



جامعة السودان للعلوم والتكنولوجيا
كلية علوم الحاسوب وتقانة المعلومات

إطار عمل مبسط لإدارة نظم أمن المعلومات

دراسة حالة : شركة أمونيا للبترول

A simple ISMS Framework

A case study AMONIA Petroleum

أكتوبر / 2010

مشروع مقدم كأحد متطلبات الحصول على درجة
الماجستير في علوم الحاسوب.

بسم الله الرحمن الرحيم
جامعة السودان للعلوم والتكنولوجيا
كلية علوم الحاسوب وتقانة المعلومات

إطار عمل مبسط لإدارة نظم أمن المعلومات

دراسة حالة : شركة أمونيا للبترول

A simple ISMS Framework

A case study AMONIA Petroleum

أكتوبر/2010

إعداد الطالب:

اليسع محجوب طيفور علي

مشروع مقدم كأحد متطلبات الحصول على درجة
الماجستير في علوم الحاسوب.

توقيع الدكتور المشرف
التاريخ

/

د. عوض محمد عوض الكريم
2010/

الحمد لله

الحمد لله الذي جعل حقيقة الإيمان في العلم قال تعالى:

(لَكِنَّ الرَّاسِخُونَ فِي الْعِلْمِ مِنْهُمْ وَالْمُؤْمِنُونَ يُؤْمِنُونَ بِمَا أُنزِلَ إِلَيْكَ وَمَا أُنزِلَ مِنْ قَبْلِكَ وَالْمُقِيمِينَ الصَّلَاةَ وَالْمُؤْتُونَ الزَّكَاةَ وَالْمُؤْمِنُونَ بِاللَّهِ وَالْيَوْمِ الْآخِرِ أُولَئِكَ سَنُؤْتِيهِمْ أَجْرًا عَظِيمًا) [النساء : 162]

والحمد لله الذي ربط علي قلوب العلماء من خشيته فجعل العلم نورا وهداية
قال تعالى:

وَيَرَى الَّذِينَ أُوتُوا الْعِلْمَ الَّذِي أُنزِلَ إِلَيْكَ مِنْ رَبِّكَ هُوَ الْحَقُّ وَيَهْدِي إِلَى صِرَاطِ الْعَزِيزِ الْحَمِيدِ [سبأ : 6]

والحمد لله الذي أمدنا بوسائل العلم وسخرها لنا عوناً علي مقتضيات الحياة ،
وجعل لنا العلم وأدواته معيناً علي طاعته وعبادته وعلي ما ينفع الناس به .

وله الحمد من قبل ومن بعد

الإهداء

إلى الذين ساروا معي في الأشواك ، فدميت ودموا ... وشقيتُ وشقوا معي ...

وعجزت فقوموا و قوموني ، كانوا لي خير معين ...

أكملت معهم وبهم الطريق ... فكانوا خير دليل وأشرق نور

أمي .. أبي .. وأخواني

شكر و عرفان

الحمد لله الذي أعانني علي أكمال هذا البحث وسخر لي من عبادته الصالحين من تعجز كلماتي عن شكرهم..

فالشكر أجزله للأستاذة الكرام بجامعة السودان، كلية علوم الحاسوب وتقانة المعلومات اللذين أناروا لنا طريق العلم وعلّمونا كيف نتعلم ونعلم..

والشكر أجزله لأستاذي الدكتور عوض محمد عوض الكريم الذي كان المشرف القدير على نجاح هذا البحث والذي حلم عن جهلي بعلمه.

والأخوه زملاء الدفعة الثالثة ماجستير علوم الحاسوب جامعة السودان اللذين سبقت دعواتهم لي بالتوفيق أفكارهم.. وساقتني أفكارهم للتوفيق..

ولالأخ المهندس أشرف محمد عبدالحليم من شركة (MTN) قسم أمن المعلومات والشبكات والشكر الخاص إلي أسرة شركة أمونيا للبتترول التي فتحت لي قلبها ثم بابها..

ولأهلي وأصدقائي..

أسأل الله أن يعينني على مكافأتهم بأحسن مما قدموا لي وجزاهم الله عني كل

خ — ❖

مدخل

قال الله -عز وجل- في كتابه الكريم: (يَا أَيُّهَا الَّذِينَ آمَنُوا لَا تَدْخُلُوا بُيُوتًا غَيْرَ بُيُوتِكُمْ حَتَّى تَسْتَأْنِسُوا وَتُسَلِّمُوا عَلَى أَهْلِهَا ذَلِكَ هِيَ لَكُمْ لَعْنَةٌ تَذَكَّرُونَ) [النور : 27].

و قال سبحانه : (وَلَا تَجَسَّسُوا وَلَا يَغْتَبَ بَعْضُكُم بَعْضًا) [الحجرات : 12].

قال الرسول - صلي الله عليه وسلم - : "من إطلع في بيت قومٍ بغير إذنهـم فقد حل لهم أن يـفـقـأوا عينهـ، فإن فـقـأوا عينه فلا دية له ولا قصاص".

و قال - صلى الله عليه وسلم -: " من تسمع حديث قوم وهم له كارهون، صب في أذنيه الأتـك".

شرع الدين الإسلامي خصوصية الفرد قبل أكثر من أربعة عشر قرناً. ووصى الفرد المسلم بحفظ عورة أخيه المسلم إن تمكن منها. ورتب سبحانه العقوبات في الحياة الدنيا والوعيد الشديد في الآخرة، لردع كل مخالف لأوامره. وفي المقابل جعل الله -عز وجل- المحافظة على خصوصية الفرد من صفات المؤمنين، الذين صدقوا الله ورسوله وعملوا بشرعته..

المستخلص

تقع المسؤولية في المحافظه علي بيانات ومعلومات أي مؤسسة علي عاتق نظم إدارة أمن وسرية المعلومات، وفاعلية هذه النظم تعتمد علي السياسات والإجراءات الفاعلة والواضحة والمصوغة صياغة جيدة. لكن التعقيد الذي يصاحب إنشاء وتنفيذ سياسات إدارة أمن المعلومات -النابع أصلا من التعقيد الموجود في المستندات المعيارية المرجع الوحيد لإنشاء هذه سياسات- هذا التعقيد يحد من إنتشار هذه السياسات بين المؤسسات خاصة المتوسطة منها والصغيرة.

تقدم هذه الدراسة للشركات المتوسطة والصغيرة م قترح إطار عمل مبسط لإدارة أمن وسرية معلوماتها بطريقه سهله وفاعلة ، وكحالة دراسة تم تطبيق الإطار الم قترح لإثبات كفاءته وفاعليته علي شركة أمونيا للبتروول كمثال لواحد من هذه الشركات .

ABSTRACT

The purpose of an Information Security management System (ISMS) is to protect the valuable information resources of an enterprise. In addition, it is necessary to ensure that appropriate, effective, well-written policies, standards, and procedures are premeditated as well as correctly implemented. Although, the related standard documents are considered as the primary and distinctive references in order to establish such systems. The struggle and complexity that face an enterprise is originally derived from density and complication of such standards. This study proposes simple and effective framework to establish ISMS especially for medium and small enterprises. As case study, the proposed framework is applied to AMONIA Petroleum Company, which ensured the feasibility and inclusiveness.

فهرس المحتويات

الصفحة	الموضوع	الباب
1.....مقدمة		1. الباب الأول

2..... م مقدمة .1.1

3..... مشكلة البحث .1.2

أهداف البحث .1.3

.....

3..

أهمية هذا البحث .1.4

.....

.....

3.....

حدود البحث .1.5

.....

.....

3.....

1.6. تنظيم البحث

.....

.....

4....

2. الباب الثاني الخلفية النظرية للبحث5
- 2.1 أمن المعلومات ماهيته وعناصره وإستراتيجياته6

2.1.1 تعريف أمن المعلومات

.....

6..

- 2.1.2 عناصر أمن المعلومات6
- 2.1.3 السياسات الأمنية للمعلومات7
- 2.1.4 مستويات تقديم الحماية8
- 2.1.5 مواضع المخاطر والإعتداءات في بيئة المعلومات10

2.1.6 العمليات الرئيسية المتصلة بأمن المعلومات

.....

10.....

- 2.1.6.1 تصنيف المعلومات10
- 2.1.6.2 التوثيق10
- 2.1.6.3 المهام والواجبات الإدارية والشخصية11
- 2.1.6.4 وسائل التعريف والتوثق11
- 2.1.6.5 سجل الأداء12
- 2.1.6.6 عمليات الحفظ الإحتياطي12
- 2.1.6.7 وسائل الأمن الفنية ونظام منع الإختراق12

2.1.6.8. نظام التعامل مع الحوادث 13

2.1.7.

أساسيات أمن

المعلومات

.....

13

2.1.8.

أمن

المنظمة

.....

14

2.1.9. المتطلبات الأمنية

الخاصة

بالموظفين

.....

14

2.1.10

كيفية تحقيق بيئة أمن

..... مناسبة

15

2.1.11

أساسيات أمن الأجهزة والشبكات

.....

15

2.1.12

**تحقيق أمن فعلي
للأنظمة في المنظمة**

.....

16

2.1.13

معلومات أمن

..... المعلومات

.....

16 ■

2.1.14. نقاط تساعد في إقناع

المسؤولين في المؤسسة بأهمية تنفيذ سياسة أمن

المعلومات.....

.....

.....

18

- 2.2 سياسات أمن المعلومات 19
- 2.2.1 تعريف سياسة الأمن 19
- 2.2.2 الحاجة إلي السياسة الأمنية 20
- 2.2.3 تحضيرات ما قبل البدء بسياسات الأمن 20
- 3. الباب الثالث المعايير القياسية 23

3.1. الم مقدمة 24.

3.2 معايير الأيزو

.....

.....

24.....

3.2.1 عائلة المواصفات القياسية العالمية) ISO/IEC 27000- :

series) 25
شهادة الأيزو 26 3.2.2

3.2.3 نشأة وتطور عائلة المواصفات القياسية العالمية ISO 27000

..... 26
ISO/IEC 27002 26 تطور 3.2.3.1
ISO/IEC 27001 27 تطور 3.2.3.2

3.2.4 لمحة سريعة عن المواصفات القياسية للعائلة ISO

27000:2009 27
ISO/IEC 27001) 27 نبذة عن 3.2.4.1
ISO 27002: ISO/IEC 17799:2005)..... 28 نبذة عن 3.2.4.2
30..... 3.2.5 معايير الأيزو الأخرى

3.3 معيار الكوبيت (30) COBIT)

3.4 معيار

ITIL
.....31

3.5 اللوائح والقوانين المتعلقة بأمن المعلومات
32.....

3.5.1 قانون 32 SOX

3.5.2 قانون 32 COSO

3.5.3 قانون 33 HIPAA

3.5.4 قانون 33 FISMA

3.5.5 قانون FIPS
.....34

4. الباب الرابع الإطار المقترح 36

4.1 إطار عمل فعال لإدارة نظم أمن المعلومات 37

4.2 المرحلة الأولى 38

4.2.1 تحديد حدود ومجال سياسات ال ISMS المطلوبة 38

4.2.2 تجميع المعلومات عن المنظمة قيد الدراسة 38

4.3 المرحلة الثانية 39

4.3.1 تحديد الأدوار والمسؤوليات 39

4.3.2 كتابة السياسات 40

4.4 المرحلة الثالثة 43

4.4.1 توصيل النتائج 43

44	تنفيذ السياسات	4.4.2
44	المراقبة و المراجعة	4.4.3
47	تطبيق إطار العمل المقترح	5. الباب الرابع
61	الخاتمة	6. الباب الخامس
62	الخلاصة	6.1
62	المعوقات	6.2
62	التوصيات	6.3
63	المراجع	7.

فهرس الجداول:

الصفحة	إسم الجدول	رقم الجدول
49	قائمة الممتلكات المطلوب حمايتها	(5/1)
56.....	تأسيس السياسات	(5/2)

فهرس الأشكال

الصفحة	إسم الشكل	الشكل
21.....	البنية الهرمية لسياسات تقنية المعلومات	(2/1)
22.....	دائرة ديمنج	(2/2)
ISO 27001/ISO 27002	تطور المعيارين 29	(3/3)
37.....	مراحل إنشاء سياسة أمن المعلومات حسب الإطار المقترح	(4/1)
37.....	الإطار المقترح لإنشاء سياسة أمن المعلومات	(4/2)
46.....	دورة حياة السياسات خلال الإطار المقترح	(4/3)