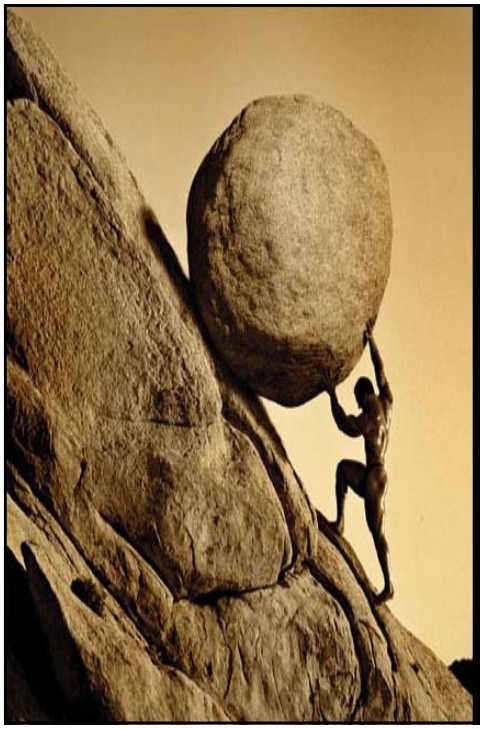


A practical roadmap to ISM Provisions & Guidelines compliance

by

Jacques A. Heide

Curaçao, 8 June 2011

CBCS

Goal: *ISM made practical*

1. Insight in how to approach ISM (*best practices*)
   Source: Provisions and guidelines for Information Security Management of the Central Bank of Curaçao and Sint Maarten
2. What you can do? and
3. (of course) how can we (consultants) help

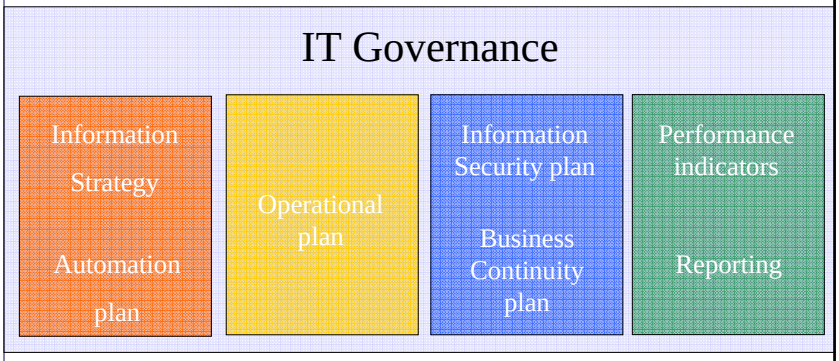
2

Agenda

1. **Introduction**
2. **Simplified SIIQ**
3. **Reverse engineering & categorizing**
4. **Processes, Policies & Procedures**
5. **Simplified approach**
6. **Closure**

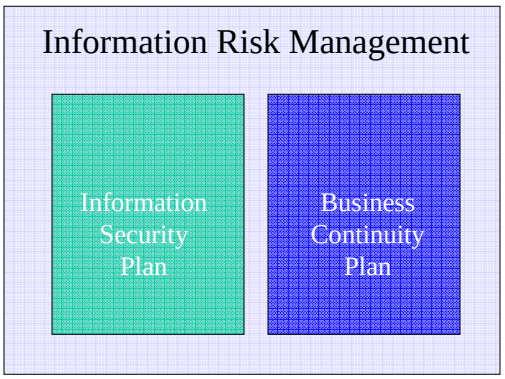
3

Governance of information provisioning



4

Helicopter view on information security



5

Information Risk management

Are the information security risks - with business continuance in mind – mitigated properly?

- Timely, deadline may be fixed?
- Completely, no surprises?
- Effective, according to expectations?
- Efficient, at acceptable costs?

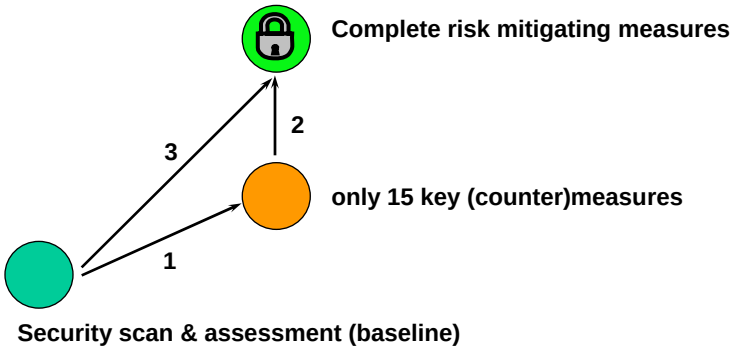
6

Timeline to certified ISM

2011	2012	2013	2014	2015
Today: initiate! BCM plan	ISM plan ready ISO 27002 compliant	ISM monitoring	…	CBCS ready! Certifica-tion?

7

Practical roadmap



8

Agenda

1. Introduction
2. Simplified SIIQ
3. Reverse engineering & categorizing
4. Processes, Policies & Procedures
5. Simplified approach
6. Closure

9

Provisions & Guidelines for ISM

Provisions and Guidelines for Information Security Management

I. Introduction 1
II. Legal base and scope 3
III. Implementation 4
IV. Information Security Management principles 5
Principle 1. Establish effective management oversight 5
Principle 2. Design, implement and maintain an information security framework 8
Principle 3. Maintain an ongoing risk assessment program 13
Principle 4. Establish information security monitoring 16
Principle 5. Establish incident management and response 19
Principle 6. Protect the privacy of customer information 21
Principle 7. Provide information security training 22
Principle 8. Audit the information security process 23
Appendix 1: Glossary/Definitions 24
Appendix 2: Links to helpful websites 26
Appendix 3: SMART Metrics 27

10

A *Simplified SIIQ* peek

1. General | 2. Info Sec | 3. BCM | 4. Outsourcing

2A. Information Security General	
1. Please indicate if your institution has installed an anti-virus solution for all servers, desktops and laptops.	Yes
2. Is the **anti-virus** program up-to-date for all protected devices ?	Yes

1. GENERAL √
2. INFORMATION SECURITY √
   - *2A. Information Security General* √
   - *2B. Access, Authentication and Authorization Controls* √
   - *2C. Network Security* √
   - *2D. Data Backup* √
   - *2E. User Equipment Security* √
   - *2F. Physical Security* √
   - *2G. IT Support* √
3. BUSINESS CONTINUITY MANAGEMENT √
   - *3A. Business Continuity Management (BCM)* √
4. OUTSOURCING TECHNOLOGY SERVICES √
   - *4A. Outsourcing* √

4. Do you have a written procedure describing how to update the anti-virus definition for all the protected devices ?	No	not considered necessary since the update is being done automatically by a professional external party when needed

11

Agenda

1. **Introduction**
2. **Simplified SIIQ**
3. **Reverse engineering & categorizing**
4. **Processes, Policies & Procedures**
5. **Simplified approach**
6. **Closure**

12

1. General | 2. Info Sec | 3. BCM | 4. Outsourcing

Categories	Description
General	Inventory: infrastructure, organization, policies, security awareness training
Infosec	Anti-virus, patch management, firewall, physical & logical access: authentication & authorization, change management policy, configuration management, people training, e-mail, internet, back-up, user equipment
BCM	Overall continuity plan, disaster recovery, recovery site, back-up, patches, documentation
Outsourcing	SLA assessment, periodic reporting

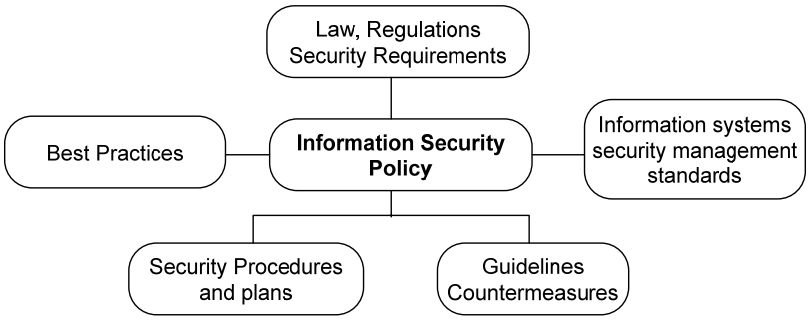
13

Agenda

1. Introduction
2. Simplified SIIQ
3. Reverse engineering & categorizing
4. Processes, Policies & Procedures
5. Simplified approach
6. Closure

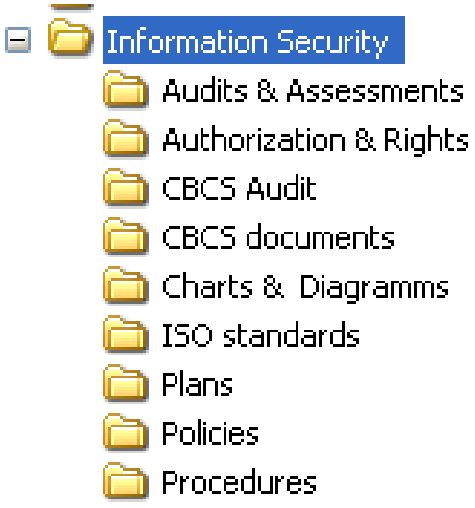
14

Complex? Vast?



15

Document structure



16

Needed plans, policies, procedures 1

- Information strategy plan
- Overall information risk management plan
- Business continuity plan
- Disaster recovery plan
- Organization chart
- Infrastructure chart
- E-mail policy
- Internet policy
- Remote access policy
- Information security policy
- Password policy
- Reporting

17

Needed plans, policies, procedures 2

- Authorization matrices of information systems
- Backup procedure
- Restore procedure
- E-mail management
- Change management procedure
- End user security procedure
- Excess hardware policy
- Incident management process /procedure
- Application security
- Manage firewalls & routers
- Change request form
- General user security awareness powerpoint
- Configuration database or list

18

Agenda

1. Introduction
2. Simplified SIIQ
3. Reverse engineering & categorizing
4. Processes, Policies & Procedures
5. Simplified approach
6. Closure

19

10 essential items for ISM

Management:

- Appoint information security responsibilities
- Adhere to privacy laws and regulations
- Develop information security policy

Procedures:

- Report security incidents
- Plan business continuity
- Comply to security policies

Countermeasures:

- Educate and train information security
- Manage anti-virus
- Prevent unauthorized copying of software
- Secure business documents (i.e. authorization, intrusion prevention)

20

Information risk management revisited

Are the information security risks - with business continuance in mind – mitigated properly by a practical simplified approach?

- **Timely**, deadline may be fixed? ☑
- **Completely**, no surprises? ☑
- **Effective**, according to expectations? ☑
- **Efficient**, at acceptable costs? ☑

Note: full effort still needed / mandatory!

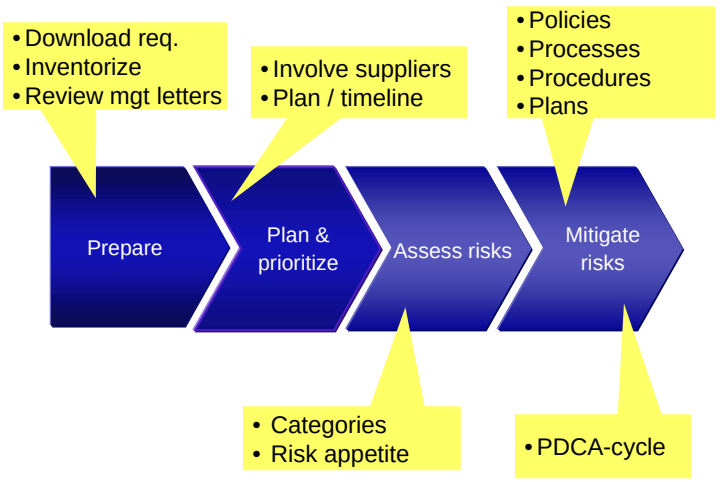
21

Agenda

1. Introduction
2. Simplified SIIQ
3. Reverse engineering & categorizing
4. Processes, Policies & Procedures
5. Simplified approach
6. Closure

22

Activities wrap-up



23

Closing remarks

1. ISM mandatory by Supervisor
2. Information security management and business (read operational) continuity is mandatory for clients, personnel, shareholders and other stakeholders
3. Complex matter
4. Curaçao has its share of possible high impact threats: weather, flooding, power, telecommunications (Internet) and personnel
5. There is help: supervisor, consultants, suppliers

24

Supplier's / consultant's view

1. Understanding of risk & impact concepts
2. Experienced in (all aspects of?) ISM
   - Assessments
   - Countermeasures, etc.
3. Plan & policy writer (!)
4. Test manager
5. 2nd opinion
6. Pre-Auditor (end result or ISM process)
7. Soundboard for board or management

25

Beware! Times have changed!

26

Q & A

27

More Info

- Jacques Heide
  ICTAS n.v.
  Santa Rosaweg 17
  P.O.Box 491
  Curaçao, N.A.
  www.ICTAS.com
  jheide@ictas.com
  +599 9 513-3717

28