Getting Certified ISO/IEC 27001

Experience Sharing

Norman PAN

Doctor A Security

About

The Company

ISO27001 certified since 2003 (then BS7799)

IT Security Monitoring Services & Solutions

Does not offer ISO27001 consultancy services

The Speaker

Norman PAN, cisa, pdcf

Today

Will cover – benefits, how to

Will not cover – our services & solutions, step by step toward ISO27001

Case 1 – Firewall & Antivirus vs Ransomware?

Risk id:

Ransomware

Risk analysis:

Existing Security Controls: Firewall & Antivirus

Impact=High; Likelihood=High?, Risk Level: High?

Risk Assessment:

Risk Level=High, Acceptable?

Risk Treatment:

Controls (Management, Operational, Technical)

=> Management Acceptable Risk Levels

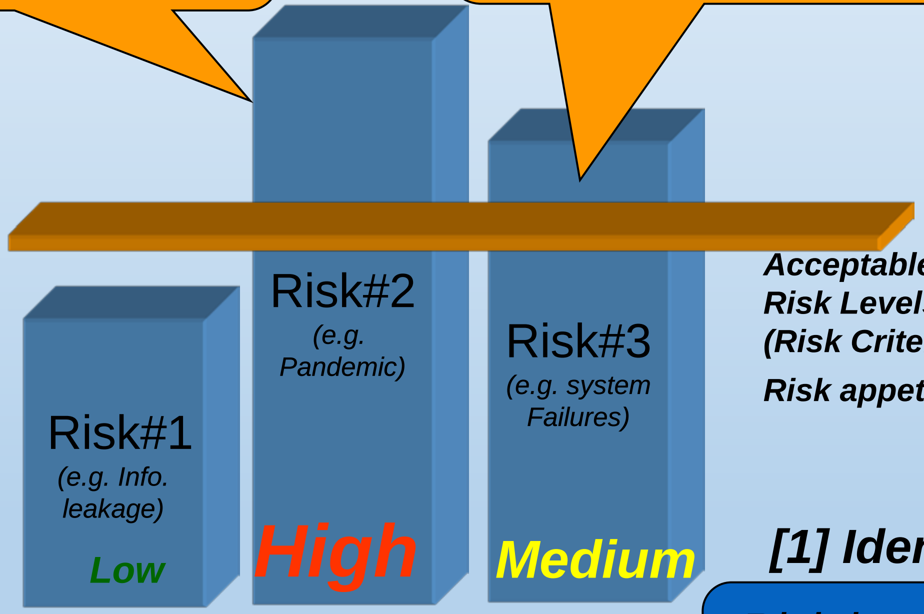
Risk Management

***[4] Risk Treatment** reduces risks to Acceptable Risk Level(s)*

Risk treatment for Primary Risk#2:
Additional Security Control:
e.g. ISO27001-A.10.3
(higher priority)

Risk treatment for Primary Risk#3:
Additional security control:
e.g. Cobit 4-1 xxx
(medium priority)

[3] Risk Assessment
***evaluates** Risk Levels*
*vs **Risk Criteria***

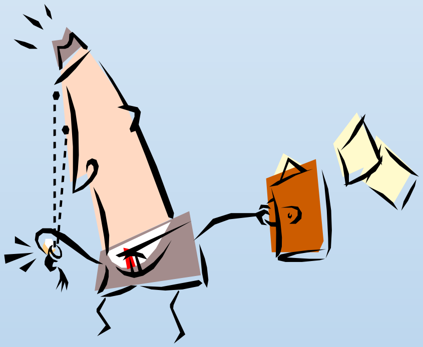


Risk#1
(e.g. Info. leakage)
Low

Risk#2
(e.g. Pandemic)
High

Risk#3
(e.g. system Failures)
Medium

Acceptable Risk Levels (Risk Criteria / Risk appetite)



Management

***[1] Identify** Risk*

*Risk levels is combination of **Impact** and **Likelihood***

[2] Risk Analysis
*determines **Risk Levels***

Why ISO27001? – Day 1

Mkt

Differentiate from Competitors

We imagined

Bought the standard 27001

Copied & pasted a set of policies, guidelines

First Audit

Statement of applicability?

Risk Assessment Procedure & Report?

What we got

Cert & Logo

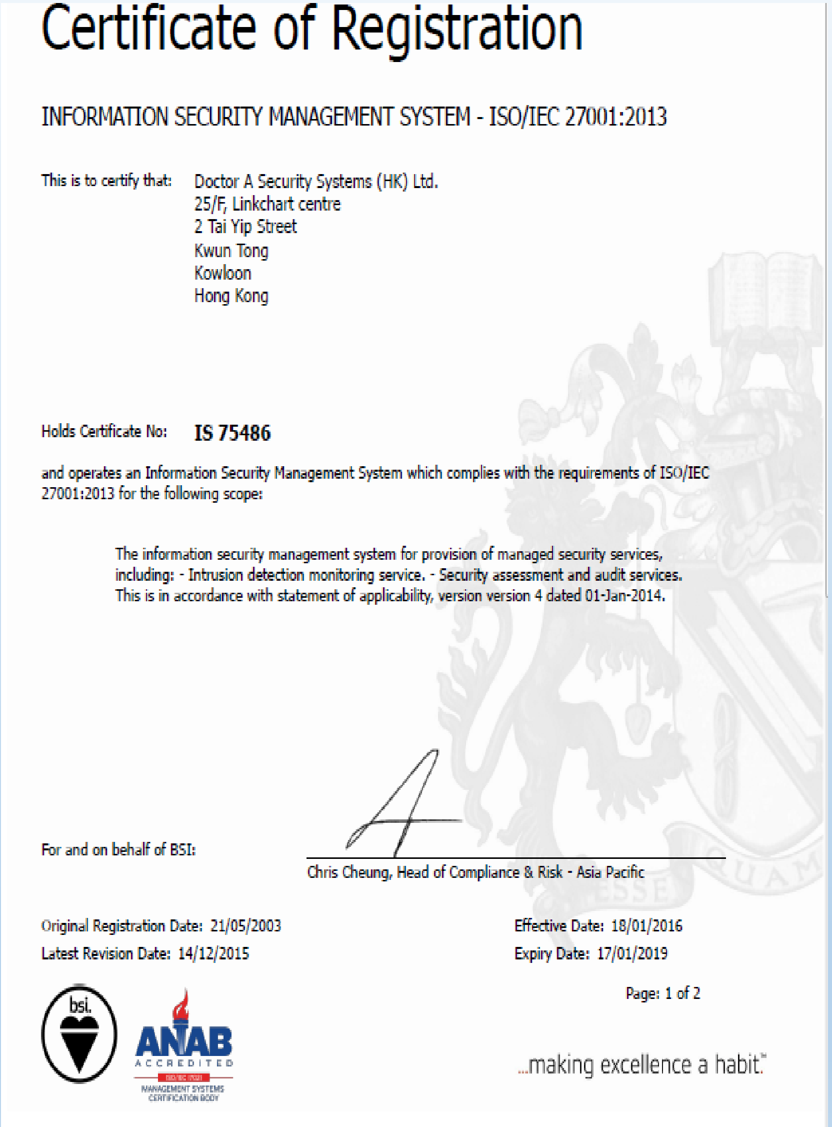
Understand

Risk Assessment

Management System – PDCA -> Continuous Improvement

Understand how to work with an Auditor

Know the boss cares



Certificate of Registration

INFORMATION SECURITY MANAGEMENT SYSTEM - ISO/IEC 27001:2013

This is to certify that:

Doctor A Security Systems (HK) Ltd.
25/F, Linkchart centre
2 Tai Yip Street
Kwun Tong
Kowloon
Hong Kong

Holds Certificate No: **IS 75486**

and operates an Information Security Management System which complies with the requirements of ISO/IEC 27001:2013 for the following scope:

The information security management system for provision of managed security services, including: - Intrusion detection monitoring service. - Security assessment and audit services. This is in accordance with statement of applicability, version version 4 dated 01-Jan-2014.

For and on behalf of BSI:

Chris Cheung, Head of Compliance & Risk - Asia Pacific

Original Registration Date: 21/05/2003
Latest Revision Date: 14/12/2015

Effective Date: 18/01/2016
Expiry Date: 17/01/2019

Page: 1 of 2

bsi.

ANAB ACCREDITED
MANAGEMENT SYSTEMS CERTIFICATION BODY

...making excellence a habit.™

Improve Customer Confidence

your customers know you care

proof that systems and procedures are in place to enable the company to be better prepared to meet the known and unknown security challenges ahead

set you apart from competitors

ISO 27001 are often necessary for inclusion on the list of approved partners.

A go? an Investment

$$

Additional Security Controls

Time

Documentations – Documents & Records

~6 months

How to

Buy the standards

ISO27000, ISO27001, ISO27002, ISO27005, ISO31000, …

Read Section 4-10

Don’t understand, read again, word by word

Risk Assessment

Acceptable Risk Levels?

Annex is for controls selection only

Do not start with Annex

To start? Understand Clauses, e.g.

4.4 The organization shall establish, implement, maintain and continually improve an information security management system, in accordance with the requirements of this International Standard.

5.1 Leadership (Top Management)

Policies, Security Objectives, Integrated into existing process, resources, communicate, intended results, directing HR, continual improvement, support management

Not So Easy …

Risk Assessment => Acceptable Risk Levels

Select Controls -> Statement of Applicability (SOA)

Monitoring

Measurements vs Business Objectives

Continual Improvement

Periodic Internal Audit, Management Review

Summary

Marketing

Differentiation

Customers know you care

You know your boss cares

Management

Reference to international best practices

Keep it running (periodic audit)

Question?

Norman PAN

Doctor A Security

e: npan[at]drasecurity.com