

Copyright © Maximus Consulting Pte Ltd, 2009. Version 1.0 – October 2009

*The right of Maximus Consulting Pte Ltd to be identified as the authors of **Challenges in Information Security Risk Management Presentation** has been asserted by them in accordance with the Copyright Act (Cap. 63), 1998 under the Singapore law. Also they assert recognition of this right as authors in accordance with any international copyright laws or conventions.*

*This publication is **Copyright © Maximus Consulting Pte Ltd, 2009. All rights reserved.** No part of this publication may be reproduced, stored in a retrieval system, or transmitted, or used in any way or form (including presentation of this material as a course, training seminar, lecture or tutorial) or by any means, electronic, mechanical, photocopying, recording or otherwise without the prior knowledge and written permission and consent of Maximus Consulting Pte Ltd.*

Maximus Consulting Pte Ltd - Tel: +65 6396 0938 - Email: enquiry@i-mxms.com

While every precaution has been taken in the preparation of this material, Maximus Consulting Pte Ltd accept no liability or assumes no responsibility for errors or omissions or for any loss or damage caused, arising directly or indirectly, in connection with the use, application and reliance on the information contained herein.



MAXIMUS CONSULTING PTE LTD

W e a v i n g Y o u r A s s u r a n c e G r i d



**Challenges in
Information Security
Risk Management (ISO/IEC 27005)**

Copyright 2009 Maximus Consulting Pte Ltd

2

Coverage

- Understanding Risk Management Requirement
- Risk Management Process in ISO/IEC 27005
- Challenges in Information Security Risk Management
- Building an effective Risk Management Program

ISO/IEC 27001 ISMS Risk Assessment Requirement

“4.2.1 c) Define the risk assessment methodology approach of the organization
Identify a risk assessment methodology that is suited to the ISMS, and the identified information security requirements. The risk assessment methodology selected shall ensure that risk assessments have a **clearly defined scope** and produce **comparable and reproducible results**”

Objective of Risk Assessment

- To provide assurance to the targeted audience
- To provide a basis for establishing policies, procedures, guidelines, standards, practices and controls
- To provide a basis for selecting effective controls
- The goal of risk assessment is not to eliminate all risks, but to reduce the organization's risk to an acceptable level

Concept Check:

Assume that you are responsible for information security within the Organization which spans over 10 locations and you are given an annual security budget is US\$15,000,000. Where will you spend the money?

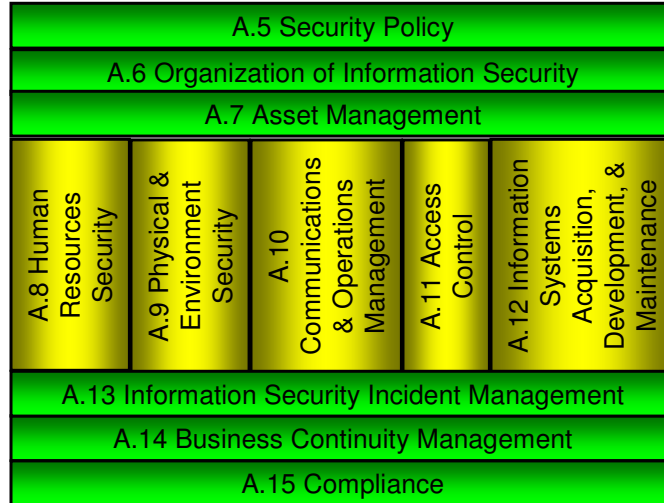
Major Benefits of Information Security Risk Management

- Exhaustive identification and assessment of risks
- Risk education and its possible mitigation actions to both managers and staff
- Good understanding of likelihood and consequences of these risks
- Informed judgment for decision making by the Management
- Priority order for risk treatment being established
- Stakeholders being involved when risk management decisions are made and kept informed of the risk management status
- Effectiveness of risk treatment monitoring

A risk assessment methodology should not be adopted solely on the basis of how quickly a risk assessment can be completed

Source: *Guide for Selecting Automated Risk Analysis Tools*, by Irene E Gilbert, NIST,
<http://csrc.nist.gov/publications/nistpubs/500-174/sp174.txt>

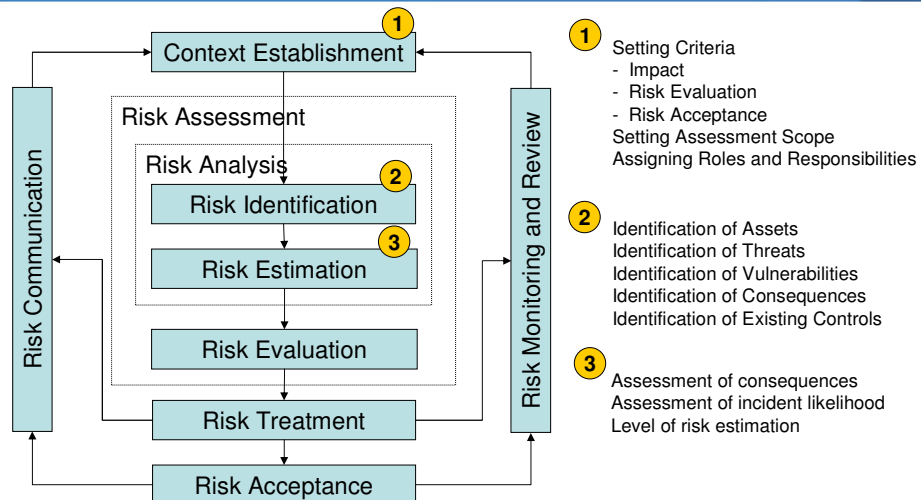
Information Security Risk Management Consideration Areas



Copyright 2009 Maximus Consulting Pte Ltd

7

Information Security Risk Management Process

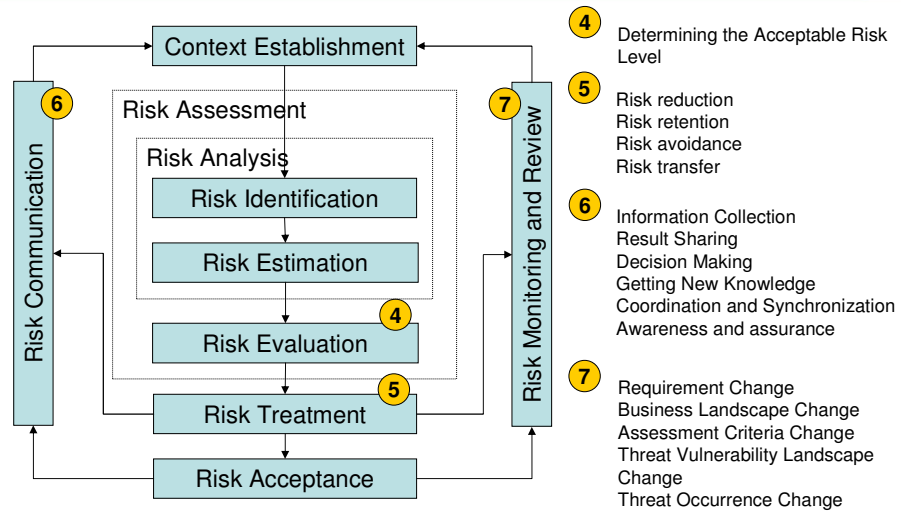


Source: ISO/IEC 27005:2008

Copyright 2009 Maximus Consulting Pte Ltd

8

Information Security Risk Management Process



Copyright 2009 Maximus Consulting Pte Ltd

9

Risk Management Challenges

- Risk Assessment Model
 - Asset Collation Methodology
 - Impact Assessment Methodology
 - Qualitative versus Quantitative Risk Analysis
 - Asset and Risk Ownership
 - Custodian Responsibilities
- Assessment Reliability
 - Expertise Availability
 - Expertise Differences
 - Assessment Synchronization
 - Assessment Exhaustiveness

Copyright 2009 Maximus Consulting Pte Ltd

10

Risk Management Challenges

- Risk Evaluation Model
 - Risk evaluation basis
 - Continual improvement methodology
- Risk Treatment Model
 - Sufficiency of mitigation controls
 - Risk treatment priority
- Landscape Adjustment and Changes
 - Adaptation to changes in business requirement
 - Adaptation to changes in threat and business environment
 - Adaptation to changes in security control environment

Key to Effective Information Security Risk Management

- Availability of Reliable Data
 - Experience of assessor
 - Expertise of assessor
 - Judgment of assessor
 - Repeatability of data
- Effective Use of Resources
 - Re-usability of data
 - Responding to changing environment
 - Level of coordination
- More Robustness
 - Enterprise framework
 - Compliance framework
 - Standardization framework

Summary

- Risk Management is a major requirement in ISO/IEC 27001 ISMS
- Selection Consideration of Risk Management Methodology
 - Understand your Risk Management Objective
 - Understand the Risk Management role within the Organization
 - Understand your Organization Culture
- Risk Management requires Reliable Data
 - Experience of assessor
 - Expertise of assessor
 - Judgment of assessor
 - Repeatability of data
- Risk Management involves substantial Resources
 - Re-usability of data
 - Responding to changing environment
 - Level of coordination

We thank our valued customers for their continual support...



Contact Details:

You Cheng Hwee
 Email: youch@i-mxms.com
 Tel: +65 6396 0938
 URL: www.i-mxms.com

Thank You