسي أيضاً؟
10	5	6	6	5	3		☐	☐	☐	Are the information flows (like incident reporting) operating effectively in practice?	هل تعتبر عملية تدفق المعلومات (مثلاً رفع تقارير الحوادث) فعالة على أرض الواقع؟
							- External Parties				**-الأطراف المعنية الخارجية**
11	10	12	11	9	8		☐	☐	☐	Is there a risk analysis process in place for 3rd -party communications and connections?	هل يتم تضمين الاتصالات والتواصل التابعة للأطراف المعنية في العقود بصورة غير مباشرة (الطرف الثالث) ضمن عملية تحليل المخاطر؟
12	5	3	6	9	3		☐	☐	☐	Is there any individual who has responsibility for ensuring that all 3-party links are in fact identified and risk assessed?	هل هنالك أي فرد مسؤول عن ضمان أن كافة الروابط مع الأطراف الثالثة المعنية قد تم تعريفها وتقييم المخاطر المتعلقة بها؟

Item No.	Weight					Notes	Findings			Questions	الأسئلة
	Average	Sample1	Sample2	Sample3	Sample4		Partially Applied	No	YES		
13	7	7	9	8	5		☐	☐	☐	Are ISM arrangements in operation on 3-party connections routinely reviewed against the requirements?	هل من ترتيبات لإدارة أمن المعلومات على أرض الواقع تراجع بانتظام طرق الاتصال مع الأطراف الثالثة وتقارنها مع المتطلبات؟
14	12	15	9	11	14		☐	☐ ☐ ☐ ☐ ☐	☐ ☐ ☐ ☐ ☐	Are there formal contracts covering 3rd party links? • Ownership and responsibility for ISM issues? • Legal requirements? • Protection of systems, networks and data via physical, logical and the right of audit by the organization? • Procedural controls business assets, availability of services in the event of disasters, management notification for security incidents? • Security clearance of staff?	هل هنالك عقود رسمية تغطي الروابط مع الأطراف الثالثة: • ملكية ومسؤولية المسائل المتعلقة بإدارة أمن المعلومات؟ • المتطلبات القانونية؟ • حماية الأنظمة والشبكات والمعطيات من الناحية المنطقية والمادية وحق المؤسسة بالتدقيق عليها؟ • إجراءات التحكم المتعلقة بالأصول، ومدى إتاحية الخدمات في حالة الكوارث، وطرق إعلام الإدارة بالحوادث الأمنية؟ • قيام كادر الطرف الثالث بالتصريح الأمني رسمياً؟

Item No.	Weight					Notes	Findings			Questions	الأسئلة
	Average	Sample1	Sample2	Sample3	Sample4		Partially Applied	No	YES		
15	3	2	3	4	2		☐	☐	☐	Does the outsourcing contract adequately address the previous issues?	هل عقود نقل الأعمال لأطراف خارجية تتضمن القضايا السابقة بشكل وافٍ؟
							Information Asset Management (7 Controls)				**إدارة الأصول المعلوماتية**
1	15	13	12	13	21		☐	☐	☐	Are there any arrangements to establish and maintain an inventory of information assets?	هل هنالك أية ترتيبات تتعلق بإنشاء وصيانة مخزن الأصول المعلوماتية؟
2	11	9	13	10	12		☐	☐	☐	Is there a 'registration process' for new application systems?	هل هنالك قوانين تحكم تطبيق الأنظمة الجديدة؟
3	15	18	14	17	11		☐	☐	☐	Are there asset tags on all PCs, network equipment, etc?	هل هنالك بطاقة تعريف الأصل المعلوماتي على كل حاسب وتجهيزة شبكية...الخ؟
4	15	20	18	12	10		☐	☐	☐	Are power and data cables clearly labeled and are wiring diagrams kept complete and up-to-date?	هل جميع كبلات الكهرباء والبيانات معنونة بوضوح، وجميع مخططات الأسلاك محفوظة بالكامل وبآحدث نسخها؟
5	17	15	19	16	18		☐	☐	☐	Is Information classification in place, covering business requirements for confidentiality, integrity and availability	هل يشتمل تصنيف المعلومات القائم على متطلبات الأعمال من أجل السرية والصحة والإتاحية؟
6	12	15	10	10	13		☐	☐	☐	Are appropriate markings used on documents, forms, reports, screens, backup media, emails, file transfers?	هل تستخدم تأشيرات مناسبة في الوثائق والصيغ والتقارير والشارات ووسائط النسخ الاحتياطي ونقل الملفات؟

Item No.	Weight					Notes	Findings			Questions	الأسئلة
	Average	Sample1	Sample2	Sample3	Sample4		Partially Applied	No	YES		
7	15	10	14	22	15		☐	☐	☐	Is staff made aware of the corresponding security requirements for handling sensitive materials?	هل يعي الكادر متطلبات الأمن المقابلة لتدابير المواد الحساسة؟
							Human Resources Security (5 Controls)				**متطلبات الأمن من جهة الموارد البشرية**
1	25	30	27	22	21		☐	☐	☐	Are information security roles, disciplinary actions and responsibilities defined in job descriptions, terms and conditions of employment etc. for specific IT security staff, system/network managers, managers and end users in general?	هل وظائف أمن المعلومات والأفعال التأديبية والمسؤوليات معرفة بصورة واضحة في التوصيف الوظيفي وبنود وشروط التوظيف...إلخ، بالنسبة للكادر الخاص بأمن المعلومات ومدراء الشبكات/الأنظمة، والمدراء والمستخدمين بصورة عامة؟
2	20	17	17	24	22		☐	☐	☐	Are there appropriate HR policies and procedures that transgress IT security rules?	هل هنالك سياسات وإجراءات مناسبة للموارد البشرية حين انتهاك مبادئ أمن تكنولوجيا المعلومات؟
3	25	22	26	25	27		☐	☐	☐	Are there enhanced screening processes for staff/managers in particularly sensitive roles or sites?	هل هنالك عمليات اختيار معمقة من أجل الكادر/ المدراء وتحديداً للأدوار أو المواقع الحساسة؟

Item No.	Weight					Notes	Findings			Questions	الأسئلة
	Average	Sample1	Sample2	Sample3	Sample4		Partially Applied	No	YES		
4	20	18	21	21	20		☐	☐	☐	Do end staff and their managers routinely receive appropriate training on information security including roles and responsibilities, login procedures etc., within the context of general IT systems training?	هل يتلقى الكوادر ومدرائهم بانتظام تدريباً مناسباً على أمن المعلومات بما في ذلك الوظائف والمسؤوليات، إجراءات الدخول ...إلخ متضمناً في مجرى التدريب العام على أنظمة تكنولوجيا المعلومات؟
5	10	13	9	8	10		☐	☐	☐	Are there any procedures and/or guidelines relating to information security elements in the cases of termination or change of employment?	هل هنالك أية إجراءات أو /و إرشادات تتعلق بعناصر أمن المعلومات في حالات من مثل ترك العمل أو تغيير التوظيف؟
							Physical and Environmental Security (23 Controls)				**متطلبات الأمن من الناحية البيئية والفيزيائية**
1	3	2	4	3	2		☐	☐	☐	Are discreet facilities sited to minimize disaster potential or cost of protective countermeasures?	هل تم وضع وسائل حكيمة لتقليل احتمالات الكوارث أو تكاليف الحلول الوقائية؟
2	3	4	3	2	2		☐	☐	☐	Is the construction physically sound e.g. walls go "slab-to-slab", thick solid doors, etc?	هل البناء يوحي بالأمن من الناحية المادية، مثلاً جدران متراصفة، أبواب سميكة صلبة ...الخ؟
3	3	1	3	4	5		☐	☐	☐	Are suitable access control systems employed with matching procedures?	هل تطبق أنظمة مناسبة للتحكم بالدخول والإجراءات المقابلة لها؟

Item No.	Weight					Notes	Findings			Questions	الأسئلة
	Average	Sample1	Sample2	Sample3	Sample4		Partially Applied	No	YES		
4	5	6	5	4	5		☐	☐	☐	Is there appropriate physical protection for external cables, junction boxes, air conditioner chillers, microwave dishes, air inlets etc. against accidental damage or deliberate interference?	هل هنالك إجراءات حماية مادية مناسبة للكبلات الخارجية، علب القواطع، مبرد المكيفات، اللواقط، مداخل التهوية...الخ ضد الأضرار غير المتعمدة أو الدخول عنوة؟
5	2	1	2	2	1		☐	☐	☐	Is there any protection/control of fire and smoke, e.g. fire-resistant/low-smoke construction materials, wiring, etc?	هل هناك أية وسائل حماية/ تحكم تتعلق بالحرائق أو الدخان مثل الأسلاك ومواد البناء المقاومة للحريق/ قليلة إصدار الدخان؟
6	**1**	**1**	**1**	**1**	**1**		☐	☐	☐	Is there any evidence of smoking?	هل يوجد تدخين في المكان؟
7	6	9	4	6	6		☐	☐	☐	Are no-smoking signs displayed?	هل توضع إشارات عدم التدخين بوضوح؟
8	7	7	5	10	6		☐	☐	☐	Are fire systems and interlocks regularly inspected and maintained inspections by professionals?	هل يتم فحص وصيانة أنظمة الإنذار ضد الحرائق والقفل بصورة منتظمة من قبل أخصائيين؟
9	4	2	5	3	6		☐	☐	☐	Is there enough awareness of fire evacuation procedures?	هل يوجد توعية كافية حول إجراءات الإخلاء عند حدوث الحريق؟
10	7	8	5	9	7		☐	☐	☐	Is there an adequate UPS capacity to support all essential computer equipment and peripherals, and all such equipment?	هل هنالك ما يكفي من وحدات عدم انقطاع التيار الكهربائي تغطي سعاتها كافة التجهيزات الحاسوبية الأساسية والمحيطية وتفرعاتها؟
11	8	7	10	6	9		☐	☐	☐	Is there an adequate Back-up generator capacity?	هل هنالك مولدة كهربائية احتياطية ذات سعة كافية؟

Item No.	Weight					Notes	Findings			Questions	الأسئلة
	Average	Sample1	Sample2	Sample3	Sample4		Partially Applied	No	YES		
12	2	2	1	1	3		☐	☐	☐	Is there adequate A/C capacity to support heat load?	هل هنالك طاقة تبريدية كافية لمعالجة الحمل الحراري؟
13	1	1	1	1	1		☐	☐	☐	Are there adequate redundant/spare units or portables available to improve resilience and permit maintenance without affecting service?	هل هنالك ما يكفي من القطع الاحتياطية أو المحمولة المتاحة لدعم المرونة والصيانة الدورية دون تأثر الخدمة؟
14	8	12	5	5	9		☐	☐	☐	Is temperature sensing with remote-reading over-temperature alarms and incident procedures available?	هل تتوفر حساسات حرارية تدعم القراءة من بعيد وإنذارات زيادة درجة الحرارة إضافةً إلى إجراءات الطوارئ؟
15	7	8	8	7	5		☐	☐	☐	Is water/flood protection with detection and remote alarms applied?	هل يوجد نظام منع وكشف وإنذار بعيد حول تسرب المياه وطوفانها؟
16	5	3	6	7	4		☐	☐	☐	Are computer and telecommunications rooms maintained in clean condition?	هل يتم المحافظة على شروط نظافة غرف التجهيزات والإتصالات؟
17	3	3	5	2	2		☐	☐	☐	Is there a special treatment for dust avoidance?	هل توجد معالجة خاصة لتجنب الغبار؟
18	2	1	2	2	3		☐	☐	☐	Is all exposed metalwork earth bonded to a common safety earth point for both safety and static reduction reasons?	هل تم تثبيت كافة الهياكل المعدنية المكشوفة وربطها إلى نقطة تأريض لأغراض السلامة وتقليل الكهرباء الساكنة؟
19	8	7	6	10	9		☐	☐	☐	Are lightning conductors, cable isolators, and fuses etc, mounted where applicable?	هل تم رفع كافة قواطع الإضاءة، عوازل الكبلات، قواطع الطاقة الكهربائية ...إلخ حين توفر الإمكانية؟

Item No.	Weight					Notes	Findings			Questions	الأسئلة
	Average	Sample1	Sample2	Sample3	Sample4		Partially Applied	No	YES		
20	2	3	2	1	2		☐	☐	☐	Are all physical equipments operated and maintained as per manufacturer's specifications and tested on-load regularly?	هل يتم تشغيل وصيانة كافة التجهيزات المادية واختبارها تحت الحمل على أساس المواصفات الفنية التي حددتها الجهة الصانعة؟
21	5	3	7	6	4		☐	☐	☐	Are all physical controls following major changes?	هل تتبع كافة وسائل التحكم المادية التغيرات الكبيرة؟
22	5	4	6	6	5		☐	☐	☐	Is there any management authorization process for removal of information assets from site?	هل يوجد عملية مصرحة إدارياً لزوم إزالة الأصول المعلوماتية من موقع ما؟
23	2	4	2	1	1		☐	☐	☐	Are there any secure disposal processes to erase sensitive corporate and personal site data fully from removable or fixed media before disposal?	هل هنالك أية عمليات آمنة من أجل مسح البيانات الحساسة والشخصية كاملةً من وسائط التخزين الثابتة أو القابلة للإزالة قبل التصرف بها؟
							Communications and Operations Management (31 Controls)				**إدارة عمليات التشغيل والاتصالات**
1	6	4	7	6	7		☐	☐	☐	Is there a full set of security procedures in place relating to general IT operations?	هل يوجد في واقع الحال مجموعة كاملة من إجراءات الأمن المتعلقة بعمليات تشغيل تكنولوجيا المعلومات عموماً؟
2	6	7	5	6	6		☐	☐	☐	Is there a full set of security procedures in place relating to systems and network management?	هل يوجد في واقع الحال مجموعة كاملة من إجراءات الأمن المتعلقة بإدارة الأنظمة والشبكة؟

Item No.	Weight					Notes	Findings			Questions	الأسئلة
	Average	Sample1	Sample2	Sample3	Sample4		Partially Applied	No	YES		
3	6	8	5	5	6		☐	☐	☐	Is there a full set of security procedures in place relating to incident management?	هل يوجد في واقع الحال مجموعة كاملة من إجراءات الأمن المتعلقة بإدارة الحوادث؟
4	6	5	7	7	3		☐	☐	☐	Is there a full set of security procedures in place relating to IT security admin?	هل يوجد في واقع الحال مجموعة كاملة من إجراءات الأمن المتعلقة بإدارة أمن تكنولوجيا المعلومات؟
5	2	4	2	1	1		☐	☐	☐	Is there a full set of security procedures in place relating to change management?	هل يوجد في واقع الحال مجموعة كاملة من إجراءات الأمن المتعلقة بإدارة التغيير؟
6	3	6	2	2	1		☐	☐	☐	Are the previous procedures reasonably well controlled?	هل يتم التحكم بالإجراءات السابقة بصورة جيدة من الناحية المنطقية؟
7	2	2	1	3	2		☐	☐	☐	Are corresponding responsibilities assigned to individuals?	هل يتم تكليف الأفراد بمسؤوليات متناسبة معهم؟
8	1	2	1	1	1		☐	☐	☐	Are there acceptance tests and capacity planning including CPU usage, disk space, network capacity, etc?	هل يوجد اختبارات قبول وتخطيط للسعات يتضمن استخدام /مشغولية المعالج، حجم القرص، سعة الشبكة ...الخ.
9	1	1	1	1	1		☐	☐	☐	Are acceptance tests completed prior to the introduction of new systems onto the network?	هل تجرى كامل اختبارات القبول قبل استقدام أنظمة جديدة إلى الشبكة؟
10	2	1	3	3	1		☐	☐	☐	Are fallback arrangements updated to reflect new/retired systems?	هل يتم تحديث إجراءات الاستعادة حتى تستوعب الأنظمة الجديدة والمتقادمة؟

Item No.	Weight					Notes	Findings			Questions	الأسئلة
	Average	Sample1	Sample2	Sample3	Sample4		Partially Applied	No	YES		
11	1	1	1	1	1		☐	☐	☐	Are there continuous/frequent virus-checks on all PCs including standalones/portables?	هل يتم باستمرار وضمن تواتر معين فحص الحواسب القائمة بذاتها منها والمحمولة ضد الفيروسات؟
12	3	3	3	2	4		☐	☐	☐	Are infection levels minimized (is the situation broadly under control)?	هل تم تخفيض مستويات الإصابة للحدود الدنيا (هل الوضع تحت السيطرة شبه التامة)؟
13	1	2	1	1	1		☐	☐	☐	Are staff and managers aware of the protection against malicious and mobile code procedures?	هل يمتلك المدراء والكادر معرفةً حول إجراءات الحماية من البرامج الخبيثة والنقالة؟
14	5	6	4	7	3		☐	☐	☐	Is there a sufficient protection against Trojans, worms, spyware, rootkits, etc?	هل يوجد حماية كافية ضد الهجمات مثل أحصنة طروادة، الديدان، البرامج التجسسية، البرامج المتطفلة ...الخ؟
15	6	4	4	10	5		☐	☐	☐	Are backup strategies and procedures documented and tested?	هل تم توثيق وتجريب استراتيجيات وإجراءات النسخ الاحتياطي؟
16	3	4	2	2	4		☐	☐	☐	Do these strategies cover data, programs, system files, parameter files, etc, for all systems including servers, desktops, phone/network systems, system/network management systems, standalone/portable systems, control systems, etc?	هل تغطي هذه الاستراتيجيات البيانات، البرامج، ملفات النظام، ملفات البارامترات ...الخ لكامل الأنظمة بما فيها المخدمات، الحواسب، أنظمة الهاتف وشبكته، أنظمة إدارة الشبكات والنظم، الأنظمة القائمة بذاتها والمحمولة، أنظمة التحكم ...الخ؟

Item No.	Weight					Notes	Findings			Questions	الأسئلة
	Average	Sample1	Sample2	Sample3	Sample4		Partially Applied	No	YES		
17	3	3	2	3	4		☐	☐	☐	Are backup frequencies and types appropriate?	هل يعتبر تواتر ونوع النسخ الاحتياطي مناسباً؟
18	6	3	9	5	7		☐	☐	☐	Are backup media protected against loss, theft, damage, fire including both on-site and off-site/remote storage?	هل وسائط النسخ الاحتياطي محمية ضد الفقد، السرقة، الضرر، الحرائق بحالتي التخزين محلياً أو في مكان آخر؟
19	3	1	5	2	4		☐	☐	☐	Do all backup media listed in the procedures/records actually exist?	هل جميع وسائط النسخ الاحتياطي المدونة في الإجراءات والسجلات موجودة حقاً؟
20	2	1	3	2	2		☐	☐	☐	Are security elements of network management procedures properly documented?	هل تم توثيق إجراءات إدارة الشبكة المتعلقة بعناصر الأمن؟
21	2	1	2	2	4		☐	☐	☐	Are information security aspects such as security arrangements for 3rd-party connections adequately covered?	هل تم تغطية الأوجه المختلفة لأمن المعلومات مثل الترتيبات الأمنية للاتصال مع الطرف الثالث بصورة كافية؟
22	4	3	5	4	4		☐	☐	☐	Is there an up-to-date and complete asset register for tapes, removable disks, CDs etc?	هل هنالك تسجيل محدث وكامل لكل أشرطة النسخ الاحتياطي، الأقراص القابلة للإزالة، الأقراص الممغنطة ...الخ؟
23	3	5	2	1	1		☐	☐	☐	Are archival media duplicated and verified prior to deletion of source data?	هل يتم التأكد من وجود نسختين مؤرشفتين من البيانات قبل محي النسخة الأصلية؟
24	2	4	2	1	1		☐	☐	☐	Are archive tapes periodically verified and re-tensioned?	هل يتم التحقق وإعادة شد الأشرطة المؤرشفة خلال تواتر زمني معين؟

Item No.	Weight					Notes	Findings			Questions	الأسئلة
	Average	Sample1	Sample2	Sample3	Sample4		Partially Applied	No	YES		
25	3	3	4	2	4		☐	☐	☐	Are there appropriate controls to maintain confidentiality of stored data?	هل يتم الحفاظ على سرية البيانات المخزنة بوسائل تحكم مناسبة؟
26	3	2	3	2	6		☐	☐	☐	Are there suitable security controls for exchange of information?	هل يوجد وسائل تحكم أمنية مناسبة لتبادل المعلومات؟
27	4	4	3	4	5		☐	☐	☐	Are there any security arrangements for Internet, Intranet and related systems?	هل يوجد ترتيبات أمنية مناسبة من أجل الإنترنت والإنترانت والأنظمة المتعلقة؟
28	1	1	1	1	2		☐	☐	☐	While using or providing Web-based applications; is there an enforced use of https, for example, to protect sensitive data en route between browser and Web server?	هل يتم مثلاً إلزام استخدام بروتوكول التصفح المشفر https عند استخدام أو توفير التطبيقات العاملة على أساس الويب وذلك لحماية البيانات الحساسة حين توجيهها بين المتصفح ومخدم الويب؟
29	5	4	5	6	7		☐	☐	☐	Are main systems monitored for logging and reporting security incidents?	هل يتم مراقبة الدخول على الأنظمة الرئيسية ورفع تقارير الحوادث الأمنية؟
30	2	3	2	3	1		☐	☐	☐	Is there a process in place for reviewing and responding appropriately to internal or external security alerts?	هل توجد عملية قائمة تتعلق بالمراجعة والاستجابة المناسبة للإنذارات الأمنية الداخلي منها والخارجي؟
31	3	2	3	4	1		☐	☐	☐	Are the logs and reports followed-up with principles of responsibility and accountability?	هل تتم متابعة ملفات الدخول والتقارير باعتماد مبادئ المسؤولية والمحاسبة؟
							Access control (14 Controls)				**التحكم بالوصول والدخول**

Item No.	Weight					Notes	Findings			Questions	الأسئلة
	Average	Sample1	Sample2	Sample3	Sample4		Partially Applied	No	YES		
1	5	6	5	4	5		☐	☐	☐	Are business requirements for access control properly documented and approved by information asset owners?	هل تم التصديق والتوثيق الجيد لمتطلبات الأعمال المتعلقة بالتحكم بالدخول من قبل مالكي (المسؤولين عن) الأصول المعلوماتية؟
2	10	10	12	11	7		☐	☐	☐	Are business requirements for access control (for breadth and depth of coverage) properly included in system security design specifications?	هل تم التضمين الجيد لمتطلبات الأعمال من أجل التحكم بالدخول (تغطية أفقية وعمودية) في المواصفات الفنية الاصة بتصميم نظام الأمن؟
3	8	8	9	9	6		☐	☐	☐	Are access rights normally limited as far as practicable?	هل عادةً ما تكون حقوق الدخول محدودة قدر المستطاع؟
4	7	6	9	8	5		☐	☐	☐	Are access rights regularly reviewed and modified as far as needed?	هل تتم مراجعة وتعديل حقوق الدخول بانتظام حسب الحاجة؟
5	5	5	5	4	6		☐	☐	☐	Is management pay special attention to access/account controls for the users of privileged system-, database-application- & network-managers?	هل تولي الإدارة اهتماماً خاصاً لوسائل التحكم في الدخول/ الحسابات المتعلقة بمستخدمي النظام، قواعد البيانات، التطبيقات ذوي الامتيازات (كامل السماحيات) ومدراء الشبكات؟
6	8	8	8	7	9		☐	☐	☐	Does the organization suffer from abuse of privileges? Is this case classified as a great potential?	هل تعاني المؤسسة من إساءة استخدام تلك الامتيازات؟ هل تصنف هذه الحالة ضمن الاحتمالات العالية؟
7	8	9	7	6	10		☐	☐	☐	Does the organization have password controls?	هل تمتلك المؤسسة وسائل التحكم بكلمات المرور؟

Item No.	Weight					Notes	Findings			Questions	الأسئلة
	Average	Sample1	Sample2	Sample3	Sample4		Partially Applied	No	YES		
8	8	10	7	8	6		☐	☐	☐	Does anyone routinely check for weak passwords and follow-up with user security awareness/training?	هل يتابع أي فرد بانتظام التدقيق لكشف كلمات العبور الضعيفة وتوعية /تدريب المستخدم أمنياً؟
9	6	5	3	8	9		☐	☐	☐	Do authorized individuals effectively limit access to applications/services ?	هل يقوم الأفراد المخولون بحد الدخول إلى التطبيقات /الخدمات بفاعلية؟
10	10	9	10	9	12		☐	☐	☐	Are network nodes authenticated and established distinct security domains using firewalls, key lock-out, etc?	هل تقوم العقد الشبكية بالتحقق وتأسيس مناطق أمنية مختلفة باستخدام جدران الحماية، منع الدخول ...الخ؟
11	2	3	3	2	1		☐	☐	☐	Are session timeouts implemented on the desktop, network, application or operating system levels?	هل تطبق تقنية إلغاء الجلسة بسبب نفاذ الوقت على الحواسب، الشبكات، التطبيقات، أنظمة التشغيل؟
12	10	8	10	9	12		☐	☐	☐	Are suitable access controls in place, including the use of individual user identities, user authentication, automated access controls, encryption, etc?	هل توجد وسائل تحكم بالدخول مناسبة، من ضمنها مثلاً استخدام بطاقات التعريف، التحقق من المستخدم، الوسائل المؤتمتة، التشفير ...الخ؟
13	7	7	7	8	6		☐	☐	☐	Are there any security controls relating to mobile, home users (remote access), laptops, mobile storage devices, VPNs, etc?	هل توجد وسائل تحكم أمنية متعلقة بالجوال، المستخدمين المنزليين (الدخول البعيد)، الحواسب النقالة، وسائل التخزين المتحركة، الشبكات الافتراضية الخاصة ...الخ؟

Item No.	Weight					Notes	Findings			Questions	الأسئلة
	Average	Sample1	Sample2	Sample3	Sample4		Partially Applied	No	YES		
14	6	6	5	7	6		☐	☐	☐	Are portable systems maintained and controlled?	هل يتم الحفاظ على والتحكم بالأنظمة المحمولة؟
							IS acquisition, development and maintenance (13 Controls)				**اكتساب، إعداد، صيانة أنظمة المعلومات**
1	7	9	8	5	7		☐	☐	☐	Do changes trigger security reviews/risk assessments and, if necessary, re-certification of systems?	هل تستدعي التغيرات القيام بمراجعة أمنية /تقييم المخاطر وحتى إعادة ترخيص الأنظمة في حال الحاجة؟
2	7	9	8	6	5		☐	☐	☐	Are formal systemic methods used routinely?	هل يتم استخدام طرق رسمية منهجية بانتظام؟
3	15	15	13	15	17		☐	☐	☐	Are data controls such as input data validation, processing validation, encryption, message authentication etc, employed appropriately?	هل تطبق وسائل تحكم مناسبة من أجل البيانات مثل التحقق من صلاحية المدخلات والمعالجة، التشفير، رسالة التحقق ...الخ؟
4	9	6	5	12	13		☐	☐	☐	Has a formal policy covering the use of cryptographic controls been implemented?	هل تم تطبيق سياسات رسمية تعنى باستخدام وسائل التحكم السرية؟

Item No.	Weight					Notes	Findings			Questions	الأسئلة
	Average	Sample1	Sample2	Sample3	Sample4		Partially Applied	No	YES		
5	9	8	10	7	11		☐	☐ ☐ ☐ ☐ ☐	☐ ☐ ☐ ☐ ☐	If yes, is it covers: • The general principles under which business information should be protected; • Standards to be applied for the effective implementation of crypto; • A process to determine the level of protection to be applied; • Management of crypto keys, including recovery of information in the event of lost, damaged or compromised keys; • Alignment with any documented requirements.	في حال كانت الإجابة نعم، هل تشمل: • أي من معلومات الأعمال تستوجب حمايتها حسب المبادئ العامة. • المعايير الواجبة التطبيق لضمان فعالية تنفيذ وسائل التحكم السرية. • القيام بتحديد مستوى الحماية الواجب تطبيقه. • إدارة مفاتيح السرية بما فيها استرجاع المعلومات في حال ضياع أو تضرر أو انكشاف المفاتيح. • التماشي مع أية متطلبات موثقة.
6	5	6	7	5	3		☐	☐	☐	Are there adequate controls isolating development from testing from production environments?	هل توجد وسائل تحكم كافية لعزل بيئة التطوير عن التجريب عن الإنتاج؟

Item No.	Weight					Notes	Findings			Questions	الأسئلة
	Average	Sample1	Sample2	Sample3	Sample4		Partially Applied	No	YES		
7	10	10	11	9	8		☐	☐	☐	Are changes acceptances built on professional ensuring that new/changed cases do not disrupt other operations?	هل يستند قبول التغييرات على تأكيد المختصين أن التغيرات/ التجديدات لا تعطل العمليات التشغيلية الأخرى؟
8	8	9	8	9	7		☐	☐	☐	Are changes properly documented, justified and authorized by management?	هل يتم توثيق التغيرات وذكر مبررات القيام بها وتصديقها من الإدارة؟
9	4	4	4	3	5		☐	☐	☐	Are tested data derived and protected against disclosure?	هل يتم حماية بيانات الاختبارات بحد ذاتها من الكشف؟
10	5	3	5	7	6		☐	☐	☐	Do control procedures cover significant changes to computing and telecommunications equipment?	هل تعالج إجراءات التحكم مواضيع التغيرات الهامة في الأنظمة الحاسوبية ووسائل الاتصالات؟
11	7	7	7	8	6		☐	☐	☐	Are there suitable processes in place to review the inventory of systems and identify whether announced vulnerabilities are relevant?	هل يوجد عمليات مناسبة تعنى بمراجعة مخزون الأنظمة وهل تم الإعلان عن ثغرات أمنية متعلقة بها؟
12	7	7	6	9	5		☐	☐	☐	Are patches assessed for applicability and risks before being implemented?	هل تقيم الرقع البرمجية (البرمجيات اللاحقة لمعالجة ثغرات البرامج المنصبة) من حيث قابلية تطبيقها ومخاطرها قبل تنفيذها؟

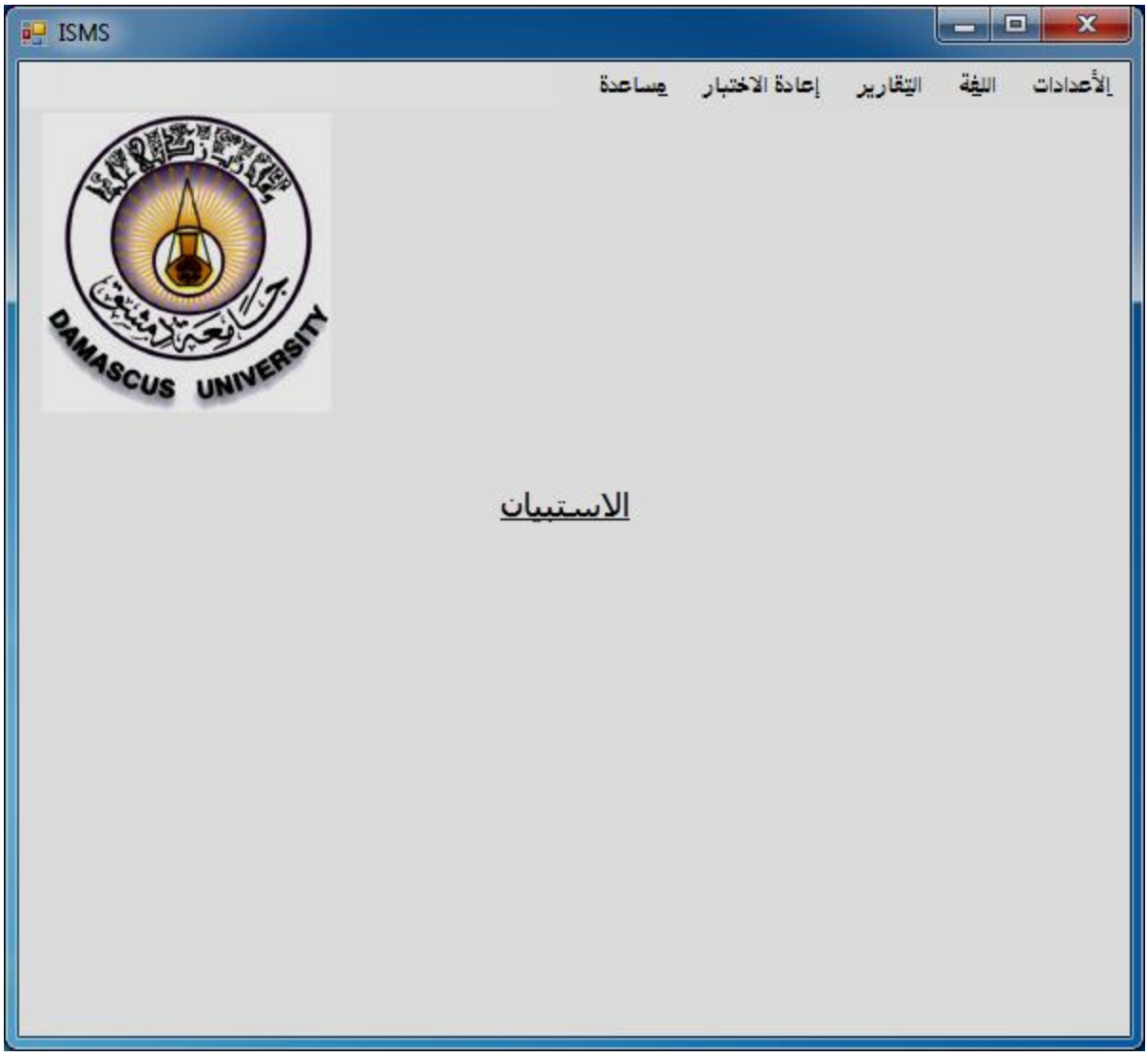
Item No.	Weight					Notes	Findings			Questions	الأسئلة
	Average	Sample1	Sample2	Sample3	Sample4		Partially Applied	No	YES		
13	7	7	8	5	7		☐	☐	☐	Are the processes for implementing urgent patches sufficiently slick and comprehensive?	هل عمليات التطبيق الطارئة للرقع البرمجية مدركة وسهلة بصورة مقبولة؟
							Information security incident management (4 Controls)				**إدارة حوادث أمن المعلومات**
1	30	33	32	30	25		☐	☐	☐	Are those who should be reporting security events and weaknesses aware of, and in fact use, the processes for reporting security events and weaknesses?	هل يتمتع القاطمون على رفع تقارير الحوادث الأمنية ونقاط الضعف بالوعي الكافي لسير عمليات معالجة هذه المهام؟ والأهم من ذلك هل يستخدمونها فعلياً؟
2	25	26	27	20	27		☐	☐	☐	Are the policies, procedures and guidelines followed in reality?	هل يتم الالتزام بالسياسات واللوائح والإرشادات على أرض الواقع؟
3	20	18	19	21	22		☐	☐	☐	Does the organization have a relatively mature incident management process, evaluation/investigation, corrective action and the other parts for managing security incidents and improving protection opportunities in place?	هل لدى المؤسسة معالجة ناضجة نسبياً لإدارة الحوادث، التقييم/ التحقيق، الفعل التصحيحي، والأجزاء الأخرى لإدارة الحوادث الأمنية وتعزيز فرص الحماية؟
4	25	23	22	29	26		☐	☐	☐	Is the organization proactively learning from incidents, improving risk knowledge and security controls accordingly?	هل تجري وبصورة متواصلة عملية التعلم من الحوادث والدعم في معرفة المخاطر ووسائل التحكم الأمنية بناءً على إدارة الحوادث؟

الملحق (3) توصيف البرنامج

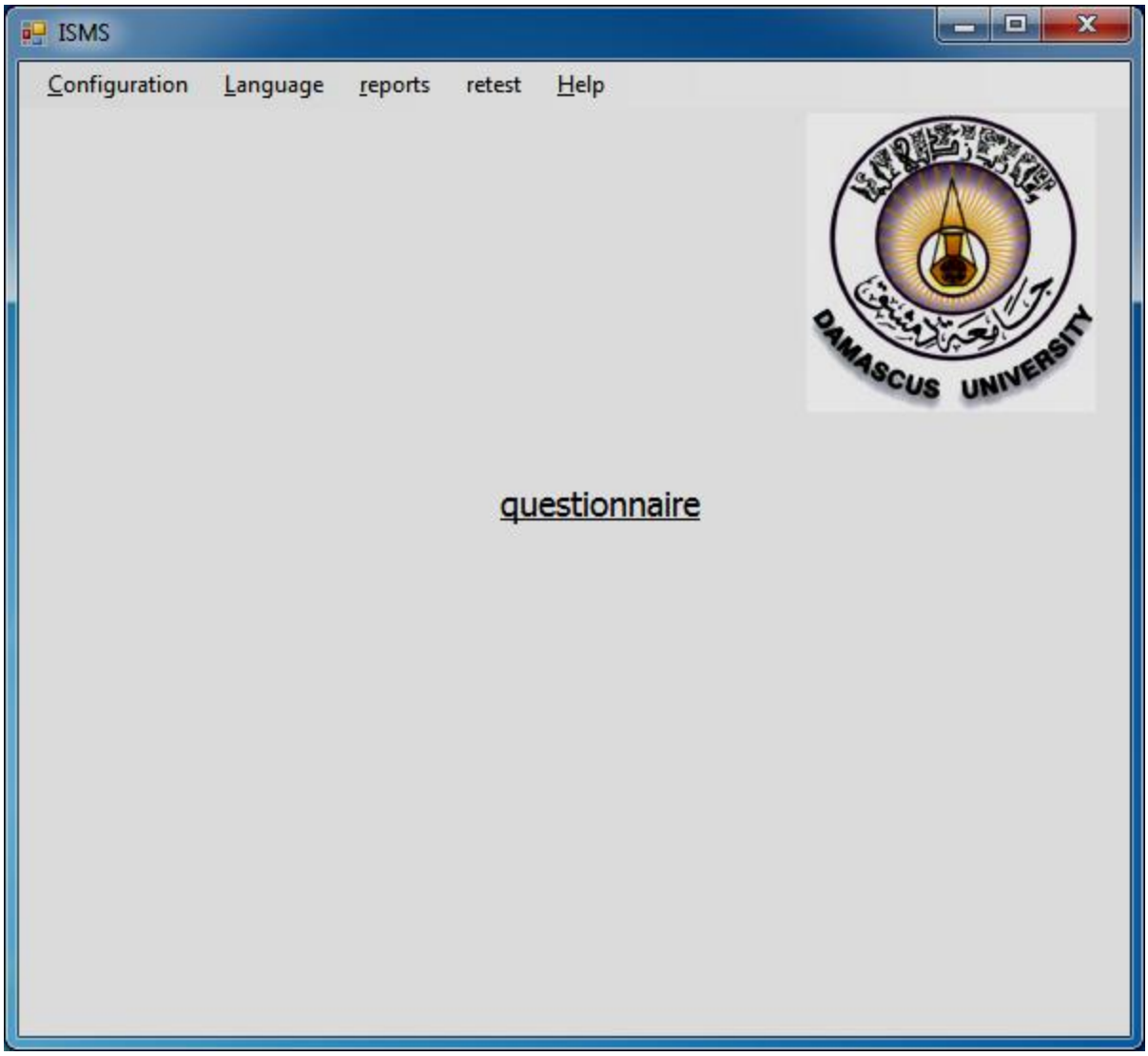
تم تطوير برنامج خاص بالنموذج المقترح يحقق ما يلي:

- تمثيل النموذج المقترح على شكل استعلام الكتروني للمتحكمات الخاصة بكل مجال في طبقات النموذج. مما يسهل تنفيذه و استخراج التقارير التي تبين الفجوة بين النموذج و واقع المؤسسة بالاضافة إلى آلية تجاوز الثغرات.
- يسمح البرنامج باضافة و تعديل و حذف المتحكمات و/أو المجالات مما يجعله مرناً للتطوير المستقبلي.
- يمكن اضافة وثائق تدعم الاجابة مثل خطة أمن المعلومات أو شهادات أو غيرها.
- يمكن إجراء الاستعلام على مراحل و تعديل الإجابات السابقة بعد إجراء تعديلات أو في حال التأكد من الاجابة.
- يقوم البرنامج باحتساب آلي –رقمي– لمستوى أمن المعلومات من خلال تطبيق المعادلة المقترحة. و تضمين التقرير النهائي لهذا القياس.
- يدعم البرنامج اللغتين العربية و الانكليزية.

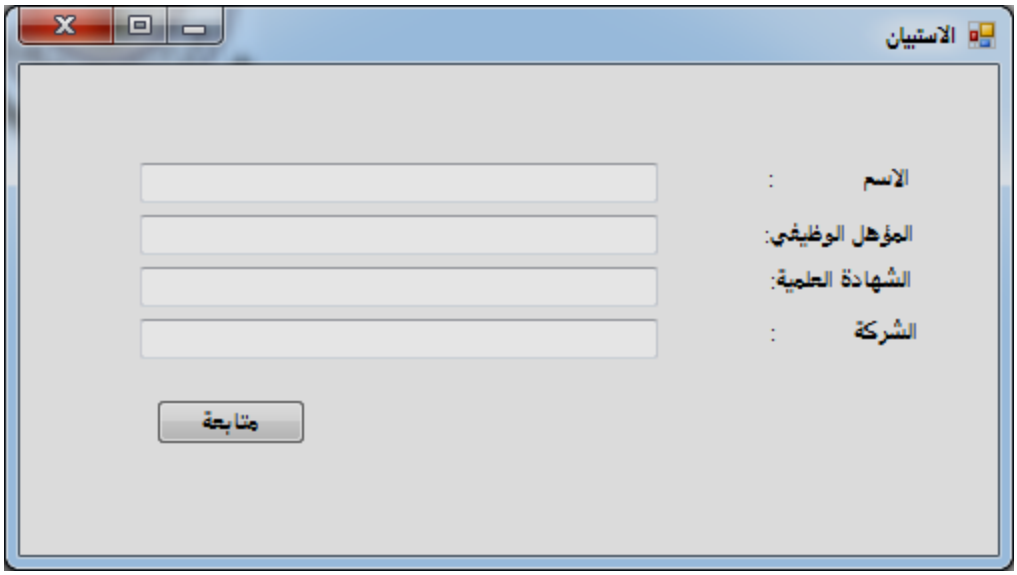
و قد تم تطوير البرنامج بلغة البرمجة C# .NET و باستخدام قواعد بيانات MS SQL 2005.
و نعرض فيما يلي بعض واجهات البرنامج.



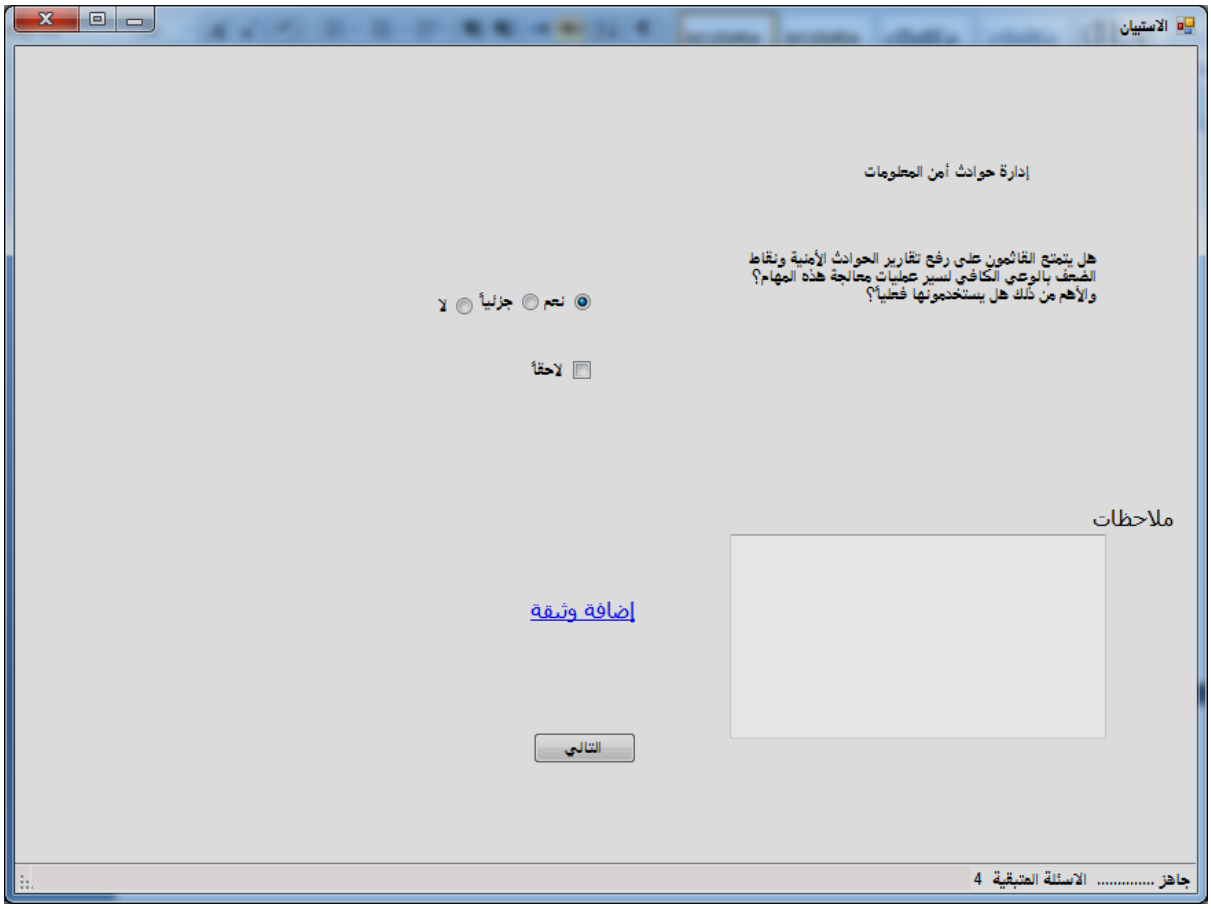
الشكل 34 الواجهة الأساسية باللغة العربية



الشكل 35 الواجهة الأساسية باللغة الانكليزية

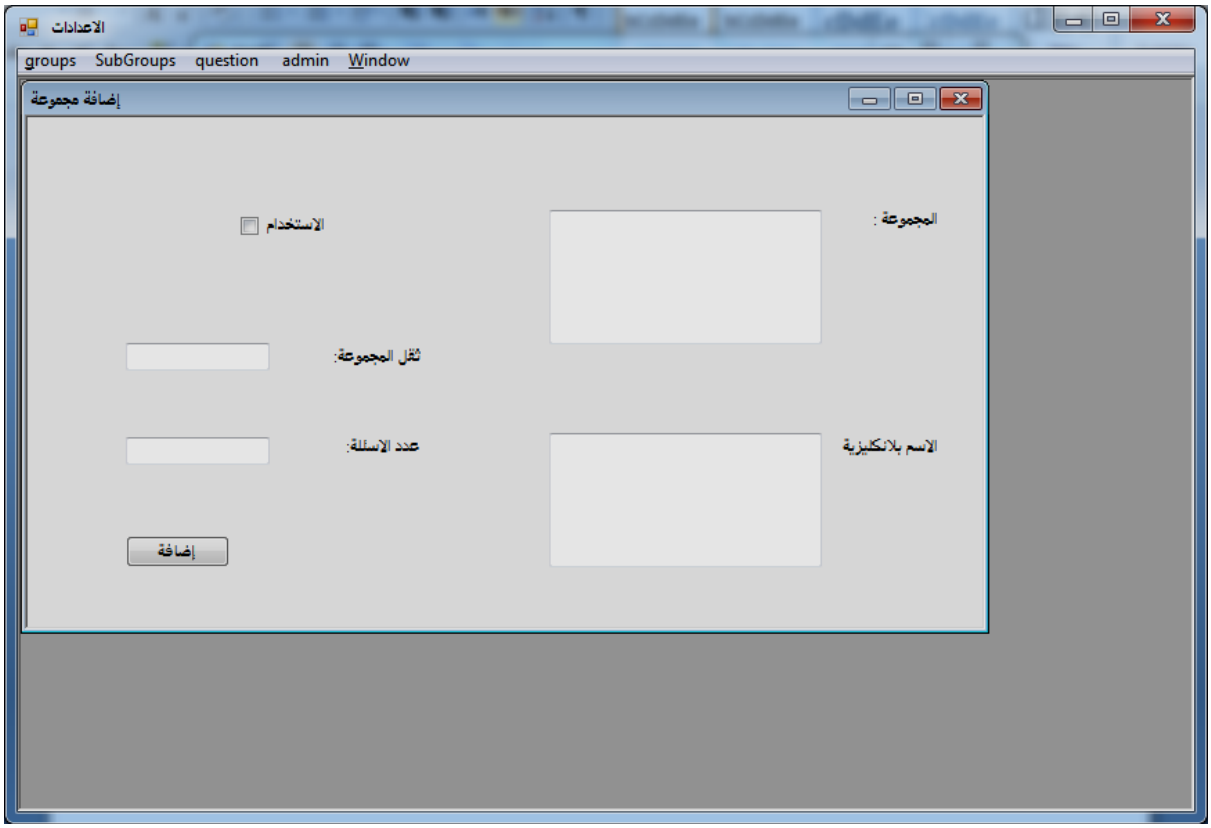


الشكل 36 واجهة إدخال معلومات منفذ الاستعلام

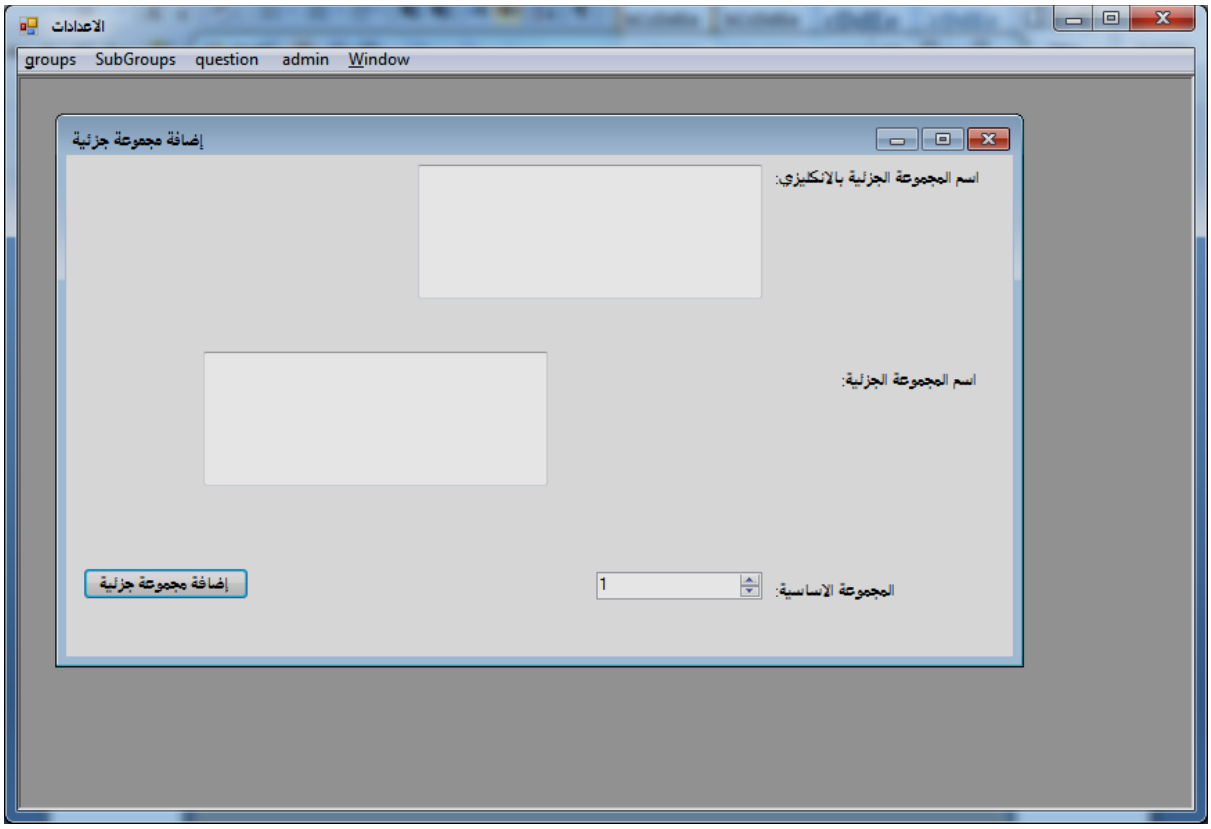


الشكل 37 مثال على إحدى المتحكمات ضمن مجال إدارة حوادث أمن المعلومات

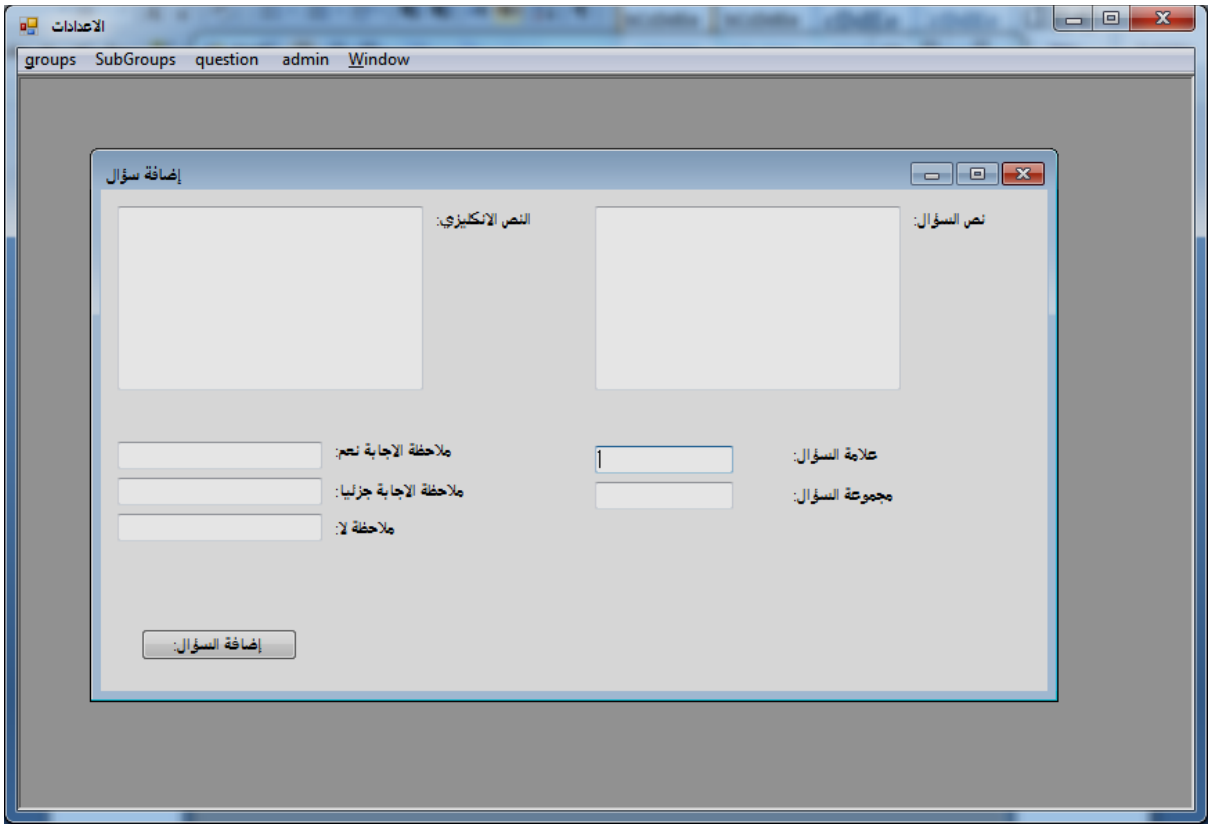
الشكل 38 تعديل إعدادات البرنامج



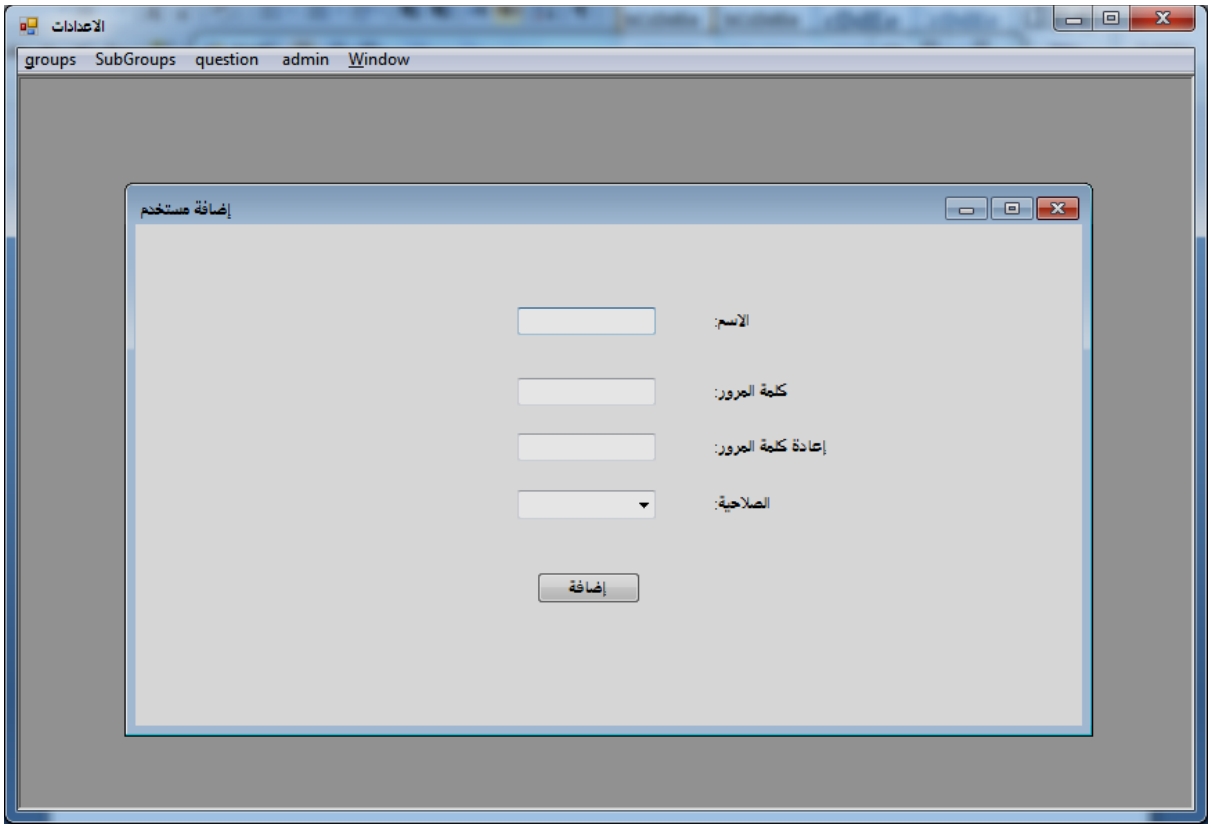
الشكل 39 إضافة مجموعة جديدة من المتحكمات –مجال جديد–



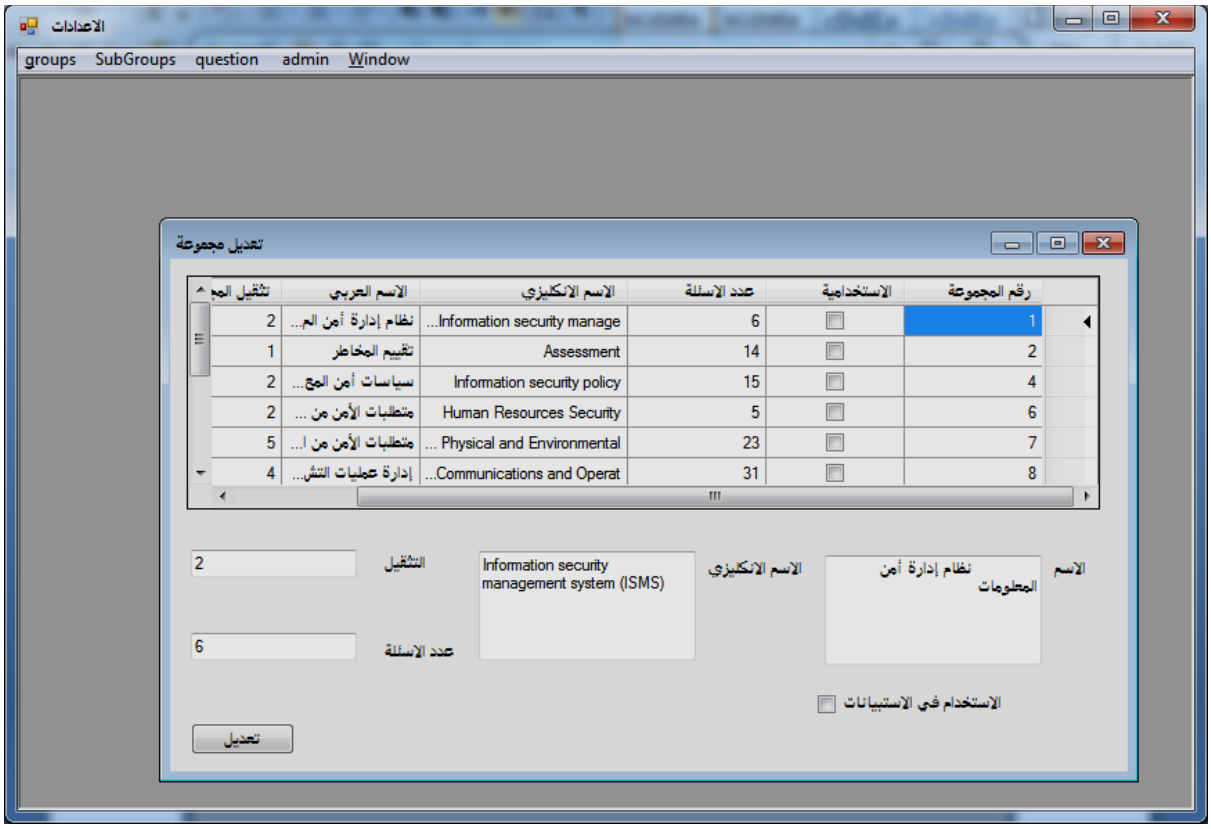
الشكل 40 إضافة مجموعة فرعية ضمن المجال



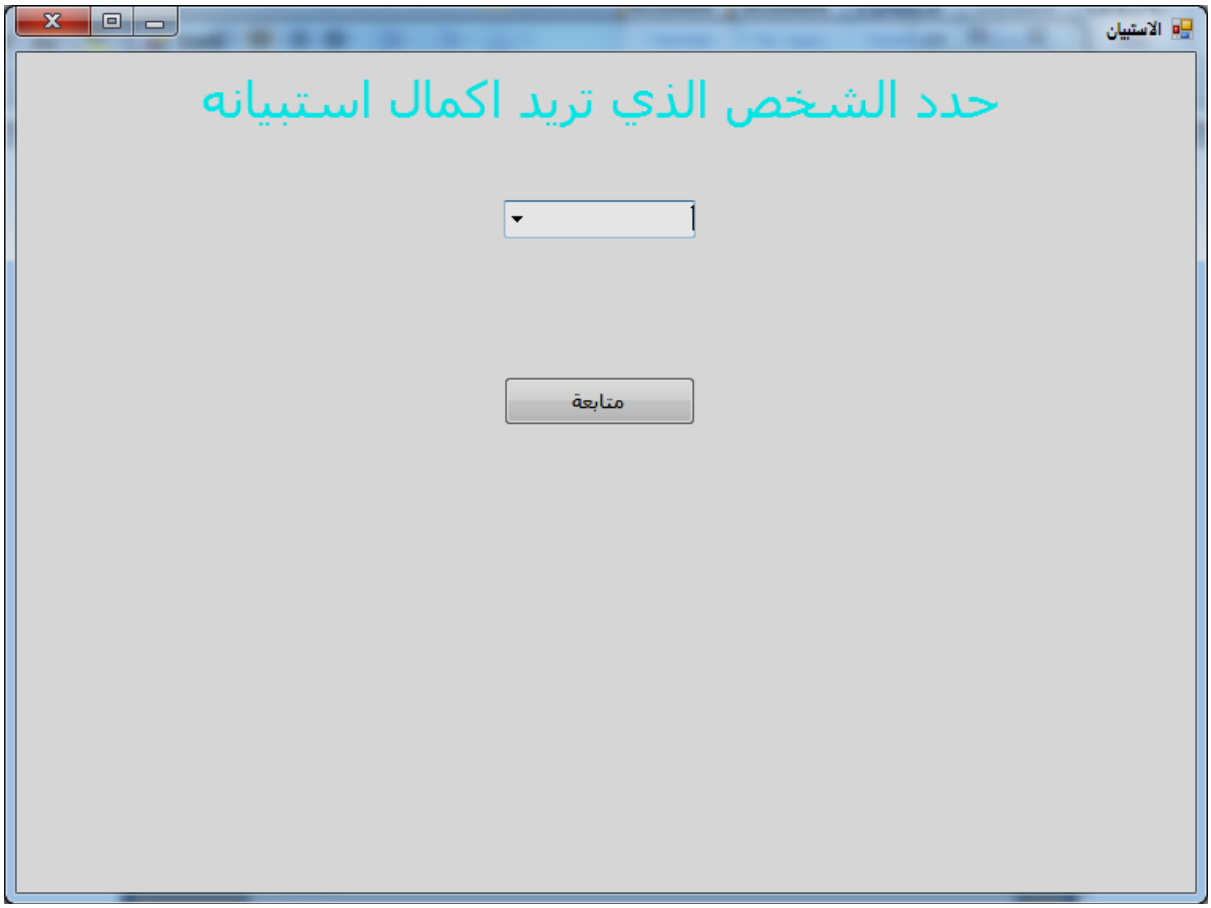
الشكل 41 تعديل المتحكمات



الشكل 42 إدارة المستخدمين



الشكل 43 إمكانية إدخال جزئي لبعض المجالات فقط



الشكل 44 استكمال استعلام سابق

نموذج عن التقارير التي يولدها البرنامج

الأمن من الناحية الفيزيائية والبيئية

- المناطق الأمنية
  - محيط الأمن الفيزيائي
  - وسائل التحكم بالمدخل الفيزيائي
  - تأمين الغرف والمكاتب والمرافق
  - الحماية من التهديدات الفيزيائية الداخلية والخارجية
  - العمل في المناطق الأمنية
  - أماكن الدخول والتسليم والتحميل العامة
- أمن المعدات
  - وضع وحماية المعدات
  - الأدوات الداعمة
  - أمن الكبلات
  - صيانة المعدات
  - أمن المعدات خارج المصرف
  - أمن المعدات المنسقة أو المعاد استخدامها
  - ترحيل الملكية

متطلبات الأمن من الناحية البيئية والفيزيائية	نعم	لا	ملاحظات
هل تم وضع وسائل حكيمة لتقليل احتمالات الكوارث أو تكاليف الحلول الوقائية؟	☒		
هل البناء يوحي بالأمن من الناحية الفيزيائية، مثلاً جدران متراصفة، أبواب سميكة صلبة ...الخ؟		☒	
هل تطبق أنظمة مناسبة للتحكم بالدخول والإجراءات المقابلة لها؟	☒		المقر الرئيسي فقط

هل هنالك إجراءات حماية فيزيائية مناسبة للكبلات الخارجية، علب القواطع، مبرد المكيفات، اللواقط، مداخل التهوية...الخ ضد الأضرار غير المتعمدة أو الدخول عنوة؟		☒	
هل هناك أية وسائل حماية/ تحكم تتعلق بالحرائق أو الدخان مثل الأسلاك ومواد البناء المقاومة للحريق/ قليلة إصدار الدخان؟	☒		المقر الرئيسي وبعض الفروع
هل يوجد تدخين في المكان؟		☒	
هل توضع إشارات عدم التدخين بوضوح؟	☒		
هل يتم فحص وصيانة أنظمة الإنذار ضد الحرائق والقفل بصورة منتظمة من قبل أخصائيين؟		☒	
هل يوجد توعية كافية حول إجراءات الإخلاء عند حدوث الحريق؟		☒	
هل هنالك ما يكفي من وحدات عدم انقطاع التيار الكهربائي تغطي سعاتها كافة التجهيزات الحاسوبية الأساسية والمحيطية وتفرعاتها؟	☒		
هل هنالك مولدة كهربائية احتياطية ذات سعة كافية؟	☒		
هل هنالك طاقة تبريدية كافية لمعالجة الحمل الحراري؟	☒		لا يوجد مؤشرات معتمدة
هل هنالك ما يكفي من القطع الاحتياطية أو المحمولة المتاحة لدعم المرونة والصيانة الدورية دون تأثر الخدمة؟	☒		

هل تتوفر حساسات حرارية تدعم القراءة من بعيد وإنذارات زيادة درجة الحرارة إضافةً إلى إجراءات الطوارئ؟		☒	
هل يوجد نظام منع وكشف وإنذار بعيد حول تسرب المياه وطوفانها؟		☒	
هل يتم المحافظة على شروط نظافة غرف التجهيزات و الاتصالات؟	☒		بدون التجهيزات
هل توجد معالجة خاصة لتجنب الغبار؟		☒	
هل تم تثبيت كافة الهياكل المعدنية المكشوفة وربطها إلى نقطة تأريض لأغراض السلامة وتقليل الكهرباء الساكنة؟	☒		بدون تقييم الجودة
هل تم رفع كافة قواطع الإضاءة، عوازل الكبلات، قواطع الطاقة الكهربائية ...إلخ حين توفر الإمكانية؟	☒		
هل يتم تشغيل وصيانة كافة التجهيزات الفيزيائية واختبارها تحت الحمل على أساس المواصفات الفنية التي حددتها الجهة الصانعة؟	☒		
هل تتبع كافة وسائل التحكم الفيزيائية التغيرات الكبيرة؟		☒	غير قابلة للتغيير
هل يوجد عملية مصرحة إدارياً لزوم إزالة الأصول المعلوماتية من موقع ما؟	☒		
هل هنالك أية عمليات آمنة من أجل مسح البيانات الحساسة والشخصية كاملةً من وسائط التخزين الثابتة أو القابلة للإزالة قبل التصرف بها؟		☒	

تحليل الهوة

يجب تطبيق وصيانة وتغيير وفحص واختبار العديد من الحمايات الفيزيائية الموجودة، على سبيل المثال لا الحصر:

- الحمايات في الفروع.
- بعض الحمايات من ناحية الإنشاءات المدنية.
- الحماية من تسرب المياه والطوفان.
- مكافحة الغبار.

الخطوات التطبيقية الهامة

الغاية

يجب منع كافة عمليات اقتحام أو ضياع أو تخريب أو إعاقة طوق المصرف وبنيته التحتية، أو مقاطعة مجرى عملياته التشغيلية الحرجة عن طريق وسائل التحكم الفيزيائية والبيئية المناسبة للمخاطر المعرفة وقيمة الأصول المحمية.

الطوق الأمني الفيزيائي

يجب أن يستخدم الطوق الأمني الفيزيائي من أجل حماية المناطق الحساسة التي تحتوي المعلومات ووسائل معالجتها. يجب تصميم وتنفيذ الحماية الفيزيائية للمكاتب والغرف والمنشآت الأخرى بحيث تتناسب مع المخاطر المُعرَّفة وقيمة الأصول المحتملة الإصابة في كل موضع، يتضمن ذلك:

- تعريف وتحديد النطاق بوضوح، ما عدا في الحالات التي تتطلب الإخفاء والتمويه من الناحية الأمنية.
- وضع القيود على المعلومات المتعلقة بالمنشأة عندما تدعم الأمن بما فيها دليل وموقع المعلومات.

استخدام الجدران والنوافذ والأبواب المحمية بواسطة القضبان والأقفال وأجهزة الإنذار وأية أدوات أخرى مناسبة.

- التحكم بأبواب وبوابات المداخل عن طريق عناصر مكتب الاستقبال أو أجهزة القفل المؤتمتة للتحكم بالعبور إلى المناطق المحظورة.
- استخدام حواجز فيزيائية إضافية حين الحاجة لمنع الدخول غير المصرح له أو التخريب الفيزيائي.

- تأمين احتياطي حماية مناسب لمواجهة النيران أو تسرب المياه أو أية تهديدات بيئية منطقية أخرى.
- استخدام أنظمة كشف الاختراق المناسبة مثل كاشف الحركة وطوق الإنذارات والمراقبة عن طريق الصوت والصورة.
- مراعاة تأمين تكرارية كافية حين التصميم لتلافي وجود نقطة إخفاق وحيدة لا تناسب الحماية الأمنية.

وسائل التحكم بالمدخل الفيزيائي

يجب أن تتم حماية مناطق تواجد وسائل معالجة المعلومات الحساسة عن طريق وسائل التحكم على المداخل للتأكد من عدم تمكن أي كان من الدخول إليها ما عدا أولئك المصرح لهم. يجب تصميم وتنفيذ الحماية الفيزيائية للمكاتب والغرف والمنشآت الأخرى بحيث تتناسب مع المخاطر المُعرَّفة وقيمة الأصول المحتملة الإصابة في كل موضع، يتضمن ذلك:

- تطبيق كلمة المرور وطريقة التحقق الثنائية (الكرت المفتاح ورقم التعريف الشخصي مثلاً) عند نقاط العبور.
- تطبيق طرق تحقق إضافية مؤتمتة مع طاقم أمني في المكان عند وجود أصول عالية الحساسية.
- تسجيل تاريخ ووقت الدخول والخروج أو /و تصوير ما يجري في منطقة العبور عند اللزوم.
- إلزام الطاقم المخول له على ارتداء بطاقات تعريف ظاهرة للعيان وتسجيل الأشخاص الذين لا يحملون مثل هذه البطاقات.
- إجراءات تحقق ومراقبة خاصة بطاقم الأطراف العقدية الثالثة الذين لا بد من إعطائهم حق الدخول إلى المناطق المحظورة.
- المراجعة الدورية وإلغاء حقوق الدخول إلى المناطق الأمنية عند اللزوم (راجع أيضاً الأمن والموارد البشرية).
- استخدام وسائل تحكم ظاهرة بوضوح للعيان لغرض الردع.
- استخدام وسائل وأدوات تحكم غير بارزة أو حتى مخفية للأصول عالية الحساسية.

الحماية من التهديدات البيئية الخارجية

يجب تصميم وتنفيذ وسائل الحماية الفيزيائية ضد أخطار النيران والطوفان والعواصف والزلازل والانفجارات والعصيان المدني وكل أشكال المخاطر الأخرى الطبيعية منها وتلك ذات المنشأ البشري، يتضمن ذلك:

- الاهتمام باحتمالات حدوث أصناف مختلفة من المخاطر وقيمة الأصول المطلوب حمايتها منها.
- الاهتمام بالتهديدات الأمنية الناجمة عن المرافق والمباني المجاورة.
- تأمين تجهيزات وأدوات مضادة أخرى (أجهزة إطفاء الحريق مثلاً) ووضعها في الموقع بصورة مناسبة.
- تأمين مواقع خارجية أو بعيدة لنسخ البيانات والنسخ الاحتياطي لوسائل معالجة المعلومات.

العمل في المناطق الحساسة

يجب تصميم وتنفيذ أدوات وإرشادات الحماية الخاصة بالعمل في المناطق الحساسة، من مثل:

- تقليص عدد الطاقم الذي يعلم بوجود ويعمل في الموقع الحساس إلى حدوده الدنيا على قاعدة الحاجة إلى المعرفة /الحاجة إلى العمل.
- تحديد أو منع العمل غير المراقب أو الذي يتم دون إشراف في المناطق الحساسة لضرورات السلامة وتجنب فرص حدوث الأخطاء والأعمال غير المشروعة.
- الحفاظ على فضاء هذه المناطق مقفلاً، وتفحصه دورياً أو /و مراقبته عن بعد بواسطة الفيديو والتقنيات الأخرى.
- الحد من استخدام تجهيزات التسجيلات الصوتية والمرئية في هكذا مناطق، بما فيها الكاميرات الموجودة في الحواسب المحمولة.

معابر الدخول والتسليم والتحميل العامة

يجب التحكم في نقاط العبور مثل مناطق التسليم والتحميل أو أية نقاط أخرى قد يلج من خلالها أشخاص غير مصرح لهم بالدخول إلى هذه المناطق، يتضمن ذلك:

الحد من إمكانية الدخول إلى مناطق التسليم والتحميل وغيرها من المرافق العامة إلى الدرجة التي لا تتعارض مع عمليات التشغيل.

تفحص المواد القادمة والخارجة والفصل بين مساريها حين توفر الإمكانية.

عزل هذه المناطق عن مناطق تخزين المعلومات ووسائل معالجتها حين توفر الإمكانية.

وضع وحماية المعدات

يجب أن يتم وضع وحماية المعدات بشكل يقلل التهديدات والأخطار البيئية، وكذلك التهديدات البشرية بواسطة الدخول غير المصرح له، وقد يتضمن ذلك:

- الحد من مخاطر سوء حماية الأجهزة، وتقليل الحاجة للدخول غير المصرح له إلى المناطق الحساسة.
- عزل المواد التي تحتاج إلى حماية خاصة لتخفيض مستوى الحماية العام المطلوب.
- تفصيل وسائل التحكم حسب الحاجة للحد من التهديدات الفيزيائية لأدنى درجة، مثل السرقة أو الضرر الناجم عن التخريب والنيران وتسرب المياه والغبار والدخان والاهتزازات وتراوح الطاقة الكهربائية والإشعاعات الالكترومغناطيسية، الخ.
- الإرشادات المتعلقة بتناول الطعام والمشروبات والتدخين على مقربة من التجهيزات.

الأدوات الداعمة

يجب أن تتم حماية الأجهزة من انقطاع التيار الكهربائي والاتصالات وغيرها من الأعطال الناجمة عن انقطاع التزويد بالأدوات الداعمة مثل المياه والصرف الصحي، يتضمن ذلك:

- التأكد من كفاية الأدوات الداعمة في ظروف التشغيل الطبيعية.
- وجود احتياطي منطقي من التجهيزات المتكررة والداعمة (مثل وحدات عدم انقطاع التيار الكهربائي) في حال حدوث انقطاع ما.

أمن الكبلات

يجب حماية كبلات الكهرباء والاتصالات التي تنقل بيانات حساسة أو خدمات المعلومات الداعمة من التدخل أو الضرر، بما في ذلك:

- أدوات فيزيائية تمنع حدوث التدخل غير المصرح له أو الضرر، بما في ذلك تطبيق حماية إضافية على الأنظمة الحساسة أو الحرجة.
- بدائل واستحياطات لوسائط النقل أو التوجيه، تحديداً للأنظمة الحرجة.
- عنونة الكبلات والتجهيزات بصورة واضحة، ما عدا في الحالات التي تفرض إزالتها أو إخفاءها لمزيد من الأمن.

- توثيق عمليات تنزيل الرقع البرمجية وعمليات الصيانة الأخرى.

صيانة المعدات

يجب أن يُحافَظ على التجهيزات بصورة سليمة لضمان استمرارية إتاحيتها وصحتها، يتضمن ذلك:

- صيانة قوة الممانعة كما تم وصفها من المصنع أو سلطات التشريع والترخيص.
- توثيق كل عمليات الصيانة، بما فيها صيانة قوة الممانعة.
- توثيق كل الهفوات الموجودة أو المشتبه بها، والعلاج المرافق، بالتوازي مع سياسة إدارة الحوادث.
- الصيانة من خلال إما موظفين مصرح ومرخص لهم، أو طرف عقدي ثالث.
- اعتماد معايير أمنية مناسبة مثل إزالة المعلومات أو مراقبة عملية الصيانة بما يتناسب مع حساسية المعلومات أو التجهيزات التي تتم صيانتها.

ترحيل الأملاك إلى خارج المنشأة

لا يجوز إخراج أي تجهيزات أو معلومات أو برامج دون تصريح مسبق ومقيد، يتضمن ذلك:

- الحد من نوع أو كمية المعلومات أو من نوع المعدات المسموح إخراجها.
- تسجيل تصاريح الإخراج ومخزون المعدات والمعلومات التي يتم إخراجها.
- يجب القيام بالتوعية المناسبة حول المخاطر الأمنية المرافقة لخروج المعلومات أو المعدات إلى البيئة الخارجية، والتدريب حول وسائل مواجهتها ووسائل التحكم للأشخاص المصرح لهم بإخراجها.

أمن الأملاك خارج المنشأة

يجب تطبيق معايير أمنية ملائمة على المعدات خارج مرافق المصرف مع الانتباه إلى اختلاف المخاطر حينها، يتضمن ذلك:

- التصريح لأي معالجة خارجية أو معلومات حول المصرف، بغض النظر عن صاحب أجهزة المعالجة.
- وسائل تحكم أمنية للمعدات الموجودة في المرافق الانتقالية أو الخارجية، بما يتلائم مع وضع وحساسية المعلومات الموجودة فيها أو التي قد يتم عبرها الدخول إليها.
- تأمين كافي، حين يحقق هذا التأمين وفر في التكاليف.

- توعية الموظفين والمتعاقدين عن مسؤوليتهم حيال حماية المعلومات والتجهيزات أيضاً، ومخاطر البيئة الخارجية الخاصة.

أمن المعدات المنسقة أو المعاد استخدامها

يجب فحص كافة المعدات ذات وسائط التخزين وتجهيزات وسائط التخزين المستقلة للتأكد من خلوها من أية بيانات حساسة أو برامج مرخصة، يتضمن ذلك:

- استخدام طرق مقبولة عموماً لإزالة المعلومات بصورة آمنة تلائم المعلومات الحساسة الموجودة أو التي يشك بوجودها على وسائط التخزين.
- قيام عناصر مدربة بذلك، أو التحقق من ذلك بواسطة عناصر مدربة.

مسرد المصطلحات Glossary

النفاذ Access

القدرة على الاستفادة من أي مورد من موارد نظام معلومات.

ضبط النفاذ Access Control

تمكين الاستخدام المرخص به للموارد ومنع الاستخدام غير المرخص أو الاستخدام بطريقة غير مرخصة.

المحاسبة Accountability

غاية الحماية التي ينتج عنها إمكانية تتبع متطلبات أعمال جهة ما من قبل هذه الجهة وحدها. وهذا يدعم عدم الرفض، والمنع، وعزل الأخطاء، واكتشاف الاختراق ومنعه، والاستعادة بعد العمل والإجراءات القانونية.

الاعتمادية Accreditation

الإعلان الرسمي من قبل الجهة المقرة بأن تطبيقاً رئيسياً أو نظاماً للدعم العام قد حصل على الموافقة ليبدأ بالعمل مستخدماً الإجراءات الوقائية المحددة مسبقاً في بيئة تشغيلية محددة. يتم اتخاذ قرار الاعتماد بناءً على شهادة الكادر الفني المعين بأن النظام يحقق المتطلبات الفنية المحددة مسبقاً من أجل تحقيق الحماية الكافية بعد تنفيذ مجموعة من ضوابط الحماية التي تم إقرارها.

الضمان Assurance

يهيئ الأرضية للثقة بأن أهداف الحماية الأربعة الأخرى (السلامة، والتوافر، والسرية والمحاسبة) قد تحققت على نحوٍ كافٍ من خلال التنفيذ المحدد.

الجهة المقرة Approving Authority

مسؤول مكتب حماية المعلومات الذي يتمتع بالسلطة التي تخوله التصريح بمعالجة (اعتماد) معلومات مؤتمتة (تطبيق رئيسي) أو (نظام دعم عام) وقبول المخاطرة المرتبطة بالنظام.

التشفير غير المتناظر Asymmetric Cryptography

التشفير بمفتاح عمومي: وهي فرع حديث من فروع الكتابة بالشيفرة تستخدم الخوارزمية فيها زوجين من المفاتيح (عام وخاص) وتستخدم مكوناً مختلفاً لهذا الزوج في كل خطوة من خطوات الخوارزمية.

التدقيق Audit

مراجعة وفحص رسميين (مستقلين عادةً) لمشروع أو نشاطات مشروع من أجل تقييم الوفاء بالالتزامات التعاقدية.

سجل التدقيق Audit Trial

سجل نشاطات النظام بحسب التسلسل الزمني من أجل ضمان إعادة بناء وفحص تسلسل الأحداث و/أو التغيرات في حدثٍ ما. و يمكن أن تنطبق سجلات التدقيق على المعلومات في نظامٍ للمعلومات، أو ضوابط وسائط الإدخال/الإخراج، أو رسالة موجهة في نظام اتصالات، أو نقل مواد حماية الاتصالات أو سجل يبين هوية الداخلين إلى النظام. ويمكن سجلات التدقيق أن تؤمن الوسائل اللازمة لإنجاز العديد من الأهداف المتعلقة بالحماية بما فيها المسؤولية الفردية، وإعادة بناء الأحداث، واكتشاف الاختراق وتحديد المشاكل إذا ما اقترنت بالإجراءات والأدوات المناسبة.

الأصالة Authenticity

خاصية كون الشيء حقيقياً ويمكن التحقق منه والثقة به، ضمان صحة الإرسال، أو الرسالة أو المُنشئ داخل نظام المعلومات.

إثبات الأصالة Authentication

التحقق من هوية المستخدم والعملية أو الجهاز غالباً كشرط مسبق من أجل السماح بالنفاذ إلى المعلومات في نظامٍ للمعلومات.

التخويل Authorization

منح أو حجب حقوق النفاذ لمستخدم، أو برنامج أو عملية.

تخويل المعالجة Authorize Processing

وهي العملية التي تحدث عندما تصدر الإدارة تصريحاً خطياً لنظام ما بالعمل بناءً على تقييم ضوابط الإدارة والضوابط الفنية والتشغيلية. وعندما يسمح مسؤول الإدارة بعمليات المعالجة في النظام فإنه بذلك يقبل المخاطر المرتبطة بذلك.

مسؤول التخويل Authorizing Official

عضو مكتب حماية المعلومات الذي يتمتع بالصلاحيات التي تخوله تولي المسؤولية الرسمية عن تشغيل نظام المعلومات عند مستوى مقبول من المخاطرة على عمليات المديرية (متضمنةً المهمة، والوظائف، والصورة والسمعة)، وأصولها أو أفرادها.

الجاهزية (الإتاحية) Availability

الجاهزية تعني: مدى جاهزية النظام (أو جزء من النظام) للعمل وإمكانية النفاذ إليه عند الحاجة لاستخدامه.
ضمان النفاذ إلى المعلومات واستخدامها في الوقت المناسب وبشكل موثوق.

التوعية Awareness

طريقة تعليمية تهيئ الأرضية للتدريب من خلال تغيير مواقف الأشخاص والمؤسسات لإدراك أهمية الحماية والنتائج السلبية لفشلها.

النسخ الاحتياطي Backup

نسخ ملفات البرمجيات على وسائط مختلفة يمكن تمييزها عن الملفات الأصلية وتستخدم لاستعادة الملفات الأصلية في حال الضرورة.

الأساس Baseline

نتائج العمل (مثل البرمجيات والوثائق) التي تمت مراجعتها والموافقة عليها وتسليمها بشكل رسمي ولا يمكن تغييرها إلا من خلال إجراءات ضبط التغيير الرسمية.

البيولوجيا الإحصائية Biometric

صورة أو قالب لخاصية سيكولوجية (مثال: بصمة الإصبع) يمكن استخدامها لتحديد هوية فردٍ ما. ويمكن استخدام البيولوجيا الإحصائية لفك رموز الأصالة ومنع رفض التسجيل.

خطة استمرارية المشروع Business Continuity Plan

وثائق محددة مسبقاً من التوجيهات أو الإجراءات تشرح كيفية الاستدامة لوظائف عمل المؤسسة أثناء وبعد حدوث توقف كبير.

منح الشهادة Certification

تقييم شامل للإدارة وضوابط الحماية الفنية والتشغيلية في نظامٍ للمعلومات وضعت لمساندة اعتماد الحماية بهدف تحديد مدى صحة تنفيذ الضوابط وعملها كما هو مطلوب بالإضافة إلى تقديم النتيجة المرجوة فيما يتعلق بتحقيق متطلبات حماية النظام.

الموقع البديل Cold Site

وحدة نسخ احتياطية تحتوي على المكونات الكهربائية والفيزيائية لوحدة الكمبيوتر، ولكنها لا تحتوي على أجهزة كمبيوتر. ويكون هذا الموقع جاهز لاستقبال أجهزة الكمبيوتر البديلة الضرورية في حال احتاج المستخدمون إلى الانتقال من الموقع الرئيسي لعملهم في الأتمتة إلى موقعٍ بديل.

Computer Aided Software Engineering

أداة من أدوات هندسة البرمجيات بمساعدة الحاسوب تكون عبارة عن بيئة متكاملة يمكنها أن تغطي كامل مراحل التطوير البرمجي.

السرية Confidentiality

ضمان عدم الكشف عن المعلومات لأشخاص أو عمليات أو أجهزة غير مصرح لها بذلك.
الحفاظ على القيود المعتمدة فيما يتعلق بالنفاذ إلى المعلومات وكشفها، بما فيها وسائل حماية الخصوصية الشخصية إضافةً إلى المعلومات الخاصة.

إدارة التشكيلات Configuration Management
الالتزام بتعريف تشكيلات المكونات الصلبة وأنظمة البرمجيات في كل مرحلة من مراحل دورة الحياة بهدف التحكم بتغيرات التشكيل والحفاظ على سلامة وقابلية متابعة التشكيل خلال كامل دورة الحياة. ويمكن أن تتضمن عناصر تشكيل المكونات الصلبة، والبرمجيات، والبرمجيات الثابتة، والاتصالات، والوثائق، والاختبار، وملحقات الاختبار بالإضافة إلى وثائق الاختبار.

خطة الحالات الطارئة Contingency Plan
وثيقة رسمية تؤسس لاستمرار عمليات التشغيل في حال وقوع كارثة. تتضمن أسماء الأطراف المسؤولة التي يجب الاتصال بها والبيانات التي يجب أن تتم استعادتها وموقعها.
سياسة الإدارة والإجراءات المصممة للحفاظ على العمليات واستعادتها، بما في ذلك تشغيل الكمبيوترات، وربما في موقعٍ بديل، في الحالات الطارئة أو حالات فشل النظام والكوارث.

الأصول الحدية Critical Assets
الأصول المادية والمعلومات المطلوبة لإنجاز مهمة في الموقع.

البنية التحتية الحدية Critical Infrastructure
الأنظمة المادية والأنظمة العاملة على المعلوماتية التي تعتبر أساسية للحد الأدنى من عمليات الاقتصاد والحكومة.

حماية البنية التحتية الحدية Critical Infrastructure Protection

الأنظمة المادية والأنظمة العاملة على المعلوماتية التي تعتبر أساسية للحد الأدنى من عمليات الاقتصاد والحكومة. وتتضمن، على سبيل المثال لا الحصر، الاتصالات، والطاقة، والصناعة المصرفية والمالية، والنقل، وأنظمة المياه وخدمات الطوارئ الحكومية والخاصة.

سلامة البيانات Data Integrity

خاصية أن البيانات لم تتعرض لأي تعديل غير مصرح به، وتغطي البيانات المخزنة وأثناء المعالجة والمرحلة التي تكون فيها البيانات قيد الإرسال.

رفض الخدمة Denial of Service

منع النفاذ المصرح به إلى الموارد أو تأخير العمليات ذات الحساسية الزمنية العالية.

مرحلة التصميم Design Phase

وهي الفترة في دورة حياة تطوير النظام التي يتم خلالها إعداد وتوثيق والتحقق من تصاميم البنية، ومكونات البرمجيات، والواجهات والبيانات من أجل تحقيق متطلبات النظام.

مرحلة التطوير Development Phase

وهي الفترة في دورة حياة تطوير النظام التي يتم خلالها تحويل نتائج مرحلة التصميم إلى نظام كامل.

التوقيع الالكتروني Digital Signature

الرمز (رقم) المقابل لرسالة يحدد بطريقة وحيدة مرسل الرسالة ويثبت أن الرسالة لم تتغير منذ الإرسال.

خطة الاستعادة بعد الكوارث Disaster Recovery Plan

خطة مكتوبة تحدد إجراءات الاستعادة في حالة الكوارث بفعل الطبيعة أو الإنسان والتي تؤثر على توافر النظام. ويتم اختبار هذه الخطة سنوياً لضمان فعاليتها وكفاءتها.

التوقف Disruption

حدث غير مخطط له يسبب توقف عمل النظام العام أو التطبيق الرئيسي لفترة غير مقبولة من الوقت (مثال: انقطاع التيار الكهربائي لفترة قصيرة أو ممتدة، عدم توافر الشبكة لفترة طويلة، تضرر أو دمار التجهيزات أو الوحدات).

فصل الواجبات Duties Separation

تقسيم الأدوار والمسؤوليات بحيث لا يتحكم فرد وحيد بعملية هامة بكاملها.

التشفير Cryptography

تحويل البيانات (يدعى "نص عادي") إلى شيفرات (يدعى "نص مشفر") بشكل يحافظ على المعنى الأصلي للبيانات لمنع التعرف عليها أو استخدامها.

حماية البيئة Environment Protection

تطبيق إجراءات الرقابة والشروط والأغراض بوصفها تدابير وقائية تؤثر على تطوير وعمل وصيانة النظام. وتتضمن هذه الإجراءات الوقائية، على سبيل المثال لا الحصر، الحماية من الحرائق وبرامج الخدمات الداعمة.

التهديد البيئي

أي حادث غير مقصود طبيعي أو عرضي أو قصور في الأداء يمكن أن يسبب ضرراً في موارد المعلوماتية والمعلومات والموظفين (أي: قصور بنيوي، تقلبات الطاقة، تقلبات الحرارة والرطوبة، وفشل أنظمة التدفئة والتبريد).

الحَدَث Event

أية مشاهدة (واقعة) تحدث في الشبكة أو النظام.

الموقع البديل كامل التجهيز Hot Site

وحدة معالجة بيانات مستقلة عن موقع العمل الأساسي وتكون جاهزة للعمل تماماً، وهي مزودة بالمكونات الصلبة وبرمجيات النظام ليتم استخدامها في حال وقوع كارثة.

التهديد البشري Human Threat

أي شخص، أو مؤسسة، يمتلك القدرة، ولديها النية، للتسبب بأضرار في مهمة الوزارة.

مرحلة التنفيذ Implementation Phase

فترة في دورة حياة تطوير النظام يتم خلالها تركيب النظام وتشغيله وتسليمه إلى المستخدم (من أجل البدء بمرحلة التشغيل والصيانة).

الحادث العرضي Incident

الاختراق أو التهديد الوشيك بحدوث اختراق، لسياسة الحماية الصريحة أو الضمنية، أو سياسات الاستخدام المقبولة، أو الممارسات النموذجية للحماية في نظام أو شبكة معلوماتية أو اتصالات. ولا تعتبر الأحداث السلبية (مثال: الفيضانات، الحرائق، انقطاع التيار الكهربائي، الحرارة الزائدة) على أنها حوادث تتعلق بالحماية الكمبيوترية.

معالجة الحوادث Incident Treatment

خطة عمل لمعالجة الاختراقات، والسرقة المعلوماتية، رفض الخدمة، والحرائق، والفيضانات والأحداث الأخرى المتعلقة بالحماية. وتتألف من عملية من ستة مراحل: الإعداد، والتعريف، والاحتواء، والإلغاء والاستعادة والدروس المستقاة.

خطة مواجهة الحوادث Incident Treatment Plan

وهي الوثائق والتوجيهات والإجراءات المحددة مسبقاً من أجل اكتشاف أي عمل عدائي معلوماتي يهدف إلى إلحاق أضرار بأنظمة المعلوماتية الخاصة بالمؤسسة ومواجهته والحد من نتائجه.

ضمان المعلومات Information Assurance

التدابير التي تحمي وتصون المعلومات وأنظمة المعلومات من خلال ضمان توافرها وسلامتها وسريتها وعدم رفضها. وتتضمن هذه التدابير دعم تجديد أنظمة المعلومات من خلال دمج قدرات الحماية والكشف والاستجابة.

موارد المعلومات Information resources

تتضمن معلومات الحكومة والمعلوماتية والموارد ذات الصلة مثل الموظفين والتجهيزات والأموال.

تقانة المعلومات (المعلوماتية) Information Technology (IT)

أية تجهيزات أو نظام أو نظام فرعي مترابط من التجهيزات المستخدمة في اكتساب، وتخزين، واحتكار، وإدارة، وتحريك، ومراقبة، وعرض، وتبديل، وتبادل، وإرسال أو استقبال البيانات أو المعلومات آلياً.

تتضمن المعلوماتية الحواسب، والتجهيزات الملحقة، والبرمجيات، والبرمجيات الثابتة والإجراءات المشابهة، والخدمات (متضمنةً خدمات الدعم) والموارد ذات الصلة.

أمن المعلومات Information Security

مجموعة من الأدوات مهمتها حماية البيانات و منع القرصنة الالكترونية.

السلامة Integrity

الدرجة التي يمنع النظام (أو جزء من النظام) عندها النفاذ أو التعديل غير المصرح به لبرامج أو بيانات الكمبيوتر.

الحماية من التعديل الخاطئ للمعلومات أو التدمير. ويتضمن ضمان أصالة المعلومات وعدم رفضها.

خطة الحالات الطارئة للمعلوماتية

سياسة الإدارة والإجراءات المصممة للحفاظ على عمليات المشروع واستعادتها بما فيها عمليات الكمبيوتر، في موقعٍ بديل، أثناء الحالات الطارئة وفشل النظام والكوارث.

الشبكة المحلية LAN

مجموعة من الكمبيوترات والأجهزة المتعلقة بها التي تتشارك خط اتصالات واحد أو وصلة لاسلكية، وتتشارك عادة بموارد معالج أو مخدم وحيد ضمن بقعة جغرافية صغيرة (على سبيل المثال: داخل المبنى).

التطوير المشترك للتطبيقات Joint Application Development

وهي تقنية تقضي بمشاركة كل من المحلل والزبون في التطوير البرمجي.

الشيفرة المؤذية Malicious Code

برنامج (مثال: حصان طروادة) تبدو كأنه يؤدي وظيفةً مفيدةً أو مرغوبة ولكنه في الواقع يحصل على دخول غير مصرحٍ به إلى موارد النظام أو يخدع المستخدم لتنفيذ عملية مؤذية.

ضوابط إدارية Management Controls

التقنيات والأمور، التي تعالجها إدارة المؤسسة عادةً، وتركز على إدارة مخاطر نظام المعلوماتية وحمايته. وبوضوحٍ أكبر، الأفعال المتخذة لإدارة تطوير وصيانة واستخدام النظام، بما فيها السياسات المحددة للنظام، والإجراءات، وقواعد التعامل، والأدوار والمسؤوليات الفردية، والمحاسبة الفردية وقرارات الحماية الخاصة بالموظفين.

التهديد الطبيعي Natural Threat

التهديد الذي تمثله الحرائق أو الكوارث الطبيعية مثل الأعاصير والزلازل والفيضانات.

عدم الرفض Non-repudiation

ضمان إرسال تقرير التسليم إلى المرسل، وبأن المستقبل يمتلك إثباتاً لهوية المرسل وبهذا لا يستطيع أي منهما إنكار أنه قد قام بمعالجة المعلومات.

أمن الشبكات Network Security

الإجراءات و الأدوات المستخدمة لحماية البيانات خلال نقلها عبر الشبكات. و تتضمن الحيلولة دون (deter) و منع (prevent) و كشف (detect) و تصحيح (correct) أي انتهاك لأمن المعلومات (security violation) سواءً المنقولة أو المخزنة.

الضوابط التشغيلية Operational Controls

الإجراءات والطرق التشغيلية التي تركز على التقنيات التي ينفذها الأشخاص (على خلاف الأنظمة). وغالباً ما تتطلب خبرات فنية أو تخصصية كما تعتمد في أغلب الأوقات على نشاطات الإدارة بالإضافة إلى الضوابط الفنية.

التشغيل والصيانة Operation and Maintenance

فترة من دورة حياة تطوير الأنظمة يتم خلالها استخدام منتج البرمجيات في بيئته التشغيلية، ومراقبته لتحقيق الأداء المرضي، وتعديله بالشكل الضروري لتصحيح الأخطاء أو من أجل الاستجابة للمتطلبات المتغيرة.

كلمة السر Password

سلسلة من الرموز (أحرف، أرقام ورموز أخرى) تستخدم للتأكد من هويةٍ ما أو التحقق من تصريح الدخول.

الحماية المادية الفيزيائية Physical Security

استخدام الحواجز المادية وإجراءات المراقبة كتدابير أو إجراءات وقائية ضد التهديدات التي تواجه الموارد والمعلومات الحساسة.

السياسة Policy

القواعد والأنظمة التي تضعها المؤسسة. وتحدد السياسة نوع موارد المعلومات الداخلية والخارجية التي يستطيع الموظفون النفاذ إليها ونوع البرامج التي يمكنهم تنصيبها على كمبيوتراتهم بالإضافة إلى صلاحياتهم من أجل الحفاظ على موارد الشبكة. تتصل السياسة أيضاً بجودة خدمة الشبكة لأنها تستطيع أن تحدد أولويات المستخدم أو مجموعة العمل أو التطبيق فيما يتعلق بالحفاظ على عرض حزمة الشبكة.

الخصوصية Privacy

تقييد النفاذ إلى معلومات المستخدم بالانسجام مع القانون وسياسة الوزارة.

مفتاح خاص Private Key

مفتاح مشفر يستخدم مع خوارزمية التشفير بالمفاتيح العمومية ويرتبط بالجهة وحدها ولا يعمم.

مفتاح عمومي Public Key

جزء من زوج من المفاتيح متاح للعموم. ويستخدم الجزء المكشوف من زوج مفاتيح التشفير في التشفير غير المتماثل.

التشفير بمفاتيح عمومية Public Key Infrastructure

المرادف الشائع "للتشفير غير المتماثل". و الذي يستخدم المفتاح العام و الخاص.

المخاطر Risks

الأثر الصافي للمهمة مع اعتبار:

احتمال أن يستخدم مصدر تهديد محدد (يحدث بشكلٍ عرضي أو يتم استغلاله بشكل مقصود) نقطة ضعف محددة في نظام المعلومات.

تقييم المخاطر Risk Assessment

عملية تحديد المخاطر على النظام وتحديد إمكانية حدوثها، والأثر الناتج عنها والإجراءات الوقائية الإضافية التي من شأنها أن تقلل من هذا الأثر.

جزء من إدارة المخاطر مترادف مع تحليل المخاطر.

إدارة المخاطر Risk Management

العملية الكلية لتحديد ومراقبة المخاطر ذات الصلة بأنظمة المعلومات والحد من آثارها. وتتضمن تقييم المخاطر، ومقارنة المزايا والسيئات، وانتقاء وتنفيذ واختبار الإجراءات الوقائية وتقييم الحماية. تأخذ هذه المراجعة الشاملة لحماية النظام الفعالية والكفاءة بعين الاعتبار، متضمنةً الأثر على المهمة والقيود التي تفرضها السياسة والقوانين والأنظمة.

تقييم الحماية Security Assessment

معاينة وتحليل إجراءات الحماية لنظام ما بعد تطبيقها في بيئة تشغيلية لتحديد حالة الحماية الموجودة في النظام.

المجال Security Domain

و هو عنوان يتضمن مجموعة الأدوات ذات الطابع المتشابه و التي تحقق غاية محددة ضمن المجال المشترك.

المتحكمات Security Controls

و تكون تحت عنوان –مجال– واحد و تتضمن أدوات للتغلب على المخاطر. مثل السياسات و الإجراءات و التعليمات و غيرها.

الهندسة الاجتماعية Social Engineering

تُعَّرف الهندسة الاجتماعية بالطريقة التي تُستخدم للحصول على المعلومات من الأشخاص بطريقة الإقناع و الخداع لإقناعهم بأن المعتدي هو شخص آخر يحق له الحصول على المعلومات و ذلك دون استخدام أية تقنية من خلال التجهيزات الأمنية.

النظام System

مجموعة من الأجزاء المنظمة (أجهزة، برمجيات، واجهات) لتحقيق وظيفة محددة أو مجموعة من الوظائف؛ تعتبر عادةً عنصراً يحقق الاكتفاء الذاتي في استخدامه التشغيلي المخطط له.
مجموعة مترابطة من موارد المعلومات تتشارك الوظيفة نفسها تحت الرقابة الإدارية المباشرة نفسها. وهي نظام يتضمن عادةً مكونات صلبة وبرمجيات ومعلومات وبيانات وتطبيقات واتصالات وأشخاص.

مدير النظام System Administrator

الشخص المسؤول عن التخطيط لتنصيب البرنامج واستخدامه من قبل مستخدمين آخرين.

تحليل النظم Systems Analysis

هو عملية إجرائية تفحصيه لحالة عمل مهني، أو مجموعة أعمال متسلسلة، أو مجموعة عناصر مترابطة بهدف تطوير نظام(قد يكون حاسوبياً) لحل مشكلة ما،أو ابتكار وسيلة لتحسين طريقة العمل، أو مساعدة متخذي القرار لتحديد تسلسل أعمال أفضل من الموجود حالياً.

دورة حياة تطوير النظام System Development Life Cycle

نموذج رسمي لمشروع مكونات الصلبة أو برمجيات يحدد إطار النشاطات والمنتجات والمراجعات والموافقات والموارد والعلاقة بينها. وكذلك الفترة التي تبدأ عند تحديد حاجةٍ ما (التخطيط) وتنتهي عندما يصبح النظام غير صالحٍ للعمل (التخلص من النظام).

خطة حماية النظام System Security Plan SSP

وثيقة تقدم توصيفاً لحماية النظام وتحدد الضوابط الفنية والتشغيلية والإدارية للنظام. وتبين خطط الحماية كيفية تنفيذ النظام لسياسات الحماية، وتحدد مسؤوليات كافة مستخدمي النظام وتقدم وصفاً لقواعد التعامل.

الدعم Support

تقنيات ومنتجات الحماية الفنية التي تتصف بفعالية تكلفتها.

الضوابط الفنية Technical Controls

آليات الحماية الآلية والتكنولوجية التي تنفذها أنظمة المعلوماتية. ويمكن للضوابط أن تؤمن حماية آلية من النفاذ غير المصرح به أو الاستخدام الخاطئ للمعلومات كما تسهل تتبع الاختراقات الأمنية.

التهديد Threat

أي ظرف أو حدث أو فعل يمكن أن يسبب ضرراً على المديرية من خلال تدمير أو كشف أو تعديل أو رفض خدمة الموارد المعلومات المؤتمتة.

الرمز الخاص Token

شيء يمتلكه المستخدم ويتحكم به (عادةً مفتاح أو كلمة سر) يستخدم للتأكد من هوية المستخدم.

حصان طروادة Trojan Horse

برنامج يظهر على أنه يؤدي وظيفةً مفيدة لكنه يحتوي على وظيفة مخبأة ومن المحتمل أن تكون مؤذية تتفادى آليات الحماية، أحياناً من خلال استغلال تصريحات قانونية لجهة من جهات النظام التي تستخدم البرنامج.

المستخدم User

شخص أو عملية تستخدم نظام معلومات مؤتمتة إما عبر وصلات مباشرة (باستخدام الحواسب الطرفية) أو الوصلات غير المباشرة (إعداد بيانات الإدخال أو استقبال النتيجة التي لم تتم مراجعتها محتواها أو تصنيفها من قبل الفرد المسؤول).

الصلاحية Validation

عملية تحديد صحة المنتج النهائي أو النظام أو جزء من النظام فيما يتعلق بمتطلبات المستخدم.

الإجابة على السؤال التالي، "هل أقوم بتصنيع المنتج الصحيح؟"

التحقق Verification

عملية تحديد إذا ما كانت منتجات فترة دورة الحياة تحقق المتطلبات التي جرى تأسيسها خلال المرحلة السابقة.

الإجابة على السؤال التالي، "هل أقوم بتصنيع المنتج بالطريقة الصحيحة؟"

نقاط/مواطن الضعف Vulnerability

خلل أو ضعف يمكن أن تتعرض لها إجراءات أو تصميم أو تنفيذ أو الضوابط الداخلية لحماية النظام (من الممكن أن تحدث بشكلٍ عرضي أو أن يتم استغلالها بشكل مقصود) وينتج عنها خرق أمني أو انتهاك لسياسة حماية النظام.

Bibliography

المراجع

Andersson, R. (2003). Evaluation of the Security of Components in Distributed Information Systems . *LiTH-ISY-3430-2003* . Sweden: Dept. of Electrical Engineering, Linköping Institute of Technology .

Bishop, M. c. (2005). *Introduction to Computer Security.* Boston: Addison-Wesley.

Bishop, M. (2003). *Computer Security: Art and Science.* Boston: Addison-Wesley.

Board, C. C. (1999). *Common criteria for Information Technology Evaluation.* USA: NIST.

Bond, A. (2004). *A quantitative evaluation framework for component security in distributed information systems.* Sweeden: Linkoping University: Institute of Technology.

Burn, R. (1977). *A Pathway to Number Theory.* Cambridge, England.

CERT. (2006). insider_threat. Retrieved from www.cert.org.

Christopher, H. (2011). Social Engineering: The Art of Human Hacking. Indiana, USA: Wiley Publication.

Cormen, T., Leiserson, C., Rivest, R., & Stein, C. (1999). *Introduction to Algorithms.* Cambridge, MA: MIT Press.

Daemen, J. a. (2001). Rijndael: The Advanced Encryption Standard. *Dr.Dobb's Journal* .

EC-Council. (2006). *Ethical Hacking and Countermeasures.* NY, USA: EC-Council.

Fallouh, D. G., Basha, D. N., & Ahmad, E. W. (2011). A Novel Approach to Design Quantitative Method for ICT Security Assessment. *Damascus University's Journal of Engineering Science* , 35.

Feistel, H. (1973). *Cryptography and Computer Privacy.* Scientific American.

ISACA and ITGI. (2007). *COBIT 4.1, Control Objectives for Information and related Technology.* ISACA and the IT Governance Institute (ITGI).

ISO/IEC 13335-1. (2004). *ISO/IEC TR 13335-1, Information technology – Security techniques – Management of information and communications technology security – Part 1: Concepts and models for information and communications technology security management.* ISO.

ISO/IEC 13335-3. (2005). *ISO/IEC TR 13335-3, (Guidelines for the Management of IT Security: Techniques for the Management of IT Security).* ISO.

ISO/IEC 15408. (1999). *ISO/IEC 15408-1, Information technology – Security techniques – Evaluation Criteria for IT security – Part 1: Introduction and general model.* ISO.

ISO/IEC 27001. (2005). *ISO/IEC 27001, Information technology-Security techniques-Information Security Management Systems (ISMS)-Requirements.* ISO.

ISO/IEC 27002. (2005). *ISO/IEC 27002 or BS 17799, Information technology-Security techniques-Code of practice for information security management.* ISO.

Jones, C. (2004). *Social Engineering: Understanding and Auditing.* SANS Institute.

Kenneth E. Kendall, J. E. (2007). *Systems Analysis and Design 7th edition.* Pearson Education.

Kumanduri, R. (1998). *Number Theory with Computer Applications.* Upper Saddle River, NJ: Prentice Hall.

Lively, C. (2003). *Psychological Based Social Engineering.* SANS Institute.

Murdoch, J. (2005). *Security Measurement.* York, United Kingdom.

NIST 800-53. (2010). *NIST SP 800-53 rev1, "Recommended Security Controls for Federal Information Systems".* USA: NIST.

NIST 800-55. (2005). *NIST SP 800-55, "Performance Measurement Guide for Information Security"*. USA: NIST.
Pfleeger, C. (2002). *Security in Computing.* Upper Saddle River, NJ: Prentice Hall.
Pieprzyk, J., Hardjono, T., & and Seberry, J. (2003). *Fundamentals of Computer Security.* New York: Springer-Verlag.
R, S. A. (2004). Measuring the Information Security Level – A Survey of Practice in Finland. *the 5th Annual International Systems Security Engineering Association (ISSEA)* (p. 10). Arlington, Virginia: ISSEA Conference.
Russia Today. (2011). *في خدمة من؟ :الفيس بوك والسكايب.* Retrieved 2011, from http://arabic.rt.com/prg/telecast/656470/
Scarfone, K. (2008, September). Technical guide to information security testing and assessment. Gaithersburg, United States of America.
Schneier, B. S. (2000). *Digital Security in a Networked World.* New York: Wiley.
Shamir, A. a. (2003). On the Cost of Factoring RSA-1024. *CryptoBytes* .
Simon, K. D. (2003). *The Art of Deception: Controlling the Human Element of Security.* NY, USA: John Wiley & Sons, Inc.
Simovits, M. (1996). *The DES: An Extensive Documentation and Evaluation.* Laguna Hills, CA: Aegean Park Press.
Stallings, W. A. (2002). *The Advanced Encryption Standard.* Cryptologia.
Stallings, W. B. (2008). *Business Data Communications, 6th edition.* Prentice Hall.
Stallings, W. C. (2004). *Computer Networking with Internet Protocols and Technology.* Upper Saddle River, NJ: Prentice Hall.
Stallings, W. C. (2005). *Cryptography and Network Security (4th Edition).* Prentice Hall.
Stinson, D. C. (2002). *Theory and Practice.* Boca Raton, FL: CRC Press.
Thornburgh, T. (2004). Social Engineering: The "Dark Art". In InfoSecCD '04:Proceedings of the 1st annual conference on Information security curriculum development, New York, NY, USA, 2004. ACM. *the 1st annual conference on Information security curriculum developmen* (pp. 133–135). NY, USA: ACM.
Tuchman, W. (1979). *Hellman Presents No Shortcut Solutions to DES.* IEEE Spectrum.
المدوّن وعضو اتحاد الصحفيين العرب في أمريكا رفيق لطف. (27 نيسان, 2011). غرف البالتوك لفبركة الأكاذيب و التحريض على سورية. (التلفزيون العربي السوري، المحاور)
غسان فلوح، نوربك باشا، و وسيم أحمد. (2011). تحليل الهوة القائمة بين الواقع و المعايير العالمية لأمن المعلومات في المؤسسات المالية في سورية. *مجلة جامعة تشرين للدراسات و الأبحاث العلمية* ، 22.
مجلس النقد و التسليف قرار 106. (2008). *التعليمات الخاصة بالمخاطر التشغيلية" قرار106-م ن-*. دمشق: مصرف سورية المركزي.
مجلس النقد و التسليف قرار 391. (2008). *المبادئ الأساسية لاستمرارية الأعمال، قرار391م ن- ب4*. دمشق: مصرف سورية المركزي.
محمد مراياتي، يحيى مير علم، محمد حسان طيان. (1987). *"علم التعمية و استخراج المعمى عند العرب"، الجزء الأول*. دمشق: مطبوعات مجمع اللغة العربية بدمشق .

أوراق البحث المنشورة

1. " **تحليل الهوة القائمة بين الواقع و المعايير العالمية لأمن المعلومات في المؤسسات المالية في سورية** ". وتم قبولها للنشر في مجلة جامعة تشرين للأبحاث و الدراسات العلمية بالكتاب رقم 320 تاريخ 2011/2/20.
2. **" A Novel Approach to Design Quantitative Method for ICT Security Assessment"** و التي تم تقديمها لمجلة جامعة دمشق للعلوم الهندسية و تم قبولها للنشر بالكتاب رقم 20146/ص تاريخ 2011/7/6.

تحليل الهوة القائمة بين الواقع والمعايير العالمية لأمن المعلومات في المؤسسات المالية في سورية

الدكتور غسان فلوح*
الدكتور نور بك باشا**
المهندس وسيم أحمد***
wassimah@scs-net.org

الملخّص

نظراً للحاجة الكبيرة لوجود نظام قياس كمي لمستوى السرية وأمن المعلومات في المؤسسات المالية والمصرفية بما يسهل تحليل الثغرات والتعرف على مستوى تطبيق المعايير الدولية في مجال أمن المعلومات بغية الوصول للتوافق التام مع المعايير الدولية بما يحقق استمرارية الأعمال على أفضل المستويات، تم الشروع بدراسة تفصيلية عن واقع أمن المعلومات في هذه المؤسسات في الجمهورية العربية السورية كجزء رئيسي من بحث أوسع يتم العمل عليه يهدف إلى الوصول لتقديم دراسة كمية لقياس مستوى أمن المعلومات في هذه المؤسسات مما يشكل ركيزة أساسية في تعريف متطلبات هذه المؤسسات والخطوات الواجب اتباعها في كل من مجالات العمل بما يخص أمن المعلومات، حيث توضح هذه الورقة العلمية نتائج الدراسة الإحصائية على أربع عينات[1] من مؤسسات مالية ومصرفية في سوريا لمعرفة توافق هذه العينة مع معايير أمن وسرية المعلومات وإيجاد ترتيب لأولوية هذه المعايير ومدى تأثيرها في استمرارية الأعمال بشكل مستقر وآمن.

الكلمات المفتاحية: السياسة الأمنية, نظام ادارة أمن المعلومات, الأصول, ادارة الكوارث, خطط استمرارية العمل, الرقابة, أمن النواحي الفيزيائية, الاتصالات.

---

* أستاذ –قسم هندسة الحواسيب و الأتمتة- كلية الهندسة الكهربائية و الميكانيكية –جامعة دمشق -سوريا.

** أستاذ –مدير مركز أبحاث هندسة البرمجيات المتقدمة- جامعة كولالمبور-ماليزيا.

*** طالب دراسات عليا(دكتوراه) - قسم هندسة الحواسيب و الأتمتة- كلية الهندسة الكهربائية و الميكانيكية –جامعة دمشق.

[1] في كل مؤسسة تم اجراء استطلاع لكل من الادارة العامة و فرع على حدة , و بالتالي فالدراسة بُنيت على ثمانية استطلاعات.

Gape analysis between the existing situation of information security in financial institutions in Syria and international standards

Dr. Ghassan Fallouh[*]

Dr. Norbik Basha[**]

Eng. Wassim Ahmad[***]

ABSTRACT

With the need to find a quantitative measurement of the level of security that financial institutions in Syria already have, which facilitate the gap analysis between them and the international standards, especially ISO27K in the field of information security, in order to improve the level of security for those institutions, comply with international requirements in this filed, and provide secure environment and services for both employees and customers; we wrote this research paper, which includes: statistical studies, in-site meetings, analyses of the existing situations of information security, and comparisons with ISO27K for 4 main financial institutions[2] in Syria, and define priorities for those standards and their effects on business continuity in a way that provide security and stable.

Keywords: security policy, ISMS (Information Security Management System), Assessment, Assets Management, physical security, telecommunications.

مقدمة

[*] Prof - Department of Computer Engineering and Automation- Faculty of Mechanical and Electrical Engineering- Damascus University -Syria.

[**] Prof -Centre for Advanced Software Engineering, University Technology Malaysia, Kuala-Lampur, Malaysia.

[***] PhD Student- Department of Computer Engineering and Automation- Faculty of Mechanical and Electrical Engineering- Damascus University -Syria.

[2] For each sample we have done 2 surveys, for the Headquarter, and branch.

يعتبر أمن المعلومات من أهم المواضيع التي تولي لها جميع المؤسسات و الهيئات العلمية في جميع أنحاء العالم اهتماماً خاصاً و موارد مالية كبيرة و ذلك للحفاظ على سوية عالية من السرية و الحماية للمعلومات و التي تعتبر لدى بعض المؤسسات – و خاصة المصارف و المؤسسات المالية – الأصول الأغلى Assets و الأكثر خطورة, و التي يسعى الجميع للحفاظ عليها من التسرب أو الضياع أو التغيير.

و مع تعاظم دور الانترنت و الخدمات الالكترونية, و خاصة المالية منها. و التزايد المخيف للبرامج الضارة و الاختراقات للمواقع و الحسابات المصرفية. ازدادت الحاجة لأبحاث و دراسات في مجال أمن الشبكات و المعلومات.

وعليه فقد دأبت الجهات العلمية المختصة بوضع معايير دولية لأمن المعلومات بحيث تسهل على المعنيين بالموضوع في كافة المؤسسات على اختلافها تطبيق سياسات أمنية محكمة و مراجعتها للوصول لحالة أمنية مستقرة و في مستوى مقبول لتقديم الخدمات و التسهيلات للزبائن أو للحفاظ على سرية المعلومات و التحكم بالوصول اليها, نذكر منها: ISO 27K,COBIT,BASEL2 و غيرها.

أهمية البحث و أهدافه:

تهدف هذا الورقة إلى إعطاء رؤية موسعة للحالة الراهنة للمؤسسات المالية في سورية وتحليل الهوة الموجودة بين الواقع الراهن و المعايير العالمية وخاصة ISO27K وشرح الخطوات التطبيقية الهامة المطلوب القيام بها بصورة منهجية للوصول الى حالة أمنية عالية، وذلك على كامل الفقرات اللاحقة.

تقوم هذا الدراسة بتعريف الهوة الموجودة بين الوضع الراهن لأمن المعلومات و المعايير العالمية, وتوضيح أولوية وأهمية كل من هذه المعايير تبعاً لنتائج الاستطلاع الذي تم القيام به، والانتقال إلى الخطوات التطبيقية الهامة للوصول إلى الحالة المطلوبة اعتماداً على المفاصل الأساسية في المعيار ISO27K وعلى الاستطلاعات بما يتوافق مع واقع ومتطلبات أمن المعلومات في المؤسسات المالية والمصرفية في الجمهورية العربية السورية.

طرائق البحث و مواده:

انطلاقاً من حصيلة الاستطلاع والاجتماعات والوثائق والجولات الميدانية التي تمت خلال السنوات الأربعة الماضية على أربعة مؤسسات مالية كبرى في سورية (تم اجراء استطلاعين في كل مؤسسة واحد للادارة العامة وآخر لأحد الفروع و ذلك على اعتبار أن عمل ومتطلبات أمن المعلومات للفروع مختلف عن الادرات) وشملت مصرفّين هامين و مؤسستين ماليتين (وكل منها يتكون من ادارة عامة و أكثر من 30 فرعاً) دون ذكر الأسماء حفاظاً على الخصوصية وسرية العمل حسب طلب هذه الجهات.

اتخذت الدراسة المنهج التالي:

1) اعتماد المعيار ISO27K كمعيار رئيسي لتقييم وضع أمن المعلومات في المؤسسات المالية في سوريا.
2) تحديد نقاط التقييم والاستطلاع انطلاقاً من المعايير ISO27K.

3) بالاضافة الى ISO27K تم اعتماد اطار العملNIST SP 800-53 rev1:2010 كخطوات عملية للوصول الى المعايير المطلوبة و تقييمها(Assessment).
4) اعتماد أجوبة الاستطلاع المتعلقة بالنقطة المدروسة, مع ملاحظة اختلاف بعض الاجوبة في المؤسسات الأربعة المدروسة حيث تم اختيار الجواب الأكثر بعداً عن المعيار المقابل و وضع النسبة من الاستطلاع الموافقة لذلك.
5) تحليل الفجوة الذي يعكس موجز عن حصيلة الإجابات.
6) مفاتيح الممارسات العملية، التي صممت على الشكل التالي:
   a) تعريف الإشكالات العامة.
   b) توضيح الخطوات التطبيقية الواجب اتباعها لتجاوز تلك الإشكالات.

يبقى التذكير بأنه تم تضمين النقاط والإشكاليات التي حصلت على تصويت جهة واحدة على الأقل من العينات التي تم تطبيق الاستطلاع عليها مع ذكر نسبة الجهات التي قامت بتأكيد الإشكاليات وضرورة معالجتها من عدد العينات الكلية.

النتائج و المناقشة:

سنقوم بعرض النتائج و المناقشة لكل مجال مدروس كما يلي:

الإشكاليات: و تعني الفقرات من المعايير ISO 27001,27002 التي وجدنا فيها إشكالات (غير مطبقة أو ناقصة أو خاطئة...)	**نسبة العينات:** و تعني النسبة من الاستطلاعات التي وجدت فيها الإشكالية	**ملاحظات عامة:** توضيحات
<u>الخطوات التطبيقية الهامة:</u>[3] وهي الخطوات الواجب اتخاذها من قبل المؤسسة المدروسة لتصحيح الإشكاليات الواردة في فقرة المعيار المناقش		

1. نظام إدارة أمن المعلومات (ISMS)

الإشكاليات	نسبة العينات	ملاحظات عامة
العلاقة بين استراتيجية المؤسسة ومحددات تقييم المخاطر وسلوك الإدارة	%75	
وضوح وجلاء الأدوار والمسؤوليات	%100	تم الإجماع على ضرورة وجود إدارة عامة مدركة لأهمية أمن المعلومات وإدارة تقنية قادرة على تنفيذ

[3] تم اعتماد عدة مراجع لتوضيح الخطوات التطبيقية وخاصة NIST SP 800-53 rev1, المراجع

		كافة الخطط والاستراتيجيات المتعلقة بأمن المعلومات
عملية المراجعة والتغذية الراجعة	%50	
<u>الخطوات التطبيقية الهامة:</u> على الإدارة بكافة مستوياتها دعم نظام أمن المعلومات بتوجيه واضح والتزام كامل ومعرفة جلية بالمسؤوليات المترتبة عند تطبيق أمن المعلومات. تتجلى الخطوة الأولى في تغيير النظرة التقليدية في التعامل مع تكنولوجيا المعلومات على أنها أداة مساعدة في العمل لا علاقة لها بأهداف وغايات العمل. لقد أصبحت المعلومات من أهم العوامل التنافسية وجزءاً ثميناً من أصول المؤسسة ويجب حمايتها والحفاظ على أمنها		

2. تقييم ومعالجة المخاطر

الإشكاليات	نسبة العينات	ملاحظات عامة
الحاجة إلى ترتيب المخاطر على ضوء أهداف ومحددات المخاطر	%50	
عكس تقييم المخاطر على الاستراتيجيات والخطط المتعلقة بأمن المعلومات بما يشمل الميزانية المخصصة	%100	بين الاستطلاع وجود فجوة كبيرة بين قوائم تقييم المخاطر في العينات المدروسة وبين الخطط والموازنة المحجوزة لإدارة ومعالجة هذه المخاطر
<u>الخطوات التطبيقية الهامة:</u>[4] **تقييم المخاطر** يجب القيام بتقييم المخاطر وتحديثه خلال فواصل مناسبة لكافة المتعلقات المعلوماتية. **معالجة المخاطر** يجب أن تتضافر جهود معالجة المخاطر لصد المخاطر المعرفة عبر استخدام وسائل التحكم الأمنية الإدارية والفنية والفيزيائية المناسبة وعبر تخصيص موازنة خاصة لمعالجة هذه المخاطر.		

[4] ISO/IEC TR 13335-3 , المراجع

3. االسياسة الأمنية

الإشكاليات	نسبة العينات	ملاحظات عامة
عملية التخطيط وتحليل الهوة بين الواقع والمتطلبات الأمنية	%50	
تضييق الفجوة بين الواقع والمتطلبات الأمنية عبر الخطوات التنفيذية	%100	
عملية المتابعة والتقييم المستمر	%50	تم ذكر إشكالية تأثير تغيير الإدارات على عمليات المتابعة والتقييم المستمر بما ينعكس سلباً على وجود استمرارية في عمليات تضييق الهوة الأمنية
القيام بخطوات وتعديلات تبعاً لعمليات التقييم المستمر	%50	

الخطوات التطبيقية الهامة:[5]

المجال

على هذه السياسات أن تؤمن في مجملها تحكم جلي بكافة البيانات المحصلة المتداولة أو المخزنة في وسائط معالجة البيانات والاتصالات أو أنظمة التخزين، وكذلك الأمر بالنسبة للبيانات المحصلة والمتداولة مع الأطراف الخارجية المتعاقدة مع المؤسسة المالية.

التصديق

على هذه السياسات أن تصدق رسمياً من قبل السلطات المخولة حسب الأصول.

التوثيق

يجب أن توثق السياسات الأمنية بطريقة مناسبة للمؤسسة.

التواصل والتدريب والتوعية

يجب تبادل سياسات أمن المعلومات ضمن المؤسسة المالية، ومع الأطراف الخارجية المتعلقة أيضاً، من خلال برنامج تدريب وتوعية مناسب.

المراجعة الدورية

يجب مراجعة هذه السياسات على فترات محددة وحين حدوث تغييرات مؤثرة في البيئة الخارجية لضمان استمرارية فعاليتها وملاءمتها ومناسبتها.

[5] .ISO/IEC 13335-1:2004 , المراجع.

4. تنظيم أمن المعلومات

الإشكاليات

يعكس هذا القسم نفس المشاكل التي تم طرحها في القسم السابق.

الخطوات التطبيقية الهامة:[6]

التزام الإدارة

اهتمام واضح ودعم عملي لمبادرات أمن المعلومات متضمناً تخصيص الموارد المناسبة لوسائل التحكم الخاصة بأمن المعلومات.

تنسيق الجهود

يجب تنسيق الأنشطة المتعلقة بأمن المعلومات عن طريق تمثيل الجهات المختلفة في المؤسسات المالية بالأدوار الأمنية والوظائفية المتعلقة.

توزيع المسؤوليات

يجب تعريف كافة المسؤوليات المتعلقة بأمن المعلومات بشكل واضح.

عمليات التفويض

على عملية التفويض المتعلقة بوسائل وقابليات معالجة المعلومات الجديدة أو المتعلقة بالتغيرات المؤثرة على الوسائل والقابليات الموجودة أن تكون معرفة ومنفذة.

اتفاقات السرية وعدم الافصاح

على اتفاقات السرية وعدم الافصاح أن تعكس حاجات المؤسسات المالية لحماية معلوماتها, و يجب مراجعة هذه الاتفاقات دورياً.

الاتصال مع السلطات الخارجية

يجب الحفاظ على آليات الاتصال مع السلطات الخارجية.

الاتصال مع المجموعات ذات الاهتمام الخاص

يجب الحفاظ على اتصال مناسب مع المجموعات ذات الاهتمام الخاص أو المنتديات الأخرى المهتمة بأمن المعلومات والجمعيات المختصة.

الاتصال والعقود مع الطرف العقدي الثالث (غير المباشر)

على الاتفاقات مع الطرف الثالث المنخرط في الدخول إلى معلومات المؤسسة أومعالجتها أو إدارتها أو وسائل معالجتها أن تغطي كافة المتطلبات الأمنية المطلوبة.

[6] .ISO/IEC 13335-1:2004 , المراجع.

الاتصال والعقود مع المستخدمين

يجب مواجهة كل المتطلبات الأمنية المعرفة قبل إعطاء المستخدم حق الدخول إلى معلومات أو أصول المؤسسة المالية. تتشابه الخطوات المتبعة هنا مع تلك المذكورة سابقاً والمتعلقة بالأطراف الخارجية.

المراجعة المستقلة لأمن المعلومات

على المؤسسات المالية خلال عمليات إدارة وتنفيذ أمن المعلومات أن تتبع أسلوب المراجعة المستقلة والمجدولة سلفاً أو الطارئة حين حدوث متغيرات مؤثرة في البنية الداخلية أو البيئة الخارجية.

5. إدارة الأصول المعلوماتية

الإشكاليات	نسبة العينات	ملاحظات عامة
إعادة تعريف الأصول المعلوماتية	%50	
تسجيل الأصول المعلوماتية	%25	
التوثيق ووضع اللصاقات المناسبة	%75	إن توثيق وأرشفة كافة المعلومات والتجهيزات والإجرائيات حسب المعايير يعتبر الركيزة التي تعتمد عليها كافة المؤسسات لمتابعة تطبيق المعايير المتعلقة بأمن المعلومات

<u>الخطوات التطبيقية الهامة:</u>[7]

مخزون الأصول

يجب حصر كافة الأصول المعلوماتية بدقة على شكل قوائم، بحيث تحتوي هذه القوائم على أسماء مالكي الأصول و المتحكمين بها و المسؤولين عن حمايتها.

ملكية الأصول (التحكم بها)

يجب أن تدار جميع الأصول بواسطة شخص أو مجموعة مكلفة من المؤسسة المالية، ممن لديهم مسؤوليات محددة وواضحة لإدارة الأصل المعني.

تصنيف الأصول

يجب تصنيف الأصول انطلاقاً من قيمتها وحساسيتها وحراجتها بالنسبة للمؤسسة، وكذلك متطلباتها القانونية.

العنونة والمعاملة

[7] ISO/IEC TR 13335-3, المراجع.

يجب إعداد مجموعة من الإجراءات المتعلقة بعنونة ومعاملة الأصول وتنفيذها بالتوافق مع جداول التصنيف التي تتبناها المؤسسة المالية.

العنونة دون الوقوع في المتاعب

1. تحديد المعلومات المرغوب استخلاصها من لصاقة العنونة مباشرةً.
2. تحديد جدول ترميز وترقيم مناسب.
3. التجميع ضمن كتلة حين توفر الإمكانية (مثلاً، إعطاء ترميز للشبكات المحلية الافتراضية، المخدمات، أو التجهيزات).

الاستخدام المقبول للمعلومات

يجب تعريف وتوثيق وتطبيق قواعد الاستخدام المقبول للآصول المعلوماتية المرتبطة بوسائل معالجة المعلومات.

6. الأمن والموارد البشرية

الإشكاليات	نسبة العينات	ملاحظات عامة
قانون وإجرائيات التوظيف	%75	إن وجود قانون تفصيلي يوضح حقوق وواجبات الموارد البشرية فيما يتعلق بأمن المعلومات كان المتطلب الرئيسي لمعظم العينات المدروسة في الجمهورية العربية السورية
تأثير طبيعة العلاقات الاجتماعية بالعلاقات المهنية على أمن المعلومات	%75	

<u>الخطوات التطبيقية الهامة:</u>

المجال

يجب أن تشمل سياسات المؤسسات المالية المتعلقة بالموارد البشرية إجمالاً جميع الأفراد خارج وداخل المؤسسات المالية الذين يستخدمون المعلومات ووسائل معالجتها.

الأدوار والمسؤوليات

يجب تعريف وتوثيق أدوار ومسؤوليات الموظفين والمتعاقدين والأطراف العقدية الثالثة من الناحية الأمنية، بما يتماشى مع سياسات الخصوصية وأمن المعلومات في المؤسسة المالية.

ما قبل التوظيف

يجب أن تقوم المؤسسات المالية أو طرف ثالث مناسب بعمليات التحقق من خلفية المرشحين للوظيفة ووضع المتعاقدين والأطراف العقدية الثالثة.

شروط وبنود التوظيف

على الموظفين والمتعاقدين والأطراف العقدية الثالثة الاتفاق والتوقيع على تصريح الحقوق والمسؤوليات الناجمة عن ارتباطهم مع المؤسسة المالية، بما في ذلك ما هو متعلق منها بخصوصية وسرية المعلومات.

اتفاقات إضافية لمرحلة ما قبل التوظيف

على الموظفين والمتعاقدين والأطراف العقدية الثالثة توقيع اتفاقات أخرى عند اللزوم، قبل إعطائهم أذن الدخول والسماحيات الأخرى إلى المعلومات ووسائل معالجتها.

مسؤوليات الإدارة

على الإدارة أن تلزم الموظفين والمتعاقدين والأطراف العقدية الثالثة بتطبيق وسائل التحكم الأمنية المنسجمة مع السياسات والإجراءات المتبعة في المؤسسة المالية.

التوعية والتعليم والتدريب

يجب القيام بحملة توعية وتدريب حول التحديثات في سياسات المؤسسات المالية وفي الإجراءات الوظيفية المتعلقة لكل من الموظفين والمتعاقدين والأطراف العقدية الثالثة.

عملية التأديب

يجب أن يتعرض الموظفون الذين يقومون بالمخالفة إلى عملية تأديبية رسمية.

مسؤوليات نهاية الخدمة

يجب التعريف والتكليف الواضح لمسؤوليات وممارسات أداء نهاية الخدمة أو تغيير الوظيفة.

استرجاع الأصول

على جميع الموظفين والمتعاقدين والأطراف العقدية الثالثة إعادة كافة الأصول المعلوماتية والفيزيائية التي في ذممهم إلى المؤسسات المالية حال نهاية علاقتهم الوظيفية أو عقدهم.

إلغاء حقوق الدخول

يجب إلغاء كافة حقوق الدخول إلى المعلومات ووسائل معالجتها حال انتهاء العلاقة الوظيفية أو العقدية.

7. الأمن من الناحية الفيزيائية والبيئية

الإشكاليات	نسبة العينات	ملاحظات عامة
تطبيق وصيانة وتغيير وفحص واختبار العديد من الحمايات الفيزيائية الموجودة	%100	تم الإجماع على ضرورة متابعة عمليات الصيانة وخصوصاً التي تتم من قبل شركات خارجية حيث تعتبر هذه العمليات سبباً رئيسياً لتسرب وفقدان المعلومات والتجهيزات
الخطوات التطبيقية الهامة:		

الطوق الأمني الفيزيائي

يجب أن يستخدم الطوق الأمني الفيزيائي من أجل حماية المناطق الحساسة التي تحتوي المعلومات ووسائل معالجتها. يجب تصميم وتنفيذ الحماية الفيزيائية للمكاتب والغرف والمنشآت الأخرى بحيث تتناسب مع المخاطر المُعرَّفة وقيمة الأصول المحتملة الإصابة في كل موضع.

وسائل التحكم بالمدخل الفيزيائي

يجب أن تتم حماية مناطق تواجد وسائل معالجة المعلومات الحساسة عن طريق وسائل التحكم على المداخل للتأكد من عدم تمكن غير المصرح لهم بالدخول اليها. كما يجب تصميم و تنفيذ الحماية الفيزيائية للمكاتب والغرف والمنشآت الأخرى بحيث تتناسب مع المخاطر المُعرَّفة وقيمة الأصول المحتملة الإصابة في كل موضع.

الحماية من التهديدات البيئية الخارجية

يجب تصميم وتنفيذ وسائل الحماية الفيزيائية ضد أخطار النيران والطوفان والعواصف والزلازل والانفجارات والعصيان المدني وكل أشكال المخاطر الأخرى الطبيعية منها وتلك ذات المنشأ البشري.

العمل في المناطق الحساسة

يجب تصميم وتنفيذ أدوات وإرشادات الحماية الخاصة بالعمل في المناطق الحساسة.

معابر الدخول والتسليم والتحميل العامة

يجب التحكم في نقاط العبور مثل مناطق التسليم والتحميل أو أية نقاط أخرى قد يلج من خلالها أشخاص غير مصرح لهم بالدخول إلى هذه المناطق.

وضع وحماية المعدات

يجب أن يتم وضع وحماية المعدات بشكل يقلل التهديدات والأخطار البيئية، وكذلك التهديدات البشرية بواسطة الدخول غير المصرح له.

الأدوات الداعمة

يجب أن تتم حماية الأجهزة من انقطاع التيار الكهربائي والاتصالات وغيرها من الأعطال الناجمة عن انقطاع التزويد بالأدوات الداعمة مثل المياه والصرف الصحي.

أمن الكبلات

يجب حماية كبلات الكهرباء والاتصالات التي تنقل بيانات حساسة أو خدمات المعلومات الداعمة من التدخل أو الضرر.

صيانة المعدات

يجب أن يُحافَظ على التجهيزات بصورة سليمة لضمان استمرارية إتاحيتها وصحتها.

ترحيل الأملاك إلى خارج المنشأة

لا يجوز إخراج أي تجهيزات أو معلومات أو برامج دون تصريح مسبق ومقيد.

أمن الأملاك خارج المنشأة

يجب تطبيق معايير أمنية ملائمة على المعدات خارج مرافق المؤسسات المالية مع الانتباه إلى اختلاف المخاطر داخل المنشأة عن خارجها.

أمن المعدات المنسقة أو المعاد استخدامها

يجب فحص كافة المعدات ذات وسائط التخزين وتجهيزات وسائط التخزين المستقلة للتأكد من خلوها من أية بيانات حساسة أو برامج مرخصة.

8. إدارة عمليات التشغيل والاتصالات

الإشكاليات	نسبة العينات	ملاحظات عامة
استراتيجية الحوادث والكوارث	%100	رغم وجود تصورات عن آليات العمل في حالات الحوادث والكوارث لم يتم تطبيق هذه التصورات وفق خطط تنفيذية بما يشمل مقرات العمل الاحتياطية وخصوصاً فيما يتعلق بالتجهيزات
استراتيجية المتغيرات	%75	
استراتيجية التوثيق والتقارير	%50	
النسخ الاحتياطي والأرشفة	%25	

<u>الخطوات التطبيقية الهامة:</u>

توثيق الإجراءات التشغيلية

يجب توثيق وصيانة وضمان إتاحة الإجراءات التشغيلية لكل من يحتاجها.

فصل المهام

يجب فصل الواجبات عن المسؤوليات إلى الحدود الممكنة، وذلك لتقليص فرص التعديل غير المتعمد(عن طريق الخطأ) أو غير المصرح به أو سوء استخدام أصول المؤسسة المالية.

فصل وسائل التطوير عن الاختبار عن التشغيل

يجب فصل أدوات التطوير عن الاختبار عن التشغيل إلى الحدود الممكنة، وذلك لتقليص مخاطر الدخول غير المصرح له أو التغيير الكلي لأنظمة التشغيل.

وسائل التحكم لحماية الموارد المركزية

يجب إدارة وضمان التحكم بوسائل معالجة المعلومات المركزية، مثل مخدمات التطبيقات ومعدات تخزين البيانات في "مراكز البيانات"، بصورة مناسبة قادرة على حمايتها من التهديدات والمحافظة على أمن الأنظمة والتطبيقات التي تستخدمها.

أمن الموارد المركزية

يجب تعريف كل المزايا الأمنية ومستوى الخدمة ومتطلبات الإدراة لكل الموارد والخدمات المركزية بالتفصيل، وإضافتها إلى اتفاقات الخدمات المقدمة ضمن المؤسسات المالية أو المحولة إلى طرف خارجي لتقديمها.

وسائل التحكم الشبكية

يجب إدارة وضمان التحكم بالشبكات بصورة مناسبة قادرة على حمايتها من التهديدات والمحافظة على أمن الأنظمة والتطبيقات التي تستخدمها، بما في ذلك المعلومات المنقولة عبرها.

أمن الخدمات الشبكية

يجب تعريف كل المزايا الأمنية ومستوى الخدمة ومتطلبات الإدراة لكل الخدمات الشبكية بالتفصيل، وإضافتها إلى اتفاقات الخدمات الشبكية المقدمة ضمن المؤسسات المالية أو المحولة إلى طرف خارجي لتقديمها.

التحكم بمحطات العمل

يجب إدارة وضمان التحكم بأجهزة محطات العمل بصورة مناسبة قادرة على حمايتها من التهديدات والمحافظة على الأمن عموماً، يتضمن ذلك معايير مشابهة للموارد المركزية والشبكية تطبق حين توفر الإمكانية التقنية والإدارية.

أمن تجهيزات محطات العمل

يجب تعريف كل المزايا الأمنية ومستوى الخدمة ومتطلبات الإدارة لكل خدمات محطات العمل بالتفصيل، وإضافتها إلى اتفاقات الخدمات المقدمة ضمن المؤسسات المالية أو المحولة إلى طرف خارجي لتقديمها، يتضمن ذلك معايير مشابهة للموارد المركزية والشبكية تطبق حين توفر الإمكانية التقنية والإدارية.

الترابط بين الأنظمة المعلوماتية

يجب إعداد وتنفيذ السياسات والإجراءات لحماية المعلومات المتعلقة الترابط بين أنظمة العمل.

الانترنت والرسائل الإلكترونية

يجب حماية المعلومات المتداولة عبر الرسائل الإلكترونية، مثل البريد الإلتروني، الرسائل البعيدة، الاجتماعات عبر الصوت والصورة، كل الاتصالات الشخصية فرد لفرد أو فرد لمجموعة أو مجموعة لمجموعة.

التجارة الإلكترونية

يجب حماية المعلومات المتداولة عبر التجارة الالكترونية والتي تستخدم الشبكات االعامة من أنشطة الاحتيال والكشف والتعديل غير المصرح له وكل نشاط آخر يؤدي إلى هجوم محتمل.

الخطوات التطبيقية للمعاملات المباشرة

يجب حماية المعلومات المتعلقة بالمعاملات المتداولة عبر الانترنت وخطواتها التطبيقية لمنع النقل الناقص أو التوجيه الخاطئ أو تبديل /كشف /مضاعفة الرسائل والرد غير المصرح له.

المعلومات المتاحة للعموم

يجب حماية صحة المعلومات المقدمة عبر حماية النظام الذي يؤمنها للعموم – مخدم الويب مثلاً– لمنع التعديل غير المصرح له.

إدارة التغيير والمشاريع

يجب التحكم بعمليات تغيير وسائل وأنظمة معالجة المعلومات عن طريق إجراءات إدارة التغيير والمشاريع المناسبة.

عوامل قبول النظام

يجب تأسيس عوامل قبول أنظمة المعاوماتية الجديدة والتحديثات والنسخ الجديدة والتأكد من نجاح اختبارها أثناء إعدادها وقبل اعتمادها.

إدارة الحوادث والمشاكل

يجب تسجيل الانحرافات عن عمليات التشغيل النظامية المتعلقة بوسائل معالجة المعلومات والتحقيق فيها باستخدام إجراءات إدارة الحوادث والمشاكل المناسبة.

إدارة التهيئة

يجب تسجيل وتحديث تهيئة أدوات معالجة المعلومات لكي تجاري التغييرات.

إدارة جودة واستيعاب الخدمة

يجب تحديد مستوى جودة الخدمة المتوقعة رسمياً لكامل مكونات الخدمة الأساسية، للواقع الحالي والمتطلبات المستقبلية أيضاً.

عقود خدمات الطرف العقدي الثالث

يجب أن تتضمن اتفاقات تسليم الخدمات على وسائل التحكم الأمنية وتعريف بالخدمات ومواصفات الخدمة المطلوبة.

9. التحكم بالوصول

الإشكاليات	نسبة العينات	ملاحظات عامة
متابعة ومراقبة تجهيزات وسياسات أمن الوصول وتغييرها في حال اقتضت الحاجة	%100	تم الإجماع على ضرورة تعريف سياسات تحكم بالوصول والدخول حيث تعتبر أي ثغرة في هذه السياسات سبباً مباشراً لمعظم عمليات الاختراق والتسريب

<u>الخطوات التطبيقية الهامة:</u>

سياسة التحكم بالوصول

يجب إرساء سياسة التحكم بالوصول وتوثيقها ومراجعتها دورياً على قاعدة حاجات العمل والمتطلبات الخارجية.

إدارة سياسة الدخول المستخدم

يجب أن تركز السياسات على ضمان دخول المستخدم المصرح له إلى المعلومات ووسائل معالجتها، ومنع دخول الغير

مصرح له.

تسجيل المستخدم

يجب تطبيق الإجراءات الرسمية لتسجيل المستخدم وإلغاء تسجيله، لضمان الدخول وعدم الدخول إلى كافة أنظمة وخدمات المعلومات. إضافةً إلى إعطاء هوية فريدة بكل مستخدم.

إدارة الامتيازات

يجب أن تكون أماكن توطين امتيازات الدخول مقيدة ومراقبة.

إدارة كلمة عبور المستخدم

يجب التحكم بأماكن توطين كلمات العبور من خلال عملية إدارة رسمية.

إدارة شارة دخول المستخدم

يجب التحكم بأماكن توطين الشارات، مثل الكروت الالكترونية، من خلال عملية إدارة رسمية.

مراجعة حقوق دخول المستخدم

يجب مراجعة حقوق دخول كل مستخدم دورياً من خلال عملية رسمية.

سياسة استخدام خدمات الشبكة

يجب أن يعطى المستخدمون حق الدخول إلى الخدمات الشبكية المصرح باستخدامها فقط.

التصريح للاتصال الخارجي

يجب اعتماد طرائق التصريح للتحكم بالدخول البعيد إلى الشبكة عندما يكون ذلك مناسباً ومجدياً من الناحية الفنية.

تعريف المعدات/ المواقع في الشبكة

يجب اقتصار الدخول إلى الشبكة على المعدات والمواقع المعرفة عندما يكون ذلك مناسباً ومجدياً من الناحية الفنية.

حماية منفذ التشخيص والتهيئة عن بعد

يجب التحكم منطقياً وفيزيائياً بالوصول إلى منافذ التشخيص والتهيئة.

فصل الشبكات

يجب فصل مجموعات المستخدمين والخدمات في الشبكات.

التحكم بالاتصال الشبكي

يجب تقييد حرية الاتصال بالشبكة بصورة مناسبة مدعمة بسياسات التحكم بالوصول ومتطلبات مختلف التطبيقات.

التحكم بالتوجيه الشبكي

يجب تطبيق وسائل التحكم بالتوجيه لضمان عدم مخالفة الاتصالات وجريان المعلومات لسياسات التحكم بالوصول من وإلى التطبيقات الموجودة على الشبكة.

التحكم باستخدام الأنظمة

يجب تنفيذ وسائل التحكم لتقييد الدخول إلى أنظمة التشغيل للمصرح لهم فقط عن طريق طلب التصريح من المستخدمين بما يتناسب مع سياسات التحكم بالوصول.

إجراءات الدخول الأمنية

وينبغي التحكم بالوصول إلى الأنظمة عن طريق إجراءات أمنية لتسجيل الدخول.

هوية وتصريح المستخدم

يجب أن يمتلك جميع المستخدمين وعلى كل الأنظمة اسم مستخدم وحيد لاستخدامهم الشخصي. ويجب اختيار آليات تصريح مناسبة مثل المبنية على المعرفة أو الشارة أو الثنائية للسماح بالاستخدام.

نظام إدارة كلمات العبور

على أنظمة إدارة كلمات العبور أن تتحقق من جودة طريقة التصريح بالدخول.

استخدام أدوات النظام التي تتجاوز وسائل التحكم

يجب أن يكون استخدام أدوات النظام التي تتجاوز زسائل التحكم مقيداً، ومراقباً بصورة مناسبة حين استخدامه (عن طريق عملية تسجيل أحداث مناسبة مثلاً).

انتهاء الجلسة

على الجلسات التفاعلية أن تغلق وتدع المستخدم خارجها بعد مدة زمنية معرفة. يجب إعادة التصريح من أجل معاودة الجلسة التفاعلية.

الحد من مدة ومكان الاتصال المسموح به

يجب أن يعطي تقييد زمن الاتصال أمناً إضافياً للتطبيقات عالية المخاطر أو لقابليات الاتصال البعيد.

تقييد الوصول إلى المعلومات

يجب تقييد الوصول إلى المعلومات ووظائف التطبيقات بما يتلاءم مع سياسات التحكم بالوصول المعرفة والمنسجمة بدورها مع سياسات المؤسسات المالية ككل، ويتضمن ذلك كل وسائل التحكم التي ذكرت في هذه الدراسة.

عزل الأنظمة الحساسة

يجب عزل الأنظمة الحساسة وتخصيصها ببيئة حاسوبية مستقلة.

10. اكتساب وتطوير وصيانة أنظمة المعلومات

الإشكاليات	نسبة العينات	ملاحظات عامة
المواصفات المطلوبة لوسائل التحكم الأمنية المرتبطة بالعروض المتعلقة بحاجة العمل لأنظمة معلومات جديدة	%100	ضرورة وجود هيئة مركزية لوضع المواصفات والمقاييس التي تحكم عمليات العروض والشراء الخاصة بأنظمة المعلومات

<u>الخطوات التطبيقية الهامة:</u>

متطلبات التحليل والتحديد

يجب أن تتضمن العروض المتعلقة بحاجة العمل لأنظمة معلومات جديدة، أو تعزيز تلك القائمة منها، على المواصفات

المطلوبة لوسائل التحكم الأمنية.

عملية تصحيح التطبيقات

يجب ان يتم التحقق من سلامة معالجة الأنظمة للبيانات المدخلة التي يتعاملون معها من عدة أوجه كالمعالجة الداخلية والرسائل ومخرجات البيانات بين العمليات والضياعات والتعديل غير المصرح به أو إساءة استخدام المعلومات.

استخدام وسائل التحكم بالتشفير

يجب تطوير وتطبيق وسائل التحكم بالتشفير المناسبة لحماية سرية وصحة ووثوقية المعلومات.

إدارة مفاتيح التشفير

يجب تنفيذ سياسات وعمليات إدارة المفاتيح لدعم استخدام تقنيات التشفير في المؤسسة المالية.

أمن برامج التشغيل

يجب تطبيق الإجراءات من أجل التحكم في تنصيب البرامج على أنظمة التشغيل والحد من مخاطر انقطاع أو تشوه الخدمات المعلوماتية.

ترميز أمن البرامج وبيانات الاختبار

يجب تقييد الدخول ترميز أمن البرامج.

وسائل التحكم في مواجهة الترميز الخبيث

يجب تطبيق وسائل حماية لمنع وكشف ومعالجة الترميزات الخبيثة.

اجراءات التحكم بالتغيير

يجب توثيق ومراقبة تنفيذ التغيرات عبر استخدام إجراءات رسمية لمراقبة التغيرات.

البرامج المطورة خارج المؤسسة المالية

يجب القيام بعمليات الإشراف والمراقبة من قبل المؤسسات المالية على البرامج المطورة خارجه باستخدام وسائل تحكم مشابهة لتلك المستخدمة في عمليات التطوير الداخلي.

تسرب المعلومات

يجب منع أو الحد من فرص تسرب المعلومات.

التحكم بالثغرات الفنية

يجب تحديث المعلومات المتعلقة بثغرات الأنظمة المعلوماتية بانتظام، وتقييمها على أساس المخاطر والتعرض للكشف واتخاذ إدوات الصد المناسبة.

11. إدارة حوادث أمن المعلومات

الإشكاليات	نسبة العينات	ملاحظات عامة

إعادة النظر في كامل إدارة الحوادث في المؤسسات المالية السورية	%100	

<u>الخطوات التطبيقية الهامة:</u>

رفع الحوادث المعلوماتية الأمنية

على جميع الموظفين والمتعاقدين والأطراف العقدية الثالثة أن تبلغ وترفع تقريرها حول أي ملاحظات أو شكوك عن أحداث أمنية عبر قنوات مناسبة وباسرع ما يمكن.

رفع نقاط الضعف المعلوماتية الأمنية

على جميع الموظفين والمتعاقدين والأطراف العقدية الثالثة أن تبلغ وترفع تقريرها حول أي ملاحظات أو شكوك عن نقاط ضعف أمنية في الأنظمة أو الخدمات عبر قنوات مناسبة وباسرع ما يمكن.

مسؤوليات وإجراءات الاستجابة للحوادث الأمنية

يجب تاسيس إجراءات ومسؤوليات الإدارة بوضوح للتأكد من استجابة سريعة ومنظمة لحوادث المعلومات الأمنية.

التحقيق في الحوادث

قد يكون اتخاذ خطوات قانونية أو تأديبية جزء من متابعة حوادث أمن المعلومات، يجب أن تتبع مباشرة أو إدارة أية تحقيقات إجراءات وتأكيدات موثقة لقبول هذه الممارسات.

جمع الأدلة

عند مباشرة التحقيق كجزء من عملية قانونية أو تأديبية محتملة، يجب أن يتبع جمع وترتيب وعرض الأدلة إجراءات وتأكيدات موثقة لقبول هذه الممارسات.

التعلم من حوادث المعلومات الأمنية

ينبغي وجود آليات تمكن من تحديد كميات ومراقبة أنواع وأحجام والتكاليف التقديرية لحوادث أمن المعلومات.

12. إدارة استمرارية العمل

الإشكاليات	نسبة العينات	ملاحظات عامة
إعادة النظر في كامل سياسات استمرارية العمل	%75	

<u>الخطوات التطبيقية الهامة:</u>

تضمين أمن المعلومات في إدارة استمرارية العمل

ينبغي إدارة وتطوير وصيانة عملية الحفاظ على استمرارية العمل في جميع أنحاء المؤسسة المالية، وهذا يتضمن متطلبات أمن المعلومات اللازمة لاستمرارية عمل المؤسسة المالية.

استمرارية العمل وتقييم المخاطر

ينبغي تحديد الأحداث التي قد تسبب في حدوث انقطاع في العمليات المالي ة، مع تحديد احتمال وتأثير مثل هذه الانقطاعات وآثارها على أمن المعلومات.

تطوير وتنفيذ خطط الاستمرارية

يجب اعداد وتنفيذ خطط استمرارية العمل لصيانة أو استعادة عمليات التشغيل، وضمان توافر المعلومات على المستوى المطلوب وفي الوقت المطلوب، متابعة الانقطاعات أو الاخفاقات في العمليات المالية.

إطار تخطيط استمرارية العمل

ينبغي وضع إطار واحد لخطط استمرارية العمل، لضمان تناسق جميع الخطط واستمرارية تقييم متطلبات أمن المعلومات، وتحديد الأولويات للاختبار والصيانة.

اختبار وتطوير وإعادة تقييم الخطط

ينبغي اختبار وتحديث خطط استمرارية العمل بشكل منتظم لضمان حداثتها وفعاليتها.

13. الامتثال

الإشكاليات	نسبة العينات	ملاحظات عامة
الحاجة لتقييم مركزي من قبل المؤسسات المالية (المصرف المركزي على سبيل المثال)	100%	إن وجود هيئة مركزية للمراقبة وتطبيق المعايير يعتبر أحد العوامل المهمة لمتابعة تطبيق هذه المعايير وفق متطلبات القطر.

<u>الخطوات التطبيقية الهامة:</u>

تحديد المتطلبات الداخلية والخارجية

ينبغي تحديد جميع الاحتياجات التعاقدية الداخلية والخارجية المطبقة تحت أمن المعلومات.

التوثيق

أن يوثق ويحدث النهج المنظم للمؤسسة والمعد لتلبية هذه المتطلبات بوضوح.

التواصل والتدريب والتوعية

ينبغي تداول المتطلبات الداخلية والخارجية بين جميع الأشخاص العاملين مع المؤسسة المالية، بما فيهم الجهات الخارجية التي تتعامل مع البيانات باسم المؤسسة المالية، عبر التدريب الملائم وبرنامج التوعية.

المراجعة الدورية

يجب القيام بمراجعة دورية للبيانات ونظامها ووسائل التحكم بها داخل المناطق الخاضعة لمسؤوليتها لضمان الامتثال للمتطلبات الداخلية والخارجية المطبقة.

و بناءً على الدراسة تم التوصل للنقاط التالية:

1) يمكن إعتبار المعايير ISO 27K و ملحقاتها (المذكورة في المراجع) الأكثر أهمية و أساساً لتحليل واقع أمن المعلومات في أي مؤسسة مالية كونها تشمل المعايير الأخرى (Basel 2, COBIT) –من ناحية أمن المعلومات–و كافية في حال تطبيقها للوصول الى حالة أمنية مستقرة وذلك وفق لما يلي:

g) ISO/IEC 27001.
h) ISO/IEC 27002.
i) ISO/IEC 13335-1:2004.
j) ISO/IEC TR 13335-3:2004.
k) ISO/IEC 15408-1:1999.
l) كما يمكن اعتماد اطار العمل NIST SP 800-53 rev1:2010 , كخطوات عملية لتطبيق السياسات الأمنية للمؤسسات الكبيرة و تقييمها.

2) اشتركت كافة المؤسسات التي أجريت عليها الدراسة بالتأكيد على ضرورة دعم وانخراط الإدارة، وبناء روابط قوية بين أمن المعلومات والعمل المالي، ليس من المنطلق التقني فحسب، وإنما بالتعامل مع المعلومات على أنها جزء من الأصول القيمة بحد ذاتها.
3) وبالانتقال إلى المخاطر، لا بد من التركيز على ضرورة أن تتبنى المؤسسات المالية السورية أن أسلوباً منهجياً للمساعدة على المقارنة و التعديل و المراجعة و التغيير عند الحاجة أيضاً. تشير التجارب العالمية إلى كون العمل في المؤسسة المالية واحداً من أكثر الأعمال حساسيةً تجاه السرية والخصوصية، حيث لا يسمح إلا بهامش ضئيل من الخطأ وإلا فسيواجه الفشل المحتوم.
4) لا يمكن الاستجابة بسياسات فعالة ومثمرة ما لم يتحقق الربط المناسب بين العمل المالي والمعلومات، ومن الضروري القيام بمراجعة عميقة وتفصيلية ووضع المؤشرات المناسبة من أجل ايصال هذه العملية إلى النجاح.
5) يعتمد تنظيم سرية المعلومات على التفاعل بين الأطراف المعنية الداخلية والخارجية، وبهذا هي أوسع من مجرد تشريعات والتزامات عامة، حيث أنها تضع الحدود التي لا يجوز تجاوزها منذ البداية وتظهر بجلاء مدى اهتمام المؤسسات المالية بأصولها المعلوماتية القيمة.
6) إن الانتقال من المفهوم التقليدي في التعامل مع تكنولوجيا المعلومات إلى المفهوم الحديث الذي يضمها إلى أصول الأعمال عملية شاقة، ليس بسبب الوسائل المعتمدة، ولكن بسبب علاقتها مع ثقافة المنظمة وبيئة العمل. وبكافة الأحوال، تعتبر هذه النقلة حركة إجبارية.
7) تشير الإحصائيات إلى أن أكثر من 80% من التهديدات التي تتعرض لها المعلومات ناتجة داخلياً من الكادر العامل، وأكثر من ذلك فإن 80% منها أيضاً غير مقصودة. يجب القيام بالعديد من الإجراءات تبدأ بمرحلة ما قبل التوظيف وحتى إنتهاء العلاقة الوظيفية لتقليص هكذا حوادث.

8) تلعب وسائل الحماية الفيزيائية دور حاجز الدفاع الأول مما يستدعي الاهتمام باختبارها وصيانتها.
9) يجب حماية العمليات التشغيلية اليومية كونها هي التي تضمن استمرار وازدهار العمل.
10)يعتبر التحكم بالوصول خلاصة الجهود المبذولة من أجل الحماية.
11)اكتساب وتطوير وصيانة المعلومات.
12)إدارة الحوادث, و أهمية وضع الخطط الفعالة للتعامل مع كل حدث و التخفيف ما أمكن من تأثيره.
13)إدارة استمرارية العمل بشكل جدي و مستمر و فعال لضمان عدم توقف الخدمات و العمليات.
14)ينبغي تحديد جميع الاحتياجات التعاقدية الداخلية والخارجية المطبقة تحت أمن المعلومات.

الاستنتاجات و التوصيات

وجدنا في نهاية هذه الدراسة و التي اعطيت نتائجها للمؤسسات المعنية, بوجود هوة كبيرة – تتفاوت درجتها بين مؤسسة و أخرى– بين الواقع الملموس و متطلبات أمن المعلومات العالمية, و أن المطلوب عمله كثير خصوصاً في غياب (أو قلة) المحددات و المعايير الوطنية من الجهات المختصة مثل المصرف المركزي ومجلس النقد و التسليف و وزارة الاتصالات و التقانة أو غيرهم من الجهات العليا ذات العلاقة[8].

كما وجدنا بأن المواضيع الخاصة بأمن المعلومات و السياسات الأمنية تتعلق الى حد كبير بشخص و كفاءة رأس الهرم الاداري و مدير المعلوماتية –التقنية– في تلك المؤسسات.

مع الأخذ في الاعتبار أنه لا يمكن لأي استراتيجية معلوماتية أمنية أن تحقق مناعة تامة ضد أي هجوم، إلا أن اختيار الضوابط المناسبة و إعداد الاستجابة للحوادث والتخطيط بعناية لإدارة التغيير بصورة مسبقة وما إلى ذلك، يحمل معه المزيد من النجاح في مقاومة العاصفة الأمنية الكبيرة القادمة، وبالتالي في حماية العمل مما قد يحدث.

إن أمن المعلومات هو عملية مستمرة ، وينبغي إعادة النظر في كل بند بانتظام، وتصحيحه وربما تغييره بقدر ما تتطلب عوامل دفع العمل، تتلخص بعض التوصيات على النحو التالي :

6. لا يمكن تطبيق أمن المعلومات دون دعم الإدارة.
7. يجب معاملة أمن المعلومات في إطار حماية أصول العمل وليس كمسألة فنية فقط.
8. يعتبر توعية وتدريب الكادر من العوامل الحاسمة، وعليه فيجب على إدارة المؤسسات المالية السورية بذل كل الجهود من أجل نشر مفهوم أمن المعلومات وأهميته.

[8] لابد من الاشارة الى وجود تعليمات لمجلس النقد و التسليف, مصرف سورية المركزي فيما يخص المخاطر التشغيلية إلا أنه لا يوجد آليات لتطبيق هذه القرارات و الرقابة عليها, المراجع.

9. يتعلق نظام إدارة أمن المعلومات أساساً بتحديد نطاقه و تشخيص المفاهيم و المنهجيات و إجراءات التصحيح و التنظيم، بالاضافة إلى التوثيق والاستعراض والإشراف.
10. بدءاً من تعريف نطاق أمن المعلومات، ينبغي على المؤسسات المالية السورية المضي في خطوات صغيرة ولكن مستقرة ومستمرة. ونقترح القضايا الفنية البحتة كنقطة بداية.

المراجع

[1] ISO/IEC 27001, Information technology- Security techniques - Information Security Management Systems (ISMS)- Requirements, 2005, 34.
[2] ISO/IEC 27002, or BS 17799, Information technology - Security techniques- Code of practice for information security management, 2005, 115.
[3] NIST SP 800-53 rev1, "Recommended Security Controls for Federal Information Systems", National Institute of Standards and Technology, USA, Department of Commerce, 2010, 422. http://csrc.nist.gov/publications/nistpubs/800-53A-rev1/sp800-53A-rev1-final.pdf
[4] ISO/IEC TR 13335-3, (Guidelines for the Management of IT Security: Techniques for the Management of IT Security), 2005, 509.
[5] ISO/IEC 13335-1, Information technology – Security techniques – Management of information and communications technology security – Part 1: Concepts and models for information and communications technology security management, 2004, 301.
[6] ISO/IEC 15408-1, Information technology – Security techniques – Evaluation Criteria for IT security – Part 1: Introduction and general model, 1999, 342.
[7] قرارات مجلس النقد و التسليف, مصرف سورية المركزي," المبادئ الأساسية لاستمرارية الأعمال" قرار 391م ن- ب4- 2008, "التعليمات الخاصة بالمخاطر التشغيلية" قرار 106-م ن- ب4-2005.

مقاربة جديدة لتصميم طريقة كمية لقياس و اختبار مستوى أمن المعلومات و الشبكات

أ.د. غسان فلوح*
أ.د. نور بك باشا**
المهندس وسيم أحمد***

الملخّص

تهدف هذه الورقة لتقديم معادلة جديدة لاختبار و قياس كمي لمستوى أمن المعلومات لكافة المؤسسات بشكل عام، و للمؤسسات المالية في سورية بشكل خاص.

تم الوصول الى هذه الطريقة – المعادلة– بعد اجراء دراسات[1] احصائية و تحليلية، و التي تم تنفيذها على عينة من المؤسسات المالية في سورية، و ذلك لاختبار و تحديد الفجوة بين واقع أمن المعلومات في تللك المؤسسات و المعايير العالمية في هذا المجال و خاصة ISO 27K ، كما أنه تمت الاستفادة من الطرق و المقاربات العالمية في هذا المجال.

كما تهدف هذه الورقة لتسليط الضوء على المتطلبات الخاصة لتطوير اطار العمل اللازم لتحسين مستوى أمن المعلومات و الشبكات في المؤسسات المالية؛ آخذين بعين الاعتبار الاعتبارات الخاصة للثقافة المحلية و متطلبات أمن المعلومات في سورية.

تم اجراء الدراسات الاحصائية و تحليلها خلال الفترة 2006–2010، وذلك على عدد من المصارف و المؤسسات المالية في سورية.

* أستاذ –قسم هندسة الحواسيب و الأتمتة– كلية الهندسة الكهربائية و الميكانيكية –جامعة دمشق –سوريا.

** أستاذ، مدير مركز أبحاث هندسة البرمجيات المتقدمة –جامعة كولالمبور–ماليزيا.

***قسم هندسة الحواسيب و الأتمتة– كلية الهندسة الكهربائية و الميكانيكية –جامعة دمشق طالب دراسات عليا(دكتوراه) –

[1]تم قبول نشر هذه الدراسات بورقة بحث علمي بالمجلة العلمية لجامعة تشرين في 17\2\2011

A Novel Approach to Design Quantitative Method for ICT Security Assessment

Eng. Wassim Ahmad[2]
wassimahm@gmail.com
Advisor: Prof. Dr. Ghassan Fallouh[3]
Co-advisor: Prof. Dr. Norbik Bashah Idris[4]

Abstract

The intent of this paper is to present a novel quantitative equation to assess information security level of general enterprises, establishments and corporate generally, and financial institutions specifically in public and private sector in Syria. This method is the result of statistical study[5] **which has been applied to a set of financial institutions in Syria as a sample of study to assess the gap between existing information security level and ISO 27K directives for ICT security, benefiting from other international approaches and models designed for this purpose.**

This study aims to spot a light on the special requirements and the modified framework required to develop ICT security in financial institutions taking in consideration the culture and the special conditions in Syria; Statistics and surveys were applied during four years (2006-2010) to four of main financial institutions in Syria including two important Banks of Syria.

[2] PhD candidate, Department of Computer Engineering and Automation, Faculty of Electrical and Mechanical engineering, Damascus University, Syria.

[3] Department of Computer Engineering and Automation, Faculty of Mechanical and Electrical Engineering, Damascus University, Syria.

[4] Centre for Advanced Software Engineering, University Technology Malaysia, Kuala-Lampur, Malaysia.

[5] This study has been accepted for publication as research paper in Tishreen University Journal for Research and Scientific Studies, Syria. Date 14 Feb. 2011.

1. Introduction and motivations

"When you can measure what you are speaking about, and express it in numbers, you know something about it; but when you cannot measure it, when you cannot express it in numbers, your knowledge is of a meager and unsatisfactory kind: it may be the beginning of knowledge, but you have scarcely, in your thoughts, advanced to a stage of science." (Thomson, 1894).

Information technology is not limited to a group of people or a group of companies only; it is applied in all sectors of life that is why ICT information security becomes increasingly important.

While some ideas for quantifiable ICT security measurements have been suggested recently (Bond, 2004), they are far from the unambiguous framework and definitions sought especially in Syria. The ambition of this work is to bring the research in the field closer to that goal especially in financial institutions in Syria which have the highest concerns about ICT security.

Simply, this research is going to find answers for these questions:

- How can ICT security level be measured or evaluated?
- What is the best way to modify international prototype to fit Syrian financial institutions requirements?
- How can we produce a quantitative equation representing the real situation and the gap between this situation and ISO 27K?
- What are the difficulties and restrictions preventing financial institutions from improving their information security level and reaching internationally acceptable level by applying international quantitative approaches?

2. Theoretical analysis

There are many definitions for ICT security, we can define it as: "a state of well-being of information and infrastructures in which the possibility of successful yet undetected theft, tampering, and disruption of information and services is kept low or tolerable" [ECCouncil, 2006].

ISO 27K defines it as "the preservation of Confidentiality, Integrity, and Availability. In addition other prosperities such as Authenticity, Accountability, Non-repudiation, and Reliability can be involved".

Reaching a secure environment in which companies can operate and provide services is the main goal for everyone since we are in the internet and electronic services era. Therefore all governments and research centers have been developing rules, regulations, guides, policies and controls to support their companies and organizations to achieve the that goal.

ISO 27K is an example of the result of that effort which helps facilitating and controlling the management of ICT security system.

National Institute of Standards and Technology NIST has well defined the benefit of measuring ICT security level in public and private sector (Performance Measurement Guide for Information Security, NIST Special Publication 800-55) which includes:

- **Increase Accountability:** Information security measures can increase accountability for information security by helping to identify specific security controls that are implemented incorrectly.
- **Improve Information Security Effectiveness:** An information security measurement program will enable organizations to quantify improvements in securing information systems and demonstrate quantifiable progress in accomplishing agency strategic goals and objectives.
- **Demonstrate Compliance:** Organizations can demonstrate compliance with applicable laws, rules, and regulations by implementing and maintaining an information security measurement program.
- **Provide Quantifiable Inputs for Resource Allocation Decisions:** Fiscal constraints and market conditions compel government and industry to operate on reduced budgets.

On the other hand neither NIST nor other institutions of research and standards has placed a quantitative method to measure ICT security level, in simple words, NIST has defined the importance of the target without showing how institutions can reach this target.

Research	Brief	Limitations
Scarfone,2008	It is one of the main models which was placed to assess ICT security level in institutions	No cultural factors were taken in consideration, moreover, it keeps the door open to modify the parameters of the resulted model to conclude quantitative model
Murdoch,2005	Measurement model of ICT security (without concluding any quantitative equation)	No resulted equation was concluded, only a measurement model (measures do not comply with conditions and culture in Syria)
Sadimies,2004	Quantitative model to measure ICT security level according to few directives of ISO 27K	Limited to few directives of ICT security, and it was applied in Finland
Bond,2004	Quantitative model to measure ICT security level according to only one directives of ISO 27K	Limited to one directive of ICT security
NIST Papers	They covered the necessity of using quantitative method to measure ICT security level	No equation or definite model was included in these paper

3. Designing and Implementing

In Syria, measuring ICT security level (including ISO 27K compliance measurement) through applying international researches or standards like: (Scarfone, 2008), (Gutierrez, 2008), (Sadimies, 2004), (Bond, 2004), and (NIST papers) is not an easy task due to the following reasons:

1. There are no laws or regulations to govern and control electronic services till now, for example: digital documents – even with digital signature- is not accepted as valid documents in courts.
2. The lack of qualified local staff in the field of information security.
3. Decision makers may face difficulties to understand the necessity of equipments, services, and procedures which are recommended by ICT security experts.
4. The culture factor, where the leader controls law, not the law is the one which controls the leader; That means both of GM and IT managers must be aware of the importance and the necessity of ICT security in their organizations to be able to apply ICT security standards according to their understanding and approach not to the standards and regulations.
5. The lack of good training and awareness programmes related to information security in both public and private sectors.
6. The fact that more than 65% of employees in IT staff are females, and 90% of them lost their well and ability to learn and develop their knowledge after having children. Although if they are not married, it is not possible for them to work in evening or night shifts, because of traditions and local culture.
7. The average salaries of government organizations are very low, which results in losing the young and qualified employees who move to work in foreign countries or even in the private sector.
8. The complexity of the existing guides –like ISO 27K- to be understood and applied by IT staff where 80% of them are not aware of security requirements.

For those reasons in addition to the necessity of assessing information security level of companies in Syria, this research was launched by studying the conditions of four main financial institutions including the largest bank which is Commercial Bank of Syria as it has 100 branches, over 5000 employees, and more than 70% of market share in Syria

This research was developed by following these steps:

1. Statistical study (survey) of the current security status of these four financial institutions through formal questionnaire forwarded to IT managers in these institutions taking both ISO 27001and ISO 27002 directives in consideration.
2. Analysing the results obtained from the four institutions, focusing on the gap between current situation and required standards.
3. Weighting each directive and control of ISO 27K according to their importance in the current environment.
4. Developing an equation reflects the real situation of the ICT security level of the financial institutions in Syria.
5. Developing an automated system that can be easily used by IT managers, security offices, and auditors to automatically evaluate the institution ICT security level in those institutions.
6. Implementing the resulted equation on one of financial institutions in Syria (the bank was not included in our set of survey samples)

3.1 Weighting ISO 27001-27002 directives and controls

Based on statistics and surveys which have been applied to our set of samples, we managed to approximate the weight of each ICT security control and directive according to its importance and to which limit it may affect the ICT security level in these institutions, for this goal we followed below mentioned methodology:

1. Combining the two domains of ISO 27001, which are:

Domain
1-ISMS (information Security Management System)
2-Risk Assessment

With the 11 domains of ISO 27002:

Domain
3-Security Policy
4-Organization of Information Security
5-Asset Management
6-Human resources security
7-Physical and Environmental security
8-Communication and Operations Management
9-Access Control
10-Information system acquisition, development and maintenance
11-Information security incident management
12-Business Continuity Management
13-Compliance

The resulted 13 domains can build comprehensive approach to ICT security.

2. Weighting each directive and control from these 13 domains according to the following:
    a) Its importance in the whole security environment.
    b) Ability to apply it. For example the control "there is a senior management forum to discuss ISM policies, risks and issues" (domain: information security policy), cannot be applied, simply because senior managers do not have time for this task, according to the survey.
    c) The existence of the service related to the control.
3. Concluding linear equation which gives the final score of ICT security level, taking in consideration that we chose a linear format for simplicity and we considered reformatting this equation using non-linear format as future work.
4. the final score will be compared to five levels of security status, which is produced automatically by the program:

Security level	Score
POOR	UP TO 40
LOW	40-60
MEDIUM	60-80
HIGH	80-90
FULL	90-100

5. The output of the program will include in-depth gap analysis between the current status

of the target of evaluation, and ISO 27K, along with recommendations to correct the situation.

4. Designing and Implementing

Here we need to have a detailed version of a prototype model to assess security level in Syrian financial institutions according to ISO 27K, taking in consideration that the design must be presented in details benefiting from all presented models and prototypes.
In this part, we are going to conclude and place a design for ICT assessment of ISO 27K compliance, so we can assess its directives weight in the resulting equation.
Expected results, limitations, and theoretical analysis must be presented in this part.
Finally automatic measurements of data will be developed as program which gives as an output the final equation and automatic analysis of the measures obtained.

4.1 Measurements and the equation

The following factors have been considered during development and implementation of this information security measurement research that yields the quantitative equation:

- Measures must yield quantifiable information (percentages, averages, and numbers).
- Data that supports the measures needs to be readily obtainable;
- Only information security processes which might be applied to all financial institutions should be considered for measurement.
- Measures must be useful for tracking performance and directing resources.
- Rules and regulations in Syria related to information security especially for financial institutions should be taken in consideration.
- Country culture, social barriers, traditions, and realistic approaches to reach a secure environment for financial institutions to operate are also considered in these measurements.

4.2 Weighting controls and domains and the resulting equation

We followed below mentioned method:

1. Each control is assigned a specific weight (integer value).
2. The summation of each domain controls values will result in the domain value, which is 100 points as maximum.
3. Each domain can be powered to a positive integer number and/or multiplied by positive integer value; according to its importance.
4. Appendix 1 displays samples of the survey conducted, and weighting of controls.
5. The final equation will be of the form:

$$L = \frac{1}{m}\sum_{i=1}^{n} \alpha_i \cdot V_i^{\beta_i}$$

Where:

- L : The final level of the organization security, which is an integer value from 1 to 100.
- m : The sum of α_i, which is related to how we decide to allocate controls –for example 13 domains-, and the value of β_i and α_i.
- n : The number of domains.
- α_i : Factors multiplied to each domain final value according to its importance.
- V_i : The domain final value, which is the summation of all its control's value, V_i is from 1 to 100.
- β_i : The power of V_i according to domain importance, β_i could be 1,2,3…

4.3 Assumptions

For the sake of this paper and to reduce complexity, we will follow the following assumptions:

4. We will consider $\beta_i = 1 \; for \; all \; i$. β_i Could be for future development.
5. $n = 13$, the number of domains.
6. $m = \sum_{i=1}^{13} \alpha_i$, where α_i is the values of α_i are the average values collected from the survey.

I	Domain	α_i
1	ISMS (information Security Management System)	2
2	Risk Assessment	1
3	Security Policy	2
4	Organization of Information Security	2
5	Asset Management	2
6	Human resources security	5

7	Physical and Environmental security	4
8	Communication and Operations Management	2
9	Access Control	4
10	Information system acquisition, development and maintenance	3
11	Information security incident management	3
12	Business Continuity Management	2
13	Compliance	3

m = 35.

7. Important Note: all variables in the equation, the number of domains, controls in each domain, and weights can be modified automatically by the program developed for this purpose.
8. The equation will be of the form:

$$L = \frac{1}{35}\sum_{i=1}^{13} \alpha_i \cdot V_i$$

5. Experimental results and discussion

Here we are going to apply our application which was developed based on the quantitative method we have concluded from our research on a bank in Syria as a sample of Syrian financial institution and measure the level of Security in this bank, then we applied our survey and experts' measure to check and see how much is our model gives right results

The results of applying our quantitative method, were assembled in detailed report and submitted to this bank, this report consists of more than 40 pages, and as it is impossible to include the results in our research paper we are going to spot a light on main weaknesses and ICT security limitations in the bank, in addition to the level of ICT security in the bank based on our quantitative model:

Security Policy

1.1. INFORMATION SECURITY POLICY

1.1.1. INFORMATION SECURITY POLICY DOCUMENT

1.1.2. REVIEW OF THE INFORMATION SECURITY POLICY

Information security policy	Yes	No	Comments
Are the policies communicated, understood and accepted? • Standards for physical security of the computer and telecommunications installation and associated facilities; • HR procedures governing access to and use of IT services (usernames and passwords, disciplinary procedures); • End user guidelines covering PC software licensing and virus prevention, etc?	☒ ☒	☒	Needs to review
Are they reasonable and workable?	☒		
Do they incorporate suitable and sufficient controls?	☒		Partially
Do they cover all essential computing and telecommunication services?		☒	Only applied on technical level

Section 2

Technical Security Policies	Yes	No	Comments
Is a technical security policy in place?	☒		
Are unused services disabled?		☒	
Are unused interfaces disabled?		☒	
Do any applications use telnet to perform management activities such as backing up configuration?	☒		
Do passwords appear in encrypted form wherever they viewed or appeared?	☒		
Do the passwords meet with the required complexity as defined by the policy?		☒	
According to policy, Is there any enforcement to change passwords regularly?	☒		
Is authentication done through: Locally configured usernames and passwords TACACS+/ RADUIS/ Database server	☒ ☒		
Is there a documented procedure for creation of users?		☒	
Does each administrator have a unique account for himself/herself?		☒	
Is there a login and logout tracking/command history?		☒	
Are all user accounts assigned the lowest privilege level that allows them to perform their duties? (Principle of Least Privilege)	☒		
Are the default settings changed in all systems and equipments?	☐	☐	
Is the NTP server service used to synchronize the clocks of all equipments?	☒		
Is configurations backed up done regularly?	☒		
Is the backup moved to an off-site/DR site?	☒		
On the system where the configuration files are stored, is the local operating system's security mechanisms used for restricting access to the files (i.e., the machine should be password enabled and prevent unauthorized individuals from accessing the machine.)?	☐	☐	
Is the TFTP protocol used to transfer network configuration or image files? If yes, Is the TFTP process restricted to certain addresses only? Is the TFTP service disabled when not in use?	☒		Yes to all
Is there a documented procedure for backup of configuration files?	☒		
Are all changes and updates documented in a manner suitable for review according to a change management procedure?	☒		
Is there a redundant machine in cold standby or hot standby?	☒		
Are disaster recovery procedures for the network documented and are they tested?	☒		
Are all attempts to any port, protocol, or service that is denied logged?		☒	

Are all CPUs /memories / storages monitored?		☒	
Is there a special logging server enabled and login restricted?	☒		
Are procedures for audit log review generated by different systems and machines documented and followed?		☒	
Are all logs (covering administrator access /access control) reviewed?		☒	
Are reports and analyses carried out based on system and log messages?		☒	
Is there any course of action to be followed if any malicious incident is noticed?		☒	
Are the network/ system /applications /services engineers aware of the latest vulnerabilities that could affect their domain of proficiency?		☒	

Gap Analysis

As long as Information Security Policy not reflected on the bank strategy and business objectives, despite of general unawareness of necessity to be fully understood by staff, it makes policies too hard to be followed or applied.

The gap can be divided to three critical missing processes as below:

- Follow up process;
- Review process;
- Corrective actions; and
- Tracking /over sighting process.

Code of Practice[1]

Objective

Information Security Policy should provide management directions and support for data protection, in accordance with the norms of professional ethics, business requirements and all relevant laws, regulations and private certificatory requirements.

Scope

ISP, taken as a whole, should provide clear controls for all data collected, used or stored in the bank's data processing, communications, and storage systems, as well as for data collected, used or stored in the systems of external parties under contract with the organization.

Approval

ISP should be formally approved by appropriate organizational authorities.

Documentation

ISP should be fully documented in designated organizational document repositories. Policy documentation could include:

- overall objectives and scope, including statements of management intent, supporting goals and principles;
- listing of identified authorities (statutory, regulatory, private) and requirements that condition or control data protection activities, including an explanation or listing of policies, principles, standards and compliance requirements relevant to the organization;
- framework for setting policy objectives and components of the policies themselves, including a structure for risk assessment and risk management;
- definitions of general and specific responsibilities for the organization's data security management;
- references to additional documentation that supports or underpins the policies; and
- Formal historical record of material changes to the policies and any accompanying approvals.

[1] SOURCES: ISO-27001/27002:2005, sects. 5.1.1 – 5.1.2.

Communication, training and awareness
ISP should be communicated to all relevant affiliates of an organization, as well as relevant external parties, via an appropriate training and awareness program.

Periodic review
ISP should be reviewed at planned intervals, and when significant changes in the external environment occur, to ensure their continued suitability, adequacy and effectiveness. Review steps could include:

- solicitation and integration of feedback from all interested parties inside and outside the Bank;
- independent contracted external reviews;
- checklists of recommendations and requirements of relevant authorities;
- consideration of trends in threat types and threat capabilities, system vulnerabilities, and available technologies for counter-measures and mitigation;
- consideration of trends in compliance requirements of domestic and private certificatory authorities;
- consideration of trends in and anticipated changes to the organizational environment, business circumstances, and resource availability;
- historical data on information security incidents at the organization itself and at peer institutions; and
- Formal historical record of the reviews undertaken as part of policy development and refinement, and their outcomes.

Coordination with other policies
Review of ISP should include consideration of other relevant organizational policies, to minimize inconsistencies and gaps. This could include:

- identification of all other relevant policies; and
- Inclusion of the representatives from the areas responsible for such policies in the periodic review of information security policy.

After applying our model, we have submitted our report to the technical department of the bank –subject to the search- and we asked about their feedback and evaluation of each directive in addition to their evaluation of their total level of security as a percentage of accuracy and we have the following results which reflect accuracy of our quantitative method.

Domain	Bank feedback (%)
ISMS (information Security Management System)	85
Risk Assessment	90
Security Policy	83
Organization of Information Security	88
Asset Management	82
Human resources security	91
Physical and Environmental security	95
Communication and Operations Management	80
Access Control	87
Information system acquisition, development and maintenance	83
Information security incident management	88
Business Continuity Management	89
Compliance	90
Average Acceptance	87%

The result shows that the Bank IT experts agree upon 87% with the results given by our equation.
This means that our equation can be considered as acceptable method for measuring ICT security level of financial institutions in Syria.

9. Conclusion

The few quantitative methods which were developed by international institutions and researchers to measure the level of ICT security level in organizations, establishments, companies...etc are limited to the culture of the countries and business sectors in the countries from which they came, moreover, these approaches needs to be fine tuned to comply with business requirements and needs in financial institutions in Syria.

We have developed new quantitative method based on ISO 27K standards benefiting from the knowledge base we assembled about business sector in Syria in general, and financial institutions in particular.

Based on the experimental results we could verify that our model reflects ICT security level in financial institutions in Syria including recommendations and countermeasures which can be a corner stone in recognising the level of security in these institutions and to solve all problems and vulnerabilities which may affect the whole process of business in these institutions.

7. Future work

We can summarize the future work in below mentioned points:

1- We have developed our quantitative method based on linear approach (as an approximation), as a future work we can compare our linear approach with none linear approaches which may result in better model and methods

2- Due to long time and big effort we need to spend on our samples while making our surveys and applying resulted models, it is strongly recommended –as a future work- to use more samples while performing surveys and concluding quantitative methods and models.

3- To foster our results and concluded methods, it is more convenient to use a third party consultants to measure the gap between ICT security level in financial institutions and the results calculated based on our quantitative method

8. Appendix 1 (Survey and Weighting – Samples-)

Item No.	Weight					Notes	Findings			Questions
	Average	Sample1	Sample2	Sample3	Sample4		Partially Applied	No	YES	
										1-Information security management system (ISMS)
1	20	15	20	23	22		☐	☐	☐	Is there any evidence that management genuinely understands and supports the ISMS?
2	15	15	16	10	20		☐	☐	☐	Is there any exclusion from ISMS scope?
3	10	8	10	9	13		☐	☐	☐	If yes; are there justified reasons for excluding any elements?
4	15	11	12	17	17		☐	☐	☐	Does organization's ISM Policy adequately reflect the organization's general characteristics and its strategic risk management approach?
5	20	18	22	17	20		☐	☐	☐	Does ISM incorporate the organization's business requirements plus any legal or regulatory obligations for information security?

Item No.	Weight					Notes	Findings			Questions
	Average	Sample1	Sample2	Sample3	Sample4		Partially Applied	No	YES	
6	20	21	25	22	12		☐	☐	☐	Has it been formally approved by management and set meaningful criteria for evaluating information security risks?
										2-Risk Assessment (14 Controls)
1	10	13	10	9	8		☐	☐	☐	Is there any systemic risk assessment method(s)?
2	6	6	5	7	7		☐	☐	☐	Are the results of risk assessments comparable and reproducible?
3	7	6	7	8	6		☐	☐	☐	Is the risk assessment method updated as a result?
4	9	5	10	12	10		☐	☐	☐	Is the definition of criteria sensible and practicable in relation to information security risks?
5	8	9	7	6	8		☐	☐	☐	Are all relevant in-scope information assets included?
6	1	1	1	1	1		☐	☐	☐	Are responsible owners identified for all the information assets?
7	6	4	5	6	9		☐	☐	☐	Is there an adequate analysis/evaluation of threats?
8	6	7	8	4	5		☐	☐	☐	Is there an adequate analysis/evaluation of vulnerabilities and impacts?
9	5	9	3	2	6		☐	☐	☐	Is there an adequate documentation of risk scenarios plus the prioritization or ranking of risks?
										2-1 Risk Treatment Plan
10	10	12	8	11	9		☐	☐	☐	Are appropriate "treatments" specified for all identified risks?
11	6	4	5	7	9		☐	☐	☐	Are changes suitably fitted in the plan?

Item No.	Weight					Notes	Findings			Questions
	Average	Sample1	Sample2	Sample3	Sample4		Partially Applied	No	YES	
12	8	10	9	8	5		☐	☐	☐	Is the Risk Treatment Plan being used and updated proactively as an information security management tool?
13	8	7	12	6	7		☐	☐	☐	Are defined controls objectives and selected controls satisfied?
14	10	9	8	12	11		☐	☐	☐	Is the organization effectively and proactively reviewing the implementation of the ISMS to ensure that the security controls identified in the Risk Treatment Plan, policies, etc. are actually implemented and are in fact in operation?
							3- Management responsibility			

Item No.	Weight					Notes	Findings			Questions
	Average	Sample1	Sample2	Sample3	Sample4		Partially Applied	No	YES	
1	20	19	23	22	15		☐	☐	☐	Are there enough resources allocated to the ISMS in terms of budget, manpower etc?
2	15	17	14	13	16		☐	☐	☐	Are sufficient funds allocated by management to address information security issues in a reasonable timescale and to a suitable level of quality?
3	6	9	6	4	5		☐	☐	☐	Do the top managers seriously commit to information security in their behaviour?

Item No.	Weight					Notes	Findings			Questions
	Average	Sample1	Sample2	Sample3	Sample4		Partially Applied	No	YES	
4	12	13	11	12	11		☐	☐	☐	Are necessary competencies and training/awareness requirements for information security professionals and others with specific roles and responsibilities explicitly identified?
5	10	8	12	11	9		☐	☐	☐	Is there a scheduled reviewing, at last once a year?
6	6	5	4	5	10		☐	☐	☐	Does management play an active part and is fully engaged in the review/s?
							3-1 Internal ISMS audits			
7	8	10	6	9	7		☐	☐	☐	Is there any internal audits plan?
8	8	9	7	6	10		☐	☐	☐	If yes, are responsibilities for conducting ISMS internal audits formally assigned to competent, adequately trained IT auditors?
9	15	15	17	16	12		☐	☐	☐	Does ISMS changes in response to the identification of significantly changed risks?
							4- Information security policy			
1	15	11	12	19	18		☐	☐ ☐ ☐ ☐	☐ ☐ ☐ ☐	Are the policies communicated, understood and accepted? Standards for physical security of the computer and telecommunications installation and associated facilities; HR procedures governing access to and use of IT services (usernames and passwords, disciplinary procedures) End user guidelines covering PC software licensing and virus prevention, etc?

Item No.	Weight					Notes	Findings			Questions
	Average	Sample1	Sample2	Sample3	Sample4		Partially Applied	No	YES	
2	8	8	10	6	7		☐	☐	☐	Are they reasonable and workable?
3	5	3	4	8	5		☐	☐	☐	Do they incorporate suitable and sufficient controls?
4	8	7	10	6	5		☐	☐	☐	Do they cover all essential computing and telecommunication services?
							4-1 Internal Responsibilities and Communications			
5	4	5	7	2	2		☐	☐ ☐ ☐ ☐	☐	Are the following positions well defined and activated: Senior manager responsible for IT and ISM; Information security professionals; Security administrators; Site/physical security manager and Facilities contacts; HR contact for HR matters such as disciplinary action and training; Systems and network managers, security architects and other IT professionals.

Item No.	Weight					Notes	Findings			Questions
	Average	Sample1	Sample2	Sample3	Sample4		Partially Applied	No	YES	
6	5	5	4	5	6		☐	☐	☐	Is ISM given sufficient emphasis (is there a 'driving force'?) and management support?
7	2	1	2	3	2		☐	☐	☐	Is there a senior management forum to discuss ISM policies, risks and issues?
8	8	9	6	10	5		☐	☐	☐	Are roles and responsibilities clearly defined and assigned to skilled individuals?
9	3	2	2	3	5		☐	☐	☐	Is there sufficient co-ordination within the BU (business unit), between BUs and with HQ?
10	5	6	7	5	3		☐	☐	☐	Are the information flows (like incident reporting) operating effectively in practice?
							4-2 External Parties			

Item No.	Weight					Notes	Findings			Questions
	Average	Sample1	Sample2	Sample3	Sample4		Partially Applied	No	YES	
11	10	12	11	9	8		☐	☐	☐	Is there a risk analysis process in place for 3rd -party communications and connections?
12	5	3	6	9	3		☐	☐	☐	Is there any individual who has responsibility for ensuring that all 3-party links are in fact identified and risk assessed?
13	7	7	9	8	5		☐	☐	☐	Are ISM arrangements in operation on 3-party connections routinely reviewed against the requirements?

Item No.	Weight: Average	Weight: Sample1	Weight: Sample2	Weight: Sample3	Weight: Sample4	Notes	Findings: Partially Applied	Findings: No	Findings: YES	Questions
14	12	12	10	12	14		☐	☐		Are there formal contracts covering 3rd party links?
								☐		Ownership and responsibility for ISM issues?
								☐		Legal requirements?
								☐	☐	Protection of systems, networks and data via physical, logical and the right of audit by the organization?
									☐	Procedural controls business assets, availability of services in the event of disasters, management notification for security incidents?
										Security clearance of staff?

9. References

[1] William Thompson, Lord Kelvin, Popular Lectures and Addresses [1891-1894], in Bartlett's Familiar Quotations, Fourteenth Edition, 1968, p. 723a.

[2] ECCouncil, www.eccouncile.org, 2006.

[3] ISO/IEC 27001:2005, Information technology-Security techniques-Information Security Management Systems (ISMS)-Requirements.

[4] ISO/IEC 27002 or BS 17799:2005, Information technology-Security techniques-Code of practice for information security management.

[5] Performance Measurement Guide for Information Security, *NIST Special Publication 800-55*, www.nist.gov.us.

[6] Bond, A. (2004). *A quantitative evaluation framework for component security in distributed information systems.* Linkoping University: Institute of Technology.

[7] Sademies A. and Savola R. Measuring the Information Security Level – A Survey of Practice in Finland. In: Proceedings of the 5th Annual International Systems Security Engineering Association (ISSEA) Conference, Arlington, Virginia, October 13-15, 2004. 10p

[8] Murdoch, J. (2005, July). Security Measurement. York, United Kingdom.

[9] Scarfone, K. (2008, September). Technical guide to information security testing and assessment. Gaithersburg, United States of America.

Brief of Thesis titled: موجز عن البحث باللغة الانكليزية

"Novell Approach to the Design and Implementation of Network and Information Security Based on Layered Approach[1]"

Introduction:

The aim of this research is to design a new model for network and information security with the following objectives:

1. Covering all aspects of Network and Information security.
2. Including international standards especially ISO 27000 series.
3. The model contains several layers which facilitate the implementation, and each layer contains several security domains.
4. Defining risks threatening information security, using specific methodology.
5. Defining Security Controls for each domain. Controls are rules and procedures to overcome a specific risk.
6. Ability to practically apply the model on the Syrian Companies.
7. Develop a new equation for measuring quantitatively the overall security status of a specific company.
8. Write research papers about the research, and submitted to well known refereed Journals to be insure the research importance and feasibility.
9. Develop a program to automate the process of applying the model.
10. Apply the model and analyze the results.

Thesis Sections

The research includes in depth study of several topics in the following sections:

[1] Note: the research thesis will be submitted in Arabic.

1. Section (1), the referential studies: reviews and analysis of the following subjects:
    a. System Analysis and design.
    b. Networking
    c. Information and Network Security
    d. Cryptography
        - Symmetric and Asymmetric Cryptography.
        - Block ciphers.
        - AES algorithm.
        - RSA algorithm.
        - Diffie-Hellman algorithm.
        - PKI infrastructure.
        - Digital Certificate and Digital Signature.
        - Cryptanalysis
    e. International standards of Network and Information Security.
        - ISO 27000 series.
        - Control Objectives for Information and related Technology (CobiT 4.1).
        - National Institute of Standards and Technology (NIST) Special Publications.
        - Social Engineering.
        - White papers and researches published, related to assessment and measurement of information security.
            - NIST SP800-115.
            - A Quantitative Evaluation Framework for Component Security in Distributed Information Systems, written by Andres Bond & Nils Pahlson, 2004.
            - Security Measurement by John Murdoch, 2005.
2. Section (2), Analysis and Design studies

In this section we introduce a proposed Model for Network and Information Security based on the referential studies which included the following standards:

a) ISO/IEC 27001.

b) ISO/IEC 27002.

c) ISO/IEC 13335-1:2004.

d) ISO/IEC TR 13335-3:2004 .

e) ISO/IEC 15408-1:1999.

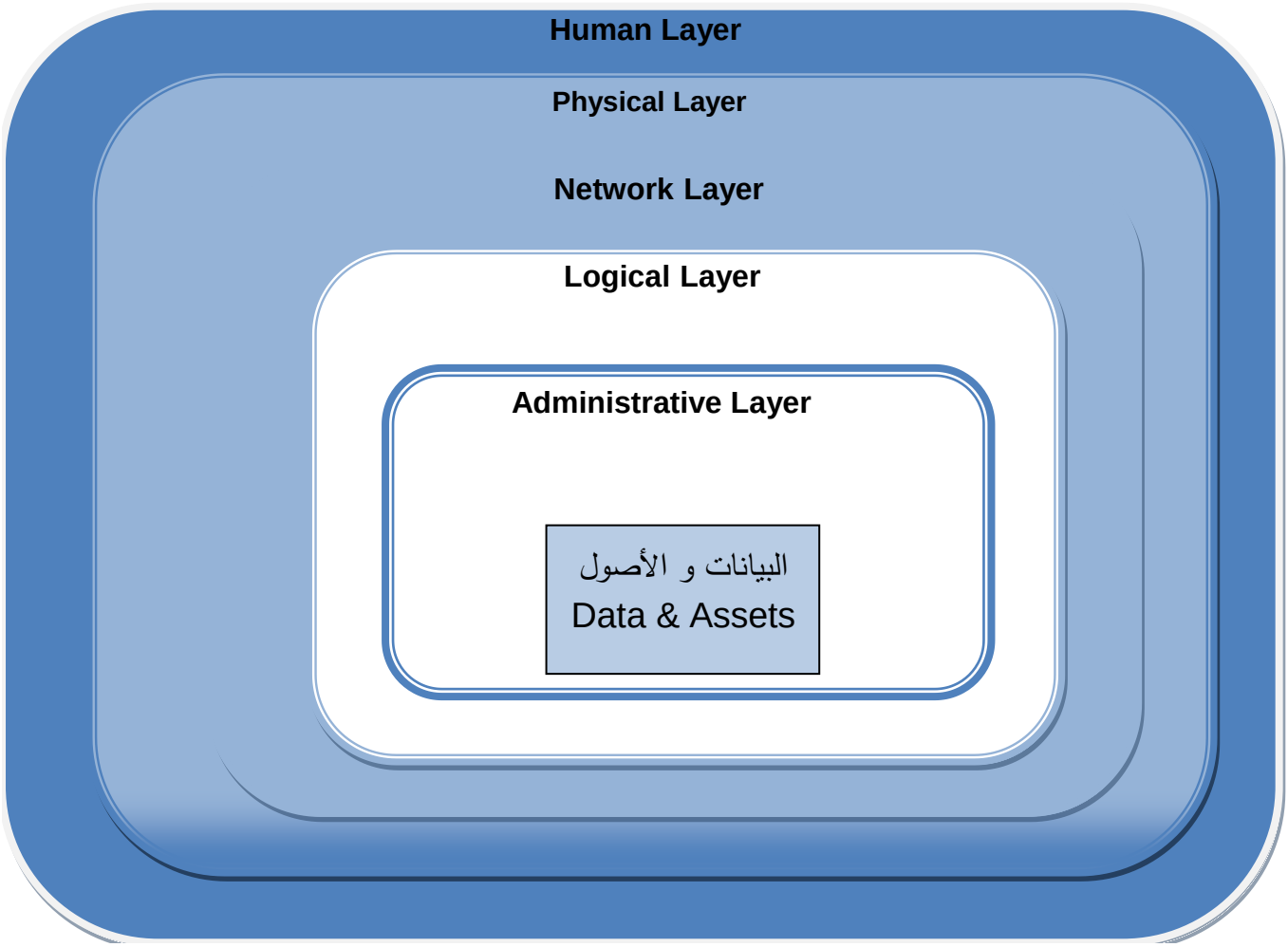
f) NIST SP800-53 rev1:2008.

The model has been developed to help achieve more secure information systems within government and private institutions by:

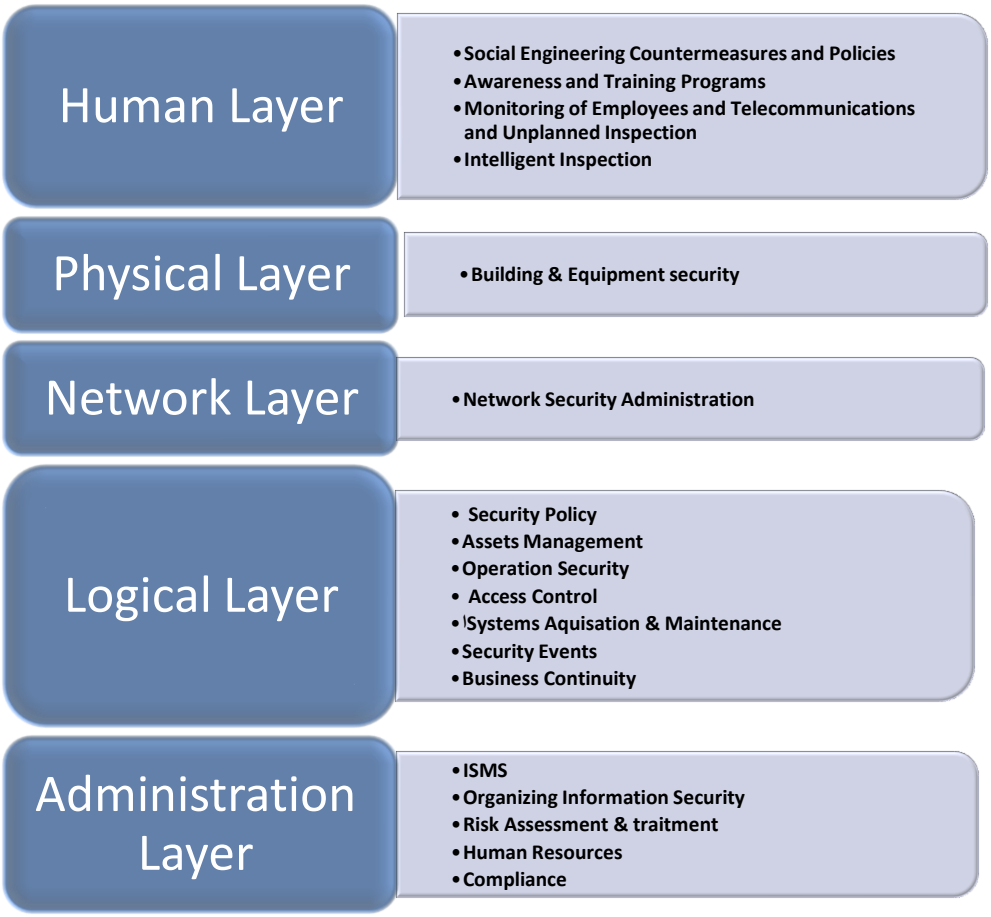
- Enabling more consistent, comparable, and repeatable assessments of security controls;
- Facilitating more cost-effective assessments of security controls contributing to the determination of overall control effectiveness;
- Promoting a better understanding of the risks to organizational operations, organizational assets, individuals, other organizations, and the Nation resulting from the operation and use of federal information systems; and
- Creating more complete, reliable, and trustworthy information for organizational officials—to support security accreditation decisions, information sharing, and government compliance.

And security controls defined in the model are able to be measured quantitatively.

a) The proposed model:



This model includes 18 security domains:



Each domain contains security controls to achieve its objectives. Information security is achieved by implementing a suitable set of controls, including policies, processes, procedures, organizational structures and software and hardware functions; in addition to controls related to countermeasure social engineering and human related aspects of security.

b) Analyze the proposed model:

We offer in this chapter an in-depth analysis of the proposed five layers model and how it is related to ISO 27K series and other international standards and guidelines, in addition to its reflection to the special situation and requirements of information security in Syria; and how this model can be applied to improve the overall security environment of institutions and companies working in Syria.

3. Section (3), implementing the proposed model and quantitative measurement:

   In this section we introduce a new equation to facilitate the implementation of the proposed model, and produce a security report analyzing the gap between the current situation of TOE (Target of Evaluation) and proposed model, in addition to the practical steps and procedures to narrow this gap.

   And using the equation to measure the security situation of the TOE.

   Then develop a special program to automate the whole process which facilitates the implantation of the model.

   And here we briefly explain the steps we have done:

   - Consider the 18 domains of the five layers:

I	Domain
1	Social Engineering Countermeasures and Policies
2	Awareness and Training Programs
3	Monitoring of Employees and Telecommunications and Unplanned Inspection
4	Intelligent Inspection
5	ISMS (information Security Management System)
6	Risk Assessment
7	Security Policy
8	Organization of Information Security
9	Network Security Administration
10	Asset Security Management
11	Human resources security
12	Physical security

13	Operations Management
14	Access Control
15	Information system acquisition, development and maintenance
16	Information security incident management
17	Business Continuity Management
18	Compliance

- Weighting each directive and control of the proposed model, according to their importance in the current environment.
  We follow below the proposed method:
  6. Each control is assigned a specific weight (integer value).
  7. The summation of each domain controls values will result in the domain value, which is 100 points as maximum.
  8. Each domain can be powered to a positive integer number and/or multiplied by positive integer value; according to its importance.
  9. The final equation will be of the form:

$$L = \frac{1}{m} \sum_{i=1}^{n} \alpha_i \cdot V_i^{\beta_i}$$

Where:

- L : The final level of the organization security, which is an integer value from 1 to 100.
- n : The number of domains.
- V_i : The domain final value, which is the summation of all its control's value, V_i is from 1 to 100.

- α_i : Factors multiplied to each domain final value according to its importance[2].
- β_i : (for future development) The power of V_i according to domain importance, in case the linear α_i values do not reflect the domain importance. β_i could be 1,2,3…
- m : The sum of α_i. In order to have a final value of L out of 100, we need to divide the summation by m. m is related to how we decide to allocate controls –for example 14 domains, each is out of 100-, and the value of β_i and α_i.

Assumptions

For the sake of this paper and to reduce complexity, we will follow the following assumptions:

10. We will consider $\beta_i = 1 \; for \; all \; i.$ β_i Could be for future development.
11. $n = 18$, the number of domains.
12. $m = \sum_{i=1}^{18} \alpha_i$, where α_i is the values of α_i are the average values collected from the survey. The following table shows the average values of α_i and calculation of m.

[2] Some domains are more important than others, and this is related to IT manager perspective, company policies, and services provided. For example some companies need Physical Security much more than Risk Assessment.

I	Domain	α_i
1	Social Engineering Countermeasures and Policies	5
2	Awareness and Training Programs	5
3	Monitoring of Employees and Telecommunications and Unplanned Inspection	4
4	Intelligent Inspection	4
5	ISMS (information Security Management System)	2
6	Risk Assessment	1
7	Security Policy	2
8	Organization of Information Security	2
9	Network Security Administration	5
10	Asset Management	2
11	Human resources security	5
12	Physical and Environmental security	4
13	Operations Management	2
14	Access Control	4
15	Information system acquisition, development and maintenance	3
16	Information security incident management	3
17	Business Continuity Management	2
18	Compliance	3

Here we consider α_i having a value between 1 and 5. Then we got m=58. And the final equation will be:

$$L = \frac{1}{58} \sum_{i=1}^{18} \alpha_i \cdot V_i$$

- The resulted value will be between 1 and 100.

We developed a program using C# .NET and MS SQL 2005 to automate the model controls and domains, and to produce automatically the security report and measure the level of security for the TOE using the proposed equation; and applying the program on a bank operating in Syria, then submitting the results to the bank IT manager, and according to his feedback our model and measuring method has got 87% of the bank expectations.

To be more confident of the overall work done we wrote a research paper titled **"A Novel Approach to Design Quantitative Method for ICT Security Assessment"**, and has been published by Damascus University Referred Journal for Engineering Sciences, No. **ص/20146** dated **2011/7/6**.

4. Section (4), Analyzing the results and future work:
   In this section we analyze the overall research, its implementation, results obtained, and the benefits of the proposed model and equation for Information security in Syria. And then suggest future developments.
5. Section (5), Appendices.
6. Glossary.
7. Table of Figures.
8. References.

الأشكال

الجداول

الفهرس