MEHARI 2010

ماهاري 2010

مقدمة عامة

أفريل 2010

يمكن طرح الاستفسارات و المقترحات على االمنتدى التالي

http://mehari.info/

CLUB DE LA SECURITE DE L'INFORMATION FRANÇAIS

11 rue de Mogador 75009 - Paris

Tél.: +33 153 25 08 80 - Fax: +33 1 53 25 08 88

Web: http://www.clusif.asso.fr

شكر

CLUSIF تود أن تتقدم بشكرها الخاص الى السادة جان فيليب جواس و جان لوي رول
Jean-Philippe Jouas & Jean-Louis Roule
مؤلفي هذه المقدمة العامة حول منهجية ماهاري

كما تود أن تتقدم بشكرها الخاص الى السيد حلمي الرايس Helmi RAIS
من شركة ALLIACOM
اللذي قام بترجمة هذه الوثيقة الى اللغة العربية وفقا لمبادئ نظام المصادر المفتوحة

الرجاء إرسال استفساراتكم و ملاحظاتكم على العناوين التالي
clusif@clusif.asso.fr
helmi.rais@gmail.com

 © CLUSIF 2010

الفهرس

I المقدمة

II استخدام منهجية ماهاري

أ) تحليل/ تقييم المخاطر
أ.1) التحليل المنهجي للحالات التي تنطوي على مخاطر
أ.2) التحليل الآني أو المحدد للحالات التي تنطوي على مخاطر
أ.3) تحليل المخاطر في المشاريع الجديدة
ب) تشخيص حالة السلامة المعلوماتية
ب.1)تشخيص السلامة المعلوماتية عنصر من عناصر تحليل المخاطر
ب.2) المخططات الأمنية المبنية على أساس التشخيص
ب.3) الدعم المقدم من قواعد المعرفة في إنشاء إطار مرجعي للسلامة المعلوماتية
ب.4) المجالات التي تشملها وحدة التشخيص الأمني
ب.5) نظرة عامة لوحدة التشخيص الأمني
ت) تحليل الرهانات
ت.1) تحليل الرهانات الأمنية كأساس لتحليل المخاطر
ت.2) تحليل الرهانات الأمنية : حجر الزاوية في أي تخطيط استراتيجي
ت.3) تصنيف الأصول : عنصر أساسي لسياسة السلامة المعلوماتية
ت.4) تحليل الرهانات الأمنية أساس للتخطيط الأمني
ث) نظرة عامة حول استخدامات منهجية ماهاري

III ماهاري و المعايير الدولية

أ) أهداف معايير الايزو 27001 27002 و 27005 ومنهجية ماهاري
أ.1) أهداف معيار الايزو 27002: 2005
أ.2) أهداف معيار الايزو 27001:2005
أ.3) أهداف معيار الايزو 27005:2008
أ.4) أهداف منهجية ماهاري
أ.5) مقارنة بين أهداف ماهاري و معايير الايزو 27001 و 27002
ب) المطابقة بين مختلف هذه المقاربات
ب.1) المطابقة مع معيار الايزو 27002:2005
ب.2) المطابقة مع معيار الايزو 27001
ب.3) المطابقة مع معيار الايزو 27005

 © CLUSIF 2010

I المقدمة

يتمثل الهدف الرئيسي من تصميم منهجية ماهاري في مساعدة مسؤولي أمن/سلامة الأنظمة المعلوماتية في مهام إدارة أمن/سلامة نظم المعلومات.

وبالإضافة إلى هؤلاء المسؤولين تهم هذه النظرة العامة مدققي السلامة المعلوماتية و مديري المخاطر و مديري النظم المعلوماتية والذين يتقاسمون جميعا نفس محاور الإهتمام .

وتعرض هذه الوثيقة تقديما مختصرا لكيفية استخدام منهجية ماهاري :

-المبادئ الأساسية والمواصفات الفنية لمنهجية ماهاري
-ادلة لتحليل الرهانات وخدمات الأمن/السلامة المعلوماتية و المخاطر المعلوماتية
-دليل مرجعي لخدمات الأمن/السلامة المعلوماتية
- قاعدة المعارف

يعتبر الهدف الرئيسي لمنهجية ماهاري توفير وسيلة لتحليل وإدارة المخاطر المعلوماتية ، و خاصة في مجال سلامة/أمن المعلومات ، بأسلوب يتفق مع متطلبات الايزو 27005:2008 و جميع الأدوات والموارد االمتطلبة لتنفيذها.

وبالاضافة الى ذلك تهدف هذه المنهجية الى :

-تسهيل التحليل المباشر والمشخص للمخاطر عن طريق سيناريوهات المخاطر المعلوماتية

-تقديم مجموعة كاملة من الأدوات لإدارة الأمن/السلامة المعلوماتية على المدى القصير والمتوسط والطويل ، بغض النظر عن نضج إدارة الأمن/السلامة المعلوماتية وبدون اعتبار نوعية الإجراءات والتدابير المتوخاة.

وبالنظر الى هذه الرهانات ، تقترح ماهاري منهجية متناسقة ،باستخدام قواعد معرفية مشخصة وقادرة على مساعدة المسؤولين عن ادارة المؤسسة أو المنظمة ومسؤولي الأمن/السلامة المعلوماتية وكل العناصر الفاعلة في مجال إدارة المخاطر المعلوماتية، في مختلف الخطوات والإجراءات المتوخاة.

وسيتم في نهاية هذه الوثيقة مناقشة علاقة ماهاري بمعايير الايزو 27000

 © CLUSIF 2010

II استخدام منهجية ماهاري

إذن ماهاري هي بالأساس منهجية لتحليل وإدارة المخاطرالمعلوماتية

و بالنظر إلى الهدف الثاني المذكور أعلاه ، تعمل ماهاري وقواعد المعرفة التابعة لها على تسهيل القيام بتحليل دقيق لحالات الخطر ،و التي سيتم وصفها لاحقا في سيناريوهات المخاطرالمعلوماتية

وباعتبار ان إدارة الأمن/السلامة المعلوماتية هي وظيفة أو نشاط يتطور مع مرور الوقت فان الإجراءات المتخذة تختلف وفقا لما انجزته المؤسسة في مجال أمن/سلامة المعلومات

ومما لا شك فيه انه خلال اتخاذ الخطوات الأولى في مجال أمن/سلامة المعلومات من المستحسن إجراء تقييم للوضعية الحالية و لسياسات السلامة المعلوماتية القائمة في الوقت الراهن ومقارنتها بمرجع معين بغرض فهم ما يتبقى فعله

و ينبغي اتخاذ إجراءات ملموسة مباشرة بعد القيام بهذا التقييم إذ يتعين اتخاذ هذه القرارات ، التي تصنف غالبا في مخططات ومراجع المؤسسة ، أوسياسات أمن/ سلامة المعلومات ،من خلال منهجية منظمة ومهيكلة

وقد تستند منهجية كهذه على تحليل للمخاطر المعلوماتية أو على تطبيق لمعايير الايزو 27001 التي تتناول نظم إدارة الأمن/السلامة المعلوماتية أو في بعض الأحيان على معايير ومراجع داخلية أو مهنية

وخلال هذه المرحلة وبدون ذكر عملية تحليل المخاطر ينبغي إيجاد إجابة واضحة لقيمة الأملاك والأصول المعرضة للخطر

"ففي كثير من الأحيان وعند دراسة ميزانية الشركة أو المؤسسة يطرح السؤال الآتي "هل هذا ضروري حقا؟

ولذلك و نظرا لعدم وجود تقييم اولي أو اتفاق عام بشان قيمة الأملاك فان العديد من المشاريع الخاصة بأمن/ سلامة المعلومات يتم تأجيرها أو التخلي عنها بل وفي كثير من الأحيان تجد المؤسسة أن الخطر الحقيقي الذي يواجهها موضع تساؤل

و كثيرا ما تطرح تساؤلات أخرى حول تحديد وحصر جميع المخاطر التي يمكن أن تتعرض لها المؤسسة أو إذا ما تم التأكد من أن هذه المخاطر في مستويات مقبولة

لذلك إذا يتعين وجود منهجية تشمل عملية تحليل المخاطر المعلوماتية

لقد تم تطوير منهجية ماهاري على أسس تكون فيها كل الأدوات المتطلبة في مرحلة معينة من تطوير السلامة المعلوماتية متناسقة و متكاملة وبناء على ذلك فيمكن إعادة استخدام أي نتائج مستخلصة في مرحلة ما عن طريق الوحدات والأدوات التابعة لماهاري ،والتي تم تصميمها لمرافقة عملية تحليل المخاطر، في مراحل لاحقة وبصفة مستقلة ضامنة بذلك فاعلية القرارات المتخذة

كل هذه الأدوات والوحدات والتي يتم تقديمها باختصار اسفله تمثل منهجية لتحليل المخاطر تضم الأدوات

اللازمة لها ،و وحدة لتحليل الأهداف و وحدة لتقييم المخاطر التي تستهدف الأصول المعلوماتية

أ) تحليل/ تقييم المخاطر

لقد ورد ذكر تحليل المخاطر في عديد المؤلفات التي تخص الأمن/السلامة المعلوماتية وخاصة في سلسلة معايير الايزو 27000 باعتبارها التعبير الاساسي لحاجات السلامة المعلوماتية، ولكن معظم . هذه المؤلفات إن لم نقل كلها لم تناقش الاساليب التي يمكن استخدامها لاجراء هذه العملية

منذ أكثر من عشر سنوات تقدم منهجية ماهاري نهجا منظما لتقييم المخاطر استنادا إلى بعض المبادئ البسيطة. وحتى يبقى تركيزنا على ماهو مهم يمكن لنا أن نصف حالة وجود خطر معلوماتي ما بعوامل مختلفة:

. عوامل هيكلية أو تنظيمية لا تعتمد على التدابير التي تخص الأمن/السلامة المعلوماتية ، ولكن النشاط الأساسي للمؤسسة أو المنظمة، وبيئتها وسياقها .

. عوامل تهدف للحد من الخطر المعلوماتي والتي ترتبط بشكل مباشر بتدابير الأمن/السلامة المعلوماتية التي تم تنفيذها.

ويمكن هنا لمنهجية ماهاري المساعدة على تنفيذ تقييم كمي ونوعي لهذه العوامل و بالتالى المساعدة في الحكم على مستويات المخاطر.

ومن اجل ذلك تعتمد ماهاري على أدوات وآليات (معايير تقييم ،طرق حساب ، إلخ.) وقاعدة معرفية ومعلومات (لا سيما بالنسبة لتشخيص حالة الأمن/السلامة المعلوماتية) ضرورية لاستكمال إطار الحد الأدنى الذي تقرحته أيزو 27005.

أ.1) التحليل المنهجي للحالات التي تنطوي على مخاطر

للإجابة على تساؤلات حول ماهية المخاطر التي تواجه المؤسسة أو المنظمة وإذا ما يمكن القبول بها أم لا(أي يمكن التغاضي عنها) يجب اتباع منهجية منظمة تعمل على تحديد جميع المخاطر المحتملة ، ثم تحليل الحالات الأشد خطورة ومن ثم اتخاذ القرار حول الإجراءات التي يجب اتخاذها للحد من هذه المخاطر إلى مستوى مقبول.

ومنهجية ماهاري توفر وتدعم هذا النهج من خلال ماتحتويه من قواعد معارف ومعلومات . وهذا الاستخدام لمنهجية ماهاري يركز على ضمان أن تكون كل حالة من حالات المخاطر الحرجة قدتم تحديدها وتغطيتها بخطة عمل تنفيدية. و يستند هذا النهج إلى قاعدة معارف ومعلومات لحالات الخطر وآليات لتقييم كل خطر معلوماتي وتحديد مستواه وبالإضافة إلى ذلك توفر المنهجية آليات للمساعدة على اتخاذ الإجراءات المناسبة.

ويمكن أن تنفذ عملية تقييم المخاطر:

-إما عن طريق مجموعة من الوظائف التي توفرها قاعدة المعارف (مايكروسوفت اكسل)والتي تمكن من دمج نتائج لمختلف وحدات ماهاري (تصنيف الأصول الناتج عن تحليل الأهداف ،وعملية تشخيص حالة الأمن / السلامة المعلوماتية على وجه الخصوص).و تسمح هذه الوظائف بتقييم مستوى المخاطر الحالي واقتراح تدابير إضافية للحد من خطورة السيناريوهات

-أو عن طريق برمجية كبرمجية RISICARE والتي توفر وظائف متقدمة للمساعدة ، والمحاكاة ...

أ.2) التحليل الآني أو المحدد للحالات التي تنطوي على مخاطر

نفس الادوات التي تم ذكرها سابقا يمكن استخدامها في فترات محددة من طرق اخرى لادارة الامن/السلامة المعلوماتية،تكون فيها ادارة المخاطر ثانوية ويتم الاعتماد فيها مباشرة على مراجع او معايير معينة أو عملية تشخيص لحالة الأمن/السلامة المعلوماتية

خلال هذه الطرق غالبا ما تكون هناك حالات خاصة يصعب فيها تطبيق القواعد المتفق عليها عندها سيكون من المهم القيام بتحليل محدد او آني للمخاطر حتى يتم تقرير ما ينبغي فعله

أ.3) تحليل المخاطر في المشاريع الجديدة
يمكن استخدام نموذج و آليات تحليل المخاطر في إطار إدارة المشاريع حتى يتم تحليل للمخاطر التي تتضمنها المشاريع الجديدة واتخاذ الإجراءات اللازمة للحد منها

ب) تشخيص حالة السلامة المعلوماتية

تشمل المنهجية على استبيانات للتشخيص المتقدم للتدابير المتخذة، واستبيانات لتقييم الحلول والآليات التي وضعت للحد من المخاطر المعلوماتية

ب.1)تشخيص السلامة المعلوماتية عنصر من عناصر تحليل المخاطر
تقدم المنهجية نموذجا منظما للمخاطر يأخذ في الاعتبار "عوامل الحد من المخاطر" في شكل خدمات خاصة بالأمن /السلامة المعلوماتية

وسيكون تقييم الثغرات الأمنية مدخلا هاما لتحليل المخاطر لضمان أن الخدمات الخاصة بالأمن / السلامة المعلوماتية تؤدي دورها على أكمل وجه وهو ما يمثل نقطة جوهرية بالنسبة لمصداقية عملية تحليل المخاطر

أحدى الركائز الأساسية للمنهجية تتمثل في قدرتها على تقييم المستوى الحالي للخطر فضلا عن مستواه في المستقبل على أساس قاعدة تشخيص مختص بتقييم مستوى جودة أو فاعلية التدابير الأمنية المقررة أو المتخذة

ب.2) المخططات الأمنية المبنية على أساس التشخيص
إحدى الطرق الممكن استعمالها تتمثل في بناء خطط العمل مباشرة اثر تشخيص حالة السلامة المعلوماتية

و تعتبر عملية إدارة السلامة المعلوماتية بالاعتماد على التشخيص بسيطة للغاية لأنها تعني أن نقوم بعملية تشخيص أمني ثم بتحسين كل الخدمات التي ليس لديها ما يكفي من مستوى الجودة بناءا على نتيجة التشخيص ويمكن استخدام الاستبيانات الخاصة بمنهجية ماهاري لهدا الغرض

و يستحسن هنا استخدام تحليل أولي للرهانات وهو ما سيتم تقديمه لاحقا في هذه الوثيقة وسيتيح هذا التحليل تحديد رهانات الجودة الخاصة بالخدمات الأمنية ، أو الاقتصار على اختيار الخدمات التي سيتم التدقيق فيها في إطار عملية التشخيص

ب.3) الدعم المقدم من قواعد المعرفة في إنشاء إطار مرجعي للسلامة المعلوماتية
تقوم وحدة التشخيص على قاعدة معارف لخدمات السلامة/الأمن المعلوماتي (وتسمى الدليل المرجعي للخدمات الأمنية) ، والتي تصف لكل خدمة:

- الغرض منها

-رهانات استخدامها

-آليات وحلول دعم الخدمة

-العناصر التي ينبغي أن تأخذ في الاعتبار عند تقييم جودة الخدمة

ويمكن لقاعدة المعرفة هذه ،التي هي بدون شك فريدة من نوعها ، أن تطبق مباشرة لإيجاد دليل مرجعي للسلامة/الأمن و الذي سيتضمن وصفا لجميع قواعد وتعليمات السلامة/الأمن التي يتعين استخدامها من طرف المنظمة أو المؤسسة

وعادة ما تستخدم هذه الطريقة في المنظمات أو المؤسسات التي لها عدد من الوحدات التنفيذية المستقلة أو المواقع المنفصلة كالشركات المتعددة الجنسيات والتي يكون لها عدد من الشركات التابعة لها أو أيضا بعض الشركات الصغيرة أو متوسطة الحجم والتي يكون لها عدد من الفروع و الوكالات الجهوية

و في مثل هده الحالات يصعب القيام بالعديد من عمليات تحليل أو تقييم المخاطر

بناء الإطار المرجعي للأمن/السلامة المعلوماتية

تمثل استبيانات التشخيص ، و خاصة الدليل المرجعي للخدمات الأمنية وما يحتويه من توضيحات إضافية، أساسا جيدا لمساعدة مسؤولي الأمن/السلامة المعلوماتية في تقرير ما ينبغي تطبيقه في المؤسسة أو المنظمة

إدارة الاستثناءات من القواعد

غالبا ما يواجه إنشاء مجموعة من القواعد صعوبات في تطبيقه نظرا لبعض الخصائص العملية و لذلك يجب معرفة كيفية إدارة استثناءات عدم تطبيق القواعد

و يمكن القول أنه باستخدام قاعدة معارف متماسكة و متناسقة بالإضافة إلى مجموعة من الأدوات ومنهجية تحليل للمخاطر يمكن لنا إدارة الصعوبات المحلية بالتعامل مع مطالب الاستثناء من القواعد من خلال تحليل محدد للمخاطر يركز على المشاكل التي سلط عليها الضوء

ب.4) المجالات التي تشملها وحدة التشخيص الأمني
من منظور تحليل المخاطر ، بمعنى تحديد جميع حالات الخطر والاستعداد للتصدي لجميع المخاطر غير المقبولة ، لا تقتصر منهجية ماهاري على النظم المعلوماتية

فاستبيانات التشخيص تشمل ، بالإضافة إلى نظم المعلومات والاتصالات التنظيم العام للأمن/السلامة المعلوماتية والحماية الشاملة لمواقع العمل ، وبيئة عمل مستخدمي النظام المعلوماتي بالإضافة إلى الجوانب التنظيمية والقانونية

ب.5) نظرة عامة لوحدة التشخيص الأمني
تقدم استبيانات التشخيص الأمني رؤية شاملة و متناسقة حول الأمن/السلامة المعلوماتية وهذا ما لابد له أن يؤخذ بعين الاعتبار

ويمكن استخدام ذلك في مجموعة مختلفة من الطرق وبصفة متطورة في عمق ومستوى التحليل وذلك في جميع مراحل نضج الوعي بالأمن/السلامة المعلوماتية للمؤسسة أو المنظمة

ت) تحليل الرهانات

أيا كانت توجهات سياسات السلامة المعلوماتية فهناك مبدأ يتفق عليه جميع المسؤولين و أصحاب القرار وهو أن يكون هناك توازن عادل بين قيمة الاستثمار في مجال السلامة المعلوماتية من ناحية و قيمة المخاطر نفسها من ناحية أخرى وهذا يعني أن الفهم الصحيح للمصالح المعرضة للخطر أمر أساسي

وهذا ما يجرنا للقول أن المعرفة الدقيقة لرهانات السلامة أمر أساسي وأن تقييم هذه الرهانات يستحق أولوية عليا و منهجية تقييم منظمة

يمثل الهدف الأساسي من تحليل الرهانات الإجابة على هذين السؤالين : ماذا علينا أن نخشى حدوثه ، وإذا حدث ذلك ، فهل سيكون ذلك أمرا خطيرا؟

وهذا يعني ، في مجال السلامة المعلوماتية أن ننظر إلى المخاطر باعتبارها النتائج المترتبة على الأحداث التي تؤثر على سير العمل المرجو للمؤسسة أو المنظمة

توفر منهجية ماهاري وحدة لتقييم الرهانات في "دليل تقييم الرهانات و تصنيف الأصول" والتي تعطينا نوعين

من النتائج

- معايير لتقييم الخلل الوظيفي

-تصنيف للمعلومات والأصول المعلوماتية

معيار تقييم الخلل الوظيفي

تمارس عملية معرفة وتحديد الخلل الوظيفي أو الأحداث التي يخشى حدوثها انطلاقا من أنشطة المنظمة أو المؤسسة. وتؤدي هذه العملية إلى:

-وصف لأنواع الأعطال المحتملة

-وضع تعريف للمعايير التي تؤثر على خطورة كل خلل وظيفي

-إجراء تقييم لحساسية هذه المعايير والتي تؤثر على مدى خطورة هذه الأعطال

تصنيف المعلومات والأصول المعلوماتية

جرت العادة في مجال سلامة/أمن المعلومات أن نتحدث عن تصنيف المعلومات وتصنيف الأصول التابعة للنظام المعلوماتي

ويحدد هذا التصنيف لكل نوع من المعلومات والأصول المعلوماتية ، ولكل معيار التصنيف المعتمدة (وهي بالأساس: توفر الخدمة والسرية و السلامة أو بعض المعايير أخرى مثل آثار التتبع) ، مؤشرات تمثل حساسية المعيار المتأثر و تحدد احتمالية فقدان هذه المعلومات أو الأصول

و يمثل تصنيف المعلومات والأصول ، بالنسبة للنظم المعلوماتية ، ترجمة لقيمة الخلل الوظيفي إلى مؤشرات حساسية أو خطورة مرتبطة بالأصول المعلوماتية

التعبير عن الرهانات الأمنية

تمثلي عمليتي تقييم الخلل الوظيفي وتصنيف المعلومات والأصول المعلوماتية طريقتان مختلفتان للتعبير عن الرهانات الأمنية

فالطريقة الأولى هي الأكثر تفضيلا بين مديري الأمن/السلامة المعلوماتية و أكثرها توفيرا للمعلومات بينما تمثل الطريقة الثانية الطريقة الأكثر شمولية و الأكثر تأثيرا في حملات التوعية و الاتصال ولكنها الأقل دقة

ت.1) تحليل الرهانات الأمنية كأساس لتحليل المخاطر

من الواضح أن هذا المبدأ أساسي في عملية تحليل المخاطر. فبدون تعريف مشترك حول النتائج المترتبة عن الأعطال الوظيفية لا يمكننا إصدار حكم قاطع حول حساسية و مستوى المخاطر

وتقدم ماهاري هنا طريقة صارمة لتقييم الرهانات وتصنيف الأصول تؤدي إلى نتائج موضوعية وعقلانية

ت.2) تحليل الرهانات الأمنية : حجر الزاوية في أي تخطيط استراتيجي

من البديهي أن يكون تحليل الرهانات الأمنية أساسيا لتنفيذ أي شكل من أشكال برامج و خطط الأمن/السلامة المعلوماتية

عمليا ، و أيا كان النهج المستخدم ، في مرحلة ما ، سيتم تخصيص استثمارات و آليات لتنفيذ خطط العمل هذه ، وحتما فإن كل مبررات هذه الاستثمارات ستكون محل تساؤل و تشكيك

فالآليات و الاستثمارات التي سيتم تخصيصها لبرامج السلامة المعلوماتية ، حالها كحال تلك التي تخصص للتأمين كليهما له علاقة مباشرة بمستوى و حساسية الخطر

فإذا لم يكن هناك تفاهم مشترك حول الأعطال الوظيفية التي يخشى وقوعها فمن المستبعد جدا أن يتم تخصيص الاستثمارات لهذا الغرض

ت.3) تصنيف الأصول : عنصر أساسي لسياسة السلامة المعلوماتية
لقد تم التطرق خلال هذه الوثيقة إلى الإطار المرجعي للأمن/السلامة المعلوماتية و التعريف بالسياسات الأمنية و ما يرتبط بهما من طرق لإدارة الأمن/السلامة المعلوماتية

عمليا ، يتعين على المؤسسات التي تدير برامجها الأمنية عن طريق مجموعة من القواعد، التمييز بين الإجراءات التي يتعين القيام بها حسب حساسية المعلومات التي يتم معالجتها. وقد جرت العادة أن تتم الإشارة إلى تصنيف المعلومات أو الأصول المعلوماتية التي تتم معالجتها

و في هذا المجال توفر وحدة تحليل الرهانات التابعة لمنهجية ماهاري آليات للقيام بتصنيف الأصول المعلوماتية

ت.4) تحليل الرهانات الأمنية أساس للتخطيط الأمني
كثيرا ما تؤدي عملية تحليل الرهانات الأمنية، والتي تطلب مساهمة الإدارة التنفيذية، إلى ضرورة اتخاذ إجراءات فورية

وقد علمتنا التجربة أنه عند مقابلة مسؤولين سامين في الإدارة التنفيذية ، بغض النظر عن حجم المؤسسة ، ويتم الاستماع إلى وجهة نظرهم حول حساسية الأعطال التنفيذية فسيتم اكتشاف احتياجات أمنية لم تؤخذ بعين الاعتبار في السابق تتطلب إجابات سريعة

و مباشرة اثر هذا يمكن أنشاء خطط العمل باستخدام طريقة سريعة ومباشرة تقوم على مجموعتين من الخبرات : مهنة المنظمة أو المنظمة في حد ذاتها و التي تم تقديمها من طرف الإدارة التنفيذية ، و حلول أو تدابير السلامة المعلوماتية التي تم تقديمها من طرف خبراء الأمن/السلامة المعلوماتية

ث) نظرة عامة حول استخدامات منهجية ماهاري

من الواضح أن الهدف الرئيسي لمنهجية ماهاري هو تقييم المخاطر والحد منها. ولقد تم إنشاء قاعدة المعارف والآليات والأدوات المتعلقة بها لتحقيق هذا الغرض

وبالتوازي مع ذلك فلقد اتضح في أذهان مصممي المنهجية أن الحاجة إلى منهج منظم لتحليل : المخاطر والحد منها يمكن أن يكون حسب طبيعة المنظمة:

-اما طريقة عمل دائمة ، مهيكلة و رئيسية

-اما طريقة عمل دائمة تستخدم بالتوازي مع طرق أخرى لادارة برامج الأمن/السلامة المعلوماتية

-إما طريقة عمل تستخدم من حين لآخر لاستكمال ممارسات إدارية أخرى

وفي هذا السياق فان ماهاري تقدم لنا مجموعة من المفاهيم والأدوات المستخدمة في تحليل المخاطر عند الضرورة

وتعمل ماهاري على مساعدة مسؤولي السلامة المعلوماتية والمدققين و مسؤولي النظم المعلوماتية ...الخ عن طريق مجموعة من الوثائق و الأدلة بالإضافة إلى قواعدها المعرفية

III ماهاري و المعايير الدولية

كثيرا ما تثار أسئلة حول كيفية تطابق منهجية ماهاري مع المعايير الدولية و خاصة منها سلسلة معايير الايزو 27000

وهنا لن نقوم بالمقارنة المباشرة بين منهجية ماهاري و تلك المعايير و الأدوات المعروفة في يومنا هذا ، فالهدف من هذه الوثيقة هو بالأحرى شرح كيفية تطابق منهجية ماهاري مع معايير الايزو من حيث توافق الأهداف ، وخاصة منها معايير الايزو 27002،27001 و 27005

أ) أهداف معايير الايزو 27001 27002 و 27005 ومنهجية ماهاري

أ.1) أهداف معيار الايزو 27002: 2005
ينص هذا المعيار على أن المنظمة أو المؤسسة ينبغي أن تحدد متطلباتها الأمنية باستخدام ثلاثة مصادر أساسية و هي:

-تحليل المخاطر

-المتطلبات القانونية و التشريعية و التنظيمية أو الشروط التعاقدية

- مجموعة من المبادئ والأهداف والمتطلبات لمعالجة المعلومات الموضوعة من طرف المؤسسة أو المنظمة لدعم عملياتها

وانطلاقا من ذلك ، يمكن تحديد واختيار نقاط المراقبة والتحكم وفقا للقائمة الواردة في "مدونة الممارسات لإدارة أمن/سلامة المعلومات" من المعيار أو من خلال أي مجموعة أخرى من نقاط المراقبة و التحكم : الايزو 27002:2005 27001:2005 و 27005:2008

ملاحظة: نص معيار 27002:2005 على المبادئ التوجيهية والمبادئ العامة للبدء في تنفيذ و صيانة وتطوير إدارة أمن/سلامة المعلومات الأمر الذي يعني أن معيار الايزو يمكن النظر إليه على أنه نقطة الانطلاق

غير أن معيار ايزو 27002 ينص في المادة 1.2 على أنه يتوجب أن يكون أي استثناء مبررا و مقبولا. انظر ملحق المعيار أ و أ.1

من جهة أخرى يقدم معيار ايزو 27002:2005 مجموعة من المبادئ التوجيهية التي يمكن للمنظمة أو المؤسسة استخدامها. غير أن مجموعة هذه المبادئ ليست شاملة ولذلك يتوجب اللجوء إلى بعض التدابير التكميلية

و مع ذلك فان المعيار لا يوصي باستخدام منهجية معينة لوضع نظام كامل لإدارة الأمن/السلامة المعلوماتية على أن كل جزئ من المعيار يظم مقدمات و تعليقات حول طبيعة الأهداف المنشودة

ملاحظة: ينص معيار الايزو على إمكانية استخدامه للمساعدة على بناء الثقة في الأنشطة المشتركة بين المنظمات وهو ما يبرز جانبا أساسيا يروج له مؤيدو المعيار و هو جانب التقييم الأمني أو المصادقة بين الشركات المتحالفة و الموردين من ناحية جودة الأمن / السلامة المعلوماتية

أ.2) أهداف معيار الايزو 27001:2005
الهدف الأساسي لهذا المعيار هو إنشاء و تطوير نظام إدارة الأمن/السلامة المعلوماتية للمنظمة أو المؤسسة والتي يمكن استخدامها في إطار داخلي أو عن طريق أطراف ثالثة بما في ذلك هيئات المصادقة

هدف التقييم و المصادقة هذا يركز بالأساس على الجوانب الرسمية والإدارية (تسجيل و توثيق القرارات ، إعلان قابلية المطابقة ، السجلات الخ) والجوانب الخاصة بالمراقبة (تقارير عمليات التدقيق ، مراجعات ، الخ) .وعلى هذا النحو فإننا أمام منهجية لضمان الجودة

على أن لب منهجية الأمن/السلامة المعلوماتية التي تم تقديمها ينطوي على تحليل للأهداف و تحليل للمخاطر التي تواجهها المنظمة أو المؤسسة واختيار التدابير المناسبة للحد من تلك المخاطر أو تقليصها إلى مستوى مقبول

يشير الايزو 27001 إلى أنه يجب استخدام منهجية لتحليل المخاطر ضمن نموذج عملية تخطيط وتكريس ، ومراقبة ، وتحسين نظام إدارة الأمن/السلامة المعلوماتية.

PDCA (PLAN، DO، CHECK، ACT)

علاوة على ذلك ،فان التوصيات أو "أفضل الممارسات" التي يمكن اختيارها للحد من المخاطر متماشية مع تلك المدرجة في / ايزو 27002:2005 ويضم ملحق المعيار وصفا كاملا لقائمة نقاط المراقبة التابعة لها

ولا يمثل أساس تقييم نظام إدارة الأمن/السلامة المعلوماتية ،حسب الايزو 27001 ، معرفة أو التحقق مما إذا كانت القرارات المتخذة صائبة أو موافقة لاحتياجات المؤسسة وإنما التأكد من أنه بمجرد اتخاذ هذه القرارات يكون لدينا بعض الضمانات أنه سيتم تطبيقها

أ.3) أهداف معيار الايزو 27005:2008

لا تمثل أهداف هذا المعيار إنشاء طريقة كاملة لإدارة المخاطر ولكن وضع إطار أدنى ، وفرض المتطلبات الأساسية للعملية التي يجب اتباعها بصفة عامة من ناحية و لعملية تحديد الثغرات ومواطن الضعف من ناحية أخرى حتى نتمكن من تقييم المخاطر وبالتالي تحديد التدابير الأمنية المتعلقة بها

هذا يعني أننا لسنا أمام منهجية متكاملة ومستقلة بذاتها و لكن أمام إطار لضمان عدم اختيار منهجيات بسيطة أو معقدة للغاية بعيدا عن مفهوم إدارة المخاطر،فالمعيار ينص فقط على وجوب اختيار منهجية ما لتحليل المخاطر

أ.4) أهداف منهجية ماهاري

تمثل منهجية ماهاري مجموعة متكاملة و متناسقة ومستقلة بذاتها من الأدوات و أساليب إدارة الأمن/السلامة المعلوماتية، والتي تم إنشاؤها على تحليل دقيق للمخاطر

وتمثل الجوانب الأساسية لماهاري مكملات ضرورية لسلسة معايير الايزو 27000 وخاصة معيار ايزو 27005 وهذه الجوانب هي: م

- نموذج المخاطر النوعية والكمية

- دراسة فاعلية التدابير الأمنية المتخذة أو المقررة

- القدرة على تقييم ومحاكاة المخاطر المتبقية لتقييم فاعلية التدابير الإضافية

أ.5) مقارنة بين أهداف ماهاري و معايير الايزو 27001 و 27002

تختلف الأهداف الأولية لمنهجية ماهاري و معايير الايزو المذكورة أعلاه

إذ تهدف منهجية ماهاري إلى توفير الأساليب و الأدوات التي يمكن استخدامها لاختيار أنسب التدابير فنيا و اقتصاديا لمؤسسة أو منظمة ما والى تقييم المخاطر المتبقية بعد تطبيق هذه التدابير ، وهو ما لا يمثل على الإطلاق وجهة نظر معايير الايزو

من ناحية أخرى يقدم معياري الايزو المذكورين أعلاه مجموعة من أفضل الممارسات التي لانشك في فائدتها ولكنها ليست دائما ملائمة لرهانات المؤسسة أو المنظمة، هذا بالإضافة إلى وسيلة لتقييم مستوى نضج الأمن/السلامة المعلوماتية بالنسبة إلى الوحدات الداخلية للمؤسسة أو الشركاء المتعاملين معها

و تضم منهجية ماهاري دليلا مرجعيا لخدمات السلامة المعلوماتية يمكن مقارنتها بما ورد في معيار الايزو 27002 . ويمكن القول في هذا الخصوص أن الخدمات التي تغطيها ماهاري أكثر شمولية من تلك التي وردت

في معيار الايزو حيث تضم مهاري كل الجوانب الأساسية المتعلقة بالأمن/السلامة المعلوماتية

ب) المطابقة بين مختلف هذه المقاربات

في الواقع تتفق منهجية ماهاري تماما مع الايزو 27002 إذ يمكن استخدام النتائج المتحصل عليها عن طريق ماهاري كمؤشرات لمدى توافق المنظمة أو المؤسسة مع أهداف معيار الايزو 27002 رغم أن هتين المقاربتين لا تسعيان لتحقيق نفس الأهداف

بالإضافة إلى ذلك فان ماهاري تستجيب لمتطلبات معايير الايزو والتي تنص على وجوب استعمال منهجية معينة لتحليل المخاطر وتحديد التدابير التي ينبغي تنفيذها

ب.1) المطابقة مع معيار الايزو 27002:2005

نقاط المراقبة المتوفرة في معيار الايزو هي نقاط عامة في شكل تدابير تنظيمية أو سلوكية في حين أن ماهاري تشدد على الحاجة إلى فاعلية التدابير التقنية حتى تكون مضمونة النتائج في تقليص الثغرات المعلوماتية

وبالرغم من هذه الاختلافات فان ماهاري توفر لنا جداول التناظر والتي تهدف إلى عرض مؤشرات متناسقة و متوافقة مع تلك المستخدمة في الايزو 27002 ، يمكن استخدامها من طرف من له متطلبات خاصة لإثبات امتثاله لذلك المعيار

والجدير بالذكر هنا أن استبيانات التدقيق التابعة لماهاري قد تمم تصميمها و تقسيمها من أجل إجراء تقييم فعال للثغرات عند استبيان المسؤولين التنفيذين المعنيين و بالتالي استنتاج مدى قدرة كل خدمة من خدمات السلامة المعلوماتية على الحد من هذه المخاطر

ب.2) المطابقة مع معيار الايزو 27001

من السهل إدماج ماهاري ضمن عملية تخطيط وتكريس ، ومراقبة ، وتطوير نظام إدارة الأمن/السلامة المعلوماتية
PDCA (PLAN، DO، CHECK، ACT)

ولاسيما ضمن مرحلة التخطيط والتي تقوم ماهاري بوصف كامل للمهام التي تمكن من إرساء نظام إدارة الأمن/السلامة المعلوماتية

أما في مرحلة التكريس والتي تهدف إلى إنشاء نظام إدارة الأمن/السلامة المعلوماتية توفر ماهاري عناصر أولية كخطط إدارة المخاطر مع تحديد الأولويات المرتبطة مباشرة بتصنيف المخاطر ومؤشرات التطور أثناء تنفيذها

خلال مرحلة المراقبة توفر ماهاري مجموعة من الوسائل التي تساعد على تحديد المخاطر المتبقية انطلاقا ،من عملية تقييم أو تدقيق خدمات السلامة المعلوماتية والتحسينات التي أدخلتها التدابير الأمنية

وبالإضافة إلى ذلك ،فسيكون من السهل إعادة التقييم مباشرة اثر أي تغيير يحدث في بيئة المنظمة أو المؤسسة (من حيث الرهانات و المخاطر والحلول والتنظيم) وذلك عن طريق عمليات تدقيق خاصة تعتمد على نتائج التدقيق الأولي والذي جرى باستعمال ماهاري

وهكذا إذن، يمكن مراجعة خطط الأمن/السلامة المعلوماتية وتطويرها مع مرور الوقت

أخيرا و خلال مرحلة التحسين أو التطوير فان المنهجية تدعو ضمنيا إلى المراقبة و التطوير المستمر مما يكفل تحقيق الأهداف المنشودة في عملية الحد من المخاطر

خلال المراحل الثلاث المذكورة سابقا ، ورغم أن ماهاري ليست في صميم العمليات ، فإنها تساهم إلى حد كبير في تنفيذها و ضمان فاعليتها

ب.3) المطابقة مع معيار الايزو 27005

ينطبق الإطار الذي وضعه هذا المعيار الجديد تماما على طريقة التي تمكن بها ماهاري من إدارة المخاطر ، على سبيل المثال

-عمليات تحليل المخاطر وتقييمها ومعالجتها ، والمستوحاة من الايزو 13335

-تحديد الأصول الرئيسية و الثانوية بالإضافة إلى مستويات التصنيف المتعلقة بها ، اثر عملية تحليل الرهانات

تحديد التهديدات المعلوماتية و المستوى التابع لها، والتي يوفر ماهاري أكثر دقة لها في وصف سيناريوهات المخاطر

- تقييم فاعلية التدابير الأمنية المتخذة في الحد من نقاط الضعف

- الجمع بين كل هذه العناصر لتقييم مستوى خطورة سيناريوهات المخاطر ، في سلم من أربعة مستويات

-القدرة على انتقاء التدابير التي يجب إدراجها في برامج أو خطط الحد من المخاطر

لذلك، فان منهجية ماهاري ليست فقط سهلة الإدماج في عملية تخطيط وتكريس ، ومراقبة ، وتطوير نظام إدارة الأمن/السلامة المعلوماتية بالطريقة التي تنص عليها الايزو 27001 ولكنها تتطابق تماما مع متطلبات الايزو 27005 في اختيار منهجية لإدارة المخاطر