Information Security Risk Assessment and Management

Aggeliki Tsohou,
Assist. Professor, Ionian University
atsohou@ionio.gr

Common Problems in Security Management in Organizations

- Justification of IT security investments
- Communication between technical experts and management
- Assurance of active participation of stakeholders in security policy design
- Assurance of top management support
- Overcoming the belief that security is only a technical issue
- Selection of the appropriate security controls

“How much” should we protect the IS?

- 100% secure systems do not exist
- We need to balance the treats/consequences with the cost of the security measures
- We need methodologies that can measure the threats and express them in units equivalent to those used for expressing the effectiveness of the security measures.

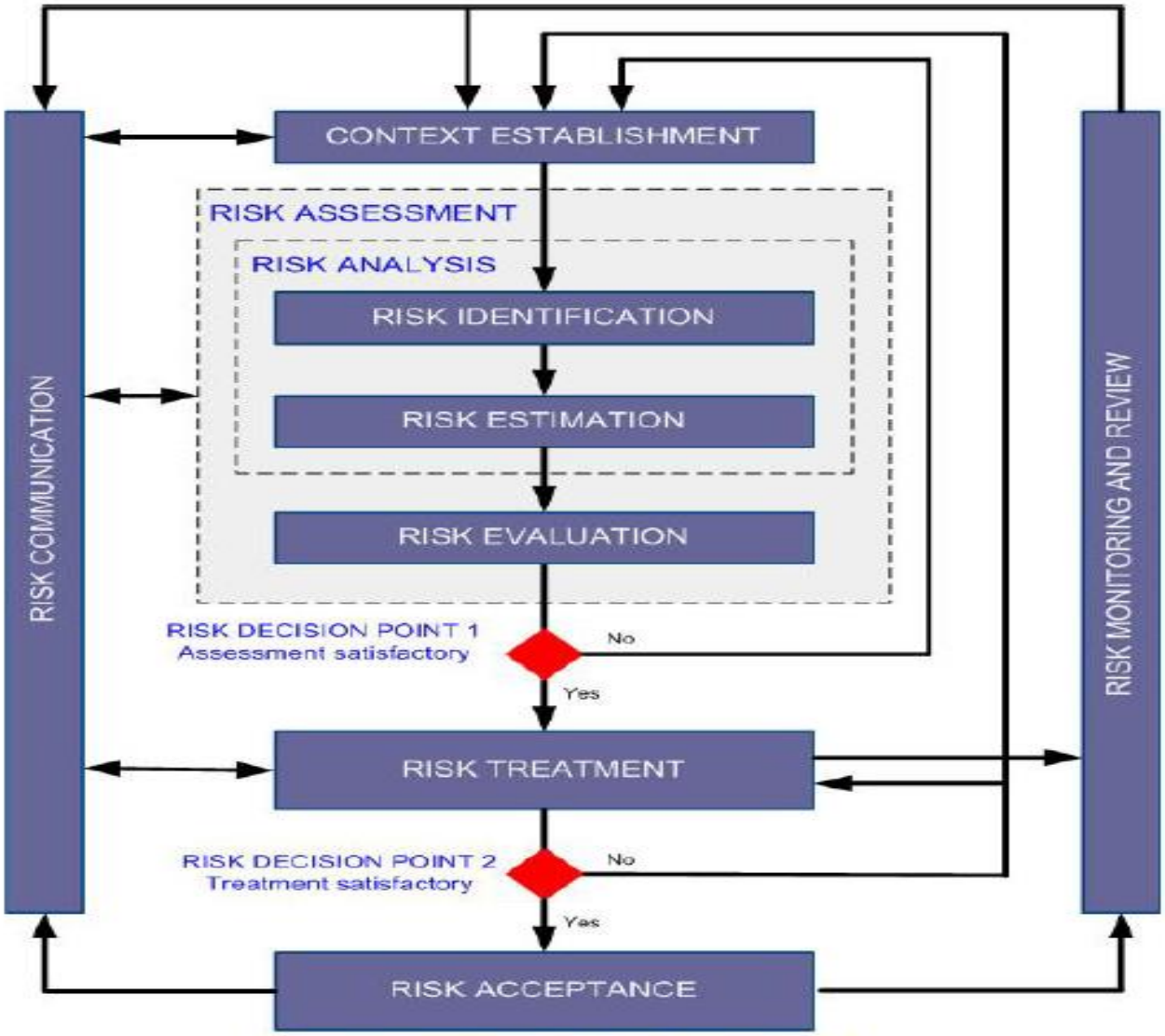
How can we measure risk?

- Risk is a function of:
  - The IS assets (A)
  - The nature and number of IS vulnerabilities (V)
  - The nature and occurrence probability of a threat (T)
  - The nature and extend of the consequences (impact) (I) that the organisation will experience in case of a security incident
- Thus R=f(A,T,V,I)

Risk Assessment Methods

- Are based on a general, high-level models of the system
- Assess the value of IS assets
- Analyse the vulnerabilities
- Analyse the Threats
- Measure the potential impact from a security incident
- Calculate the Risk Factor
- Propose suitable countermeasures

Core processes



Risk Assessment Output

A justified proposal of specific security measures that are appropriate and adequate for the specific information system

Practical Problems

- There are too many risk assessment methods, but it is not feasible to evaluate them in detail, neither to compare them
  - ENISA developed a risk assessment methods inventory

    http://rm-inv.enisa.europa.eu/methods/rm_ra_methods.html
- They don't necessarily cover all the steps of the process
- They don't necessarily cover all the different types of assets for an IS

Strengths and Weaknesses

- Strengths
  - They are a communication tool between the different stakeholders, and especially IT experts and management
  - They can provide a justification of security investments
  - They assist in compliance with legal requirements
- Weaknesses
  - They are based on a simplified model of the IS
  - The results are based on subjective estimations (mainly assets' value and impacts)
  - Human threats are not easy to predict

An Example: CRAMM risk assessment method

CCTA

RISK

ANALYSIS and

MANAGEMENT

METHOD

Overview

STAGE 1	Scope the Security Problem
STAGE 2	Evaluate the Risks
STAGE 3	Select Appropriate Countermeasures

STAGE 1 - The Major Steps

- Agree the basis of the review (at the first management meeting)
- Identify assets
- Create asset model(s)
- Value assets
- Agree results with management (at the second management meeting)

STAGE 2 - The Major Steps

- Match asset groups and threats
- Identify appropriate impacts
- Assess threats and vulnerabilities
- Calculate the risks
- Agree results with management

  (at the third management meeting)

STAGE 3 - The Major Steps

- Calculate recommended countermeasures
- Review the measures
- Review measures statuses (marking as «installed» etc.)
- Design security plan
- Agree results with management

(at the fourth management meeting)

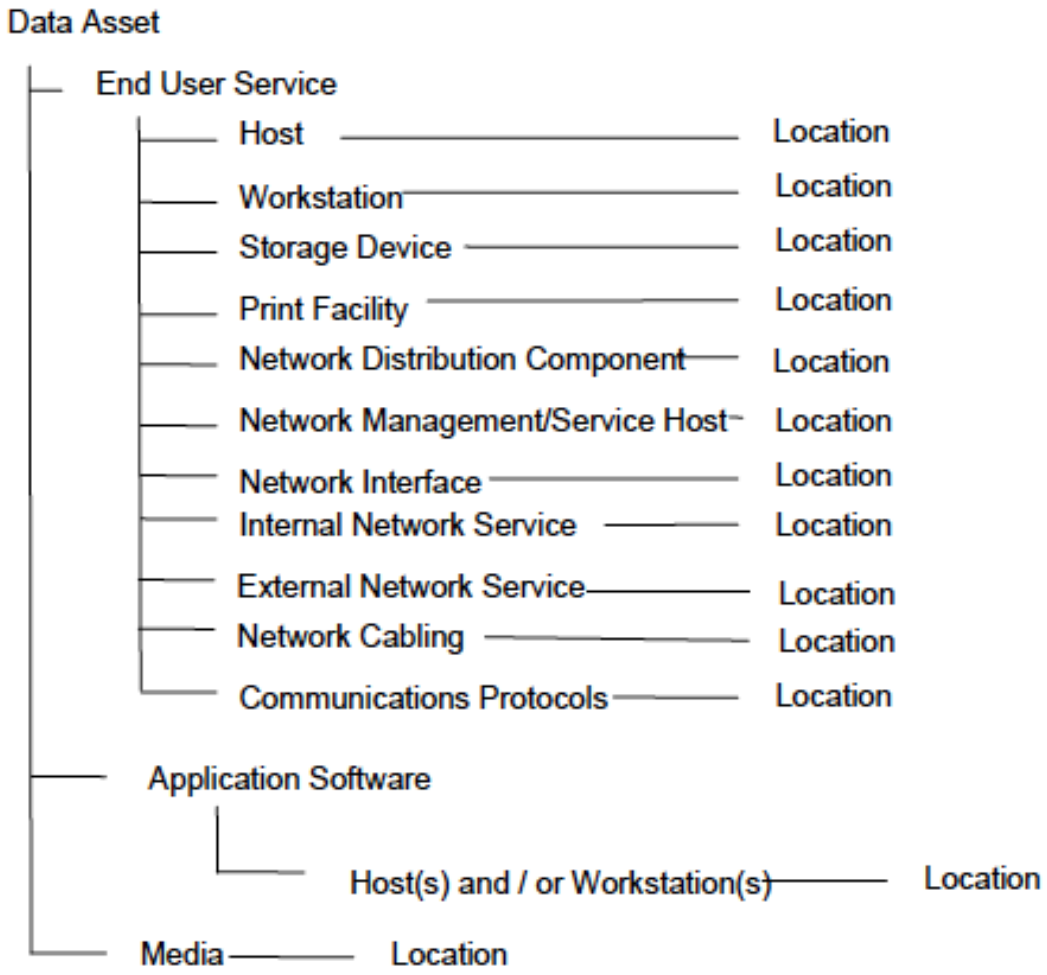
CRAMM Stage 1 – Step 1: Identification of assets

- Defining Locations
- Defining Physical assets
- Defining Software assets
- Defining Data assets
  - Subsets or supersets according to the use made of the data
- Defining Service provided by the system to the user

CRAMM Stage 1 – Step 1: Identification of assets

- Identify
  - Data assets and the End-user-service which supports it
- Link
  - Physical assets to end-user-service
  - Locations to Physical assets
  - Software to Data assets
  - Software to Physical assets
  - Media assets to Data assets

CRAMM Stage 1 – Step 1: Identification of assets



Asset Models, Cramm v5.1 User Guide

CRAMM Stage 1 – Step 1: Evaluation of assets

- Evaluation of assets' value
  - Software Assets: according to replacement financial value
  - Hardware Assets: according to replacement financial value
  - Data Assets: Stakeholders' estimations

CRAMM Stage 1 – Step 1: Evaluation of assets

Through their impact in terms of…

- Physical Asset Destruction
- Data Unavailability
- Data Destruction
- Data Disclosure
- Data Modification
- Communications related impacts

CRAMM Stage 1 – Step 1: Evaluation of assets

Worst (reasonable) case scenarios for

- Data unavailability
  - 10 periods possible. 15 minutes to 2 months
- Destruction
  - Since last successful back-up
  - Total
- Disclosure
  - Staff
  - Contracted service providers
  - Outsiders

CRAMM Stage 1 – Step 1: Evaluation of assets

Worst (reasonable) case scenarios for

- Modification
  - Small scale
  - Wide scale
  - Deliberate
- Communications
  - Insertion
  - Non-delivery
  - Replay
  - Repudiation of origin
  - Repudiation of receipt
  - Mis-routing
  - Traffic monitoring
  - Out of sequence

CRAMM Stage 1 – Step 1: Evaluation of assets

Category of Impact	Scale
Personal safety	2-4, 6-10
Personal information	1-6
Legal and regulatory obligations	3-7
Law enforcement	3, 4, 7, 8
Commercial and economic interests	1-7, 9, 10
Financial loss	1-8
Public order	1-3, 6, 7, 9, 10
International relations	3,7,9,10
Defence	1,3,7,8,9
Security and intelligence	7,9,10
Policy and operations of public service	1,3,5,6,7
Management and operations of organisation	1, 3, 5-7
Loss of goodwill	2,3,5,7

Calculating Implied Asset Values

- Implied value determined by the value of data and software that the physical assets support
- Physical assets are given an implied value
- Locations also have implied values

$$1 + 1 = 3$$

CRAMM Stage 1 – Step 2: Management Review

- Management Report
- Valuation Report
  - All asset types
- Impact assessment
  - Values calculated by CRAMM
- Asset Model
  - Details of selected asset model
- Backtrack
  - Shows where impact values derived from (factors that lead to impact recommendations)

CRAMM Stage 2 - Step 1: Identification of Threats

Which asset is threatened by which→

→Threat/Vulnerability combination→

→with what impact

Threat / Vulnerability Asset Impact = Risk

combined as a **"triple"**

CRAMM Stage 2 - Step 1: Identification of Threats

- Masquerading of identity (x3)
- Unauthorised use of an application
- Introduction of damaging or disruptive s/w
- Misuse of system resources
- Communications infiltration (x3)
- Accidental Mis-routing
- Technical failures (x9)
- Power failure
- User error
- Fire

CRAMM Stage 2 - Step 1: Identification of Threats

- Air conditioning failure
- System and network software failure
- Application software failure
- Operations error
- Hardware maintenance error
- Software maintenance error
- Water damage
- Natural disaster
- Staff shortage
- Theft (x2)
- Willful damage (x2)
- Terrorism

CRAMM Stage 2 - Step 2: Threat Assessment

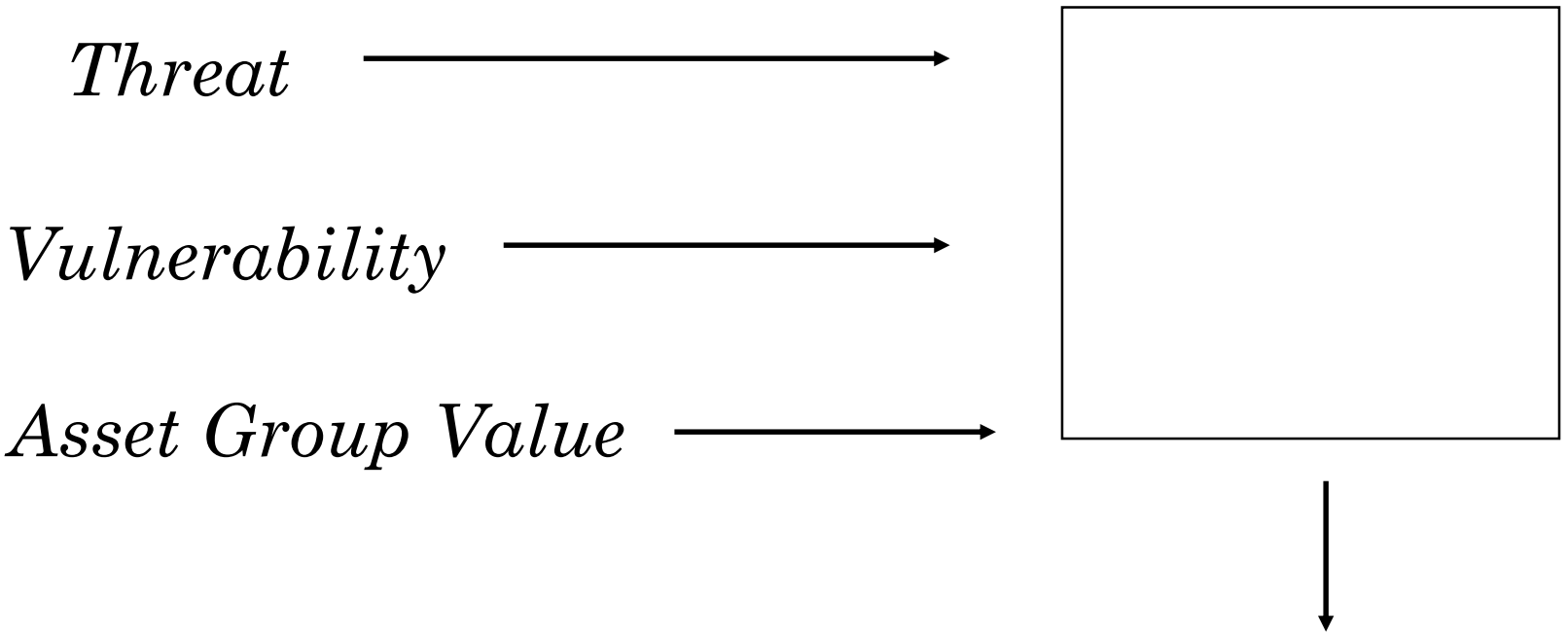
- Measured through the likelihood of occurrence

- Questionnaire-based to assess the likelihood of occurrence for each threat.
  - Very High
  - High
  - Medium
  - Low
  - Very Low

CRAMM Stage 2 – Step 3: Vulnerability Assessment

- Also questionnaire-based to assess the likelihood of the threat succeeding and the extend of the damage
  - High
  - Medium
  - Low

CRAMM Stage 2 – Step 4: Assessment of Risks



Measured on a scale of 1 - 7

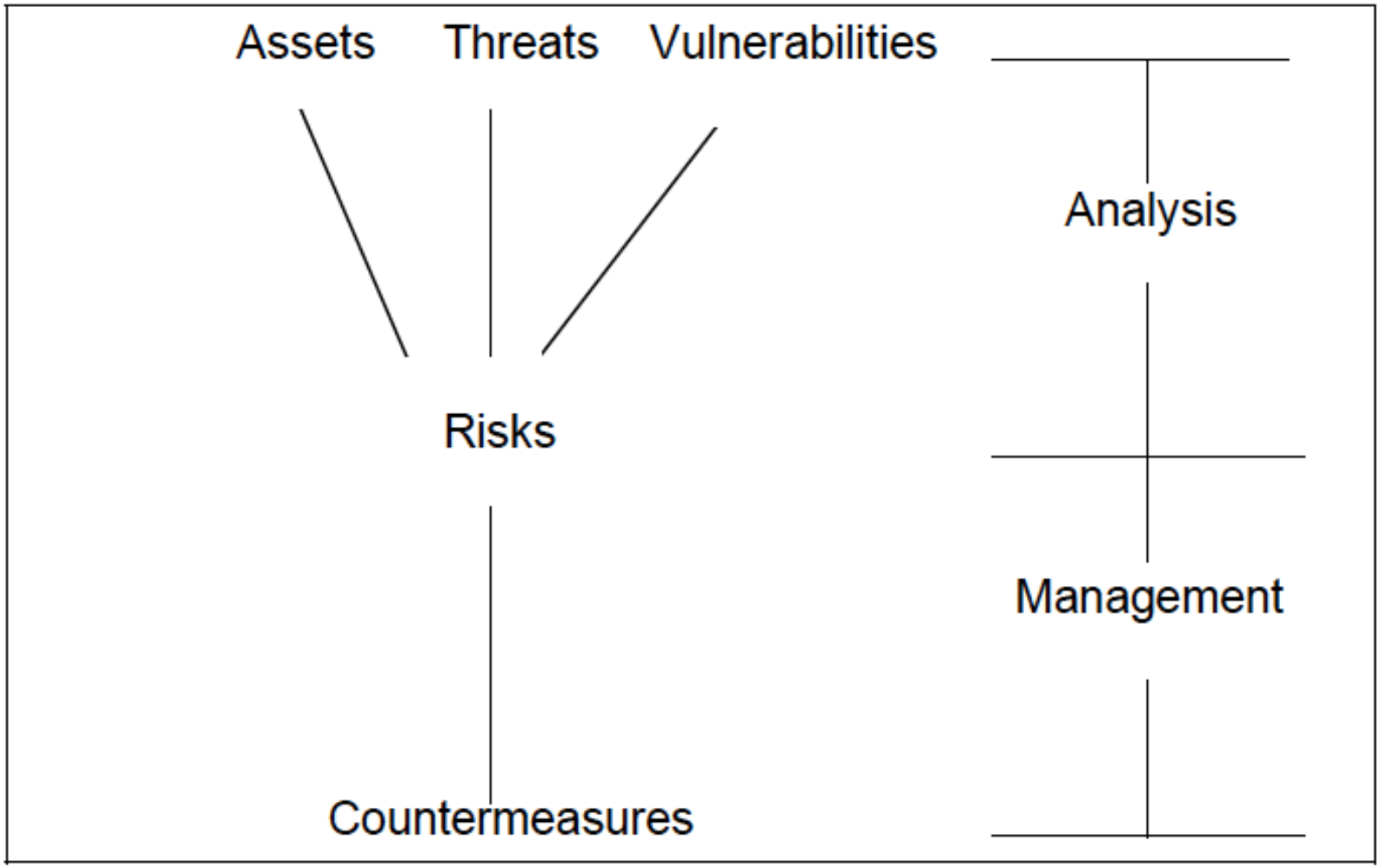
CRAMM Stage 2 – Step 5: Management Report

- Management Report
  - Skeleton headings
- Asset Group Report
  - Details of all asset groups
- Threats to asset Groups
  - Threat to asset group relationships
- Threat & Vulnerability Questionnaires
  - Completed questionnaires
- Measures of Risk Report
  - Threat, vulnerability and risk levels
- Backtrack
  - Shows where risk values derived from

CRAMM Stage 2 – Step 5: Management Report

- Present the findings of the Threats & Vulnerability assessment
- Present the levels of risk to the system
- Skeleton report available from CRAMM tool
- Report should contain
  - Introduction
  - Summary of asset valuation
  - Risk assessment

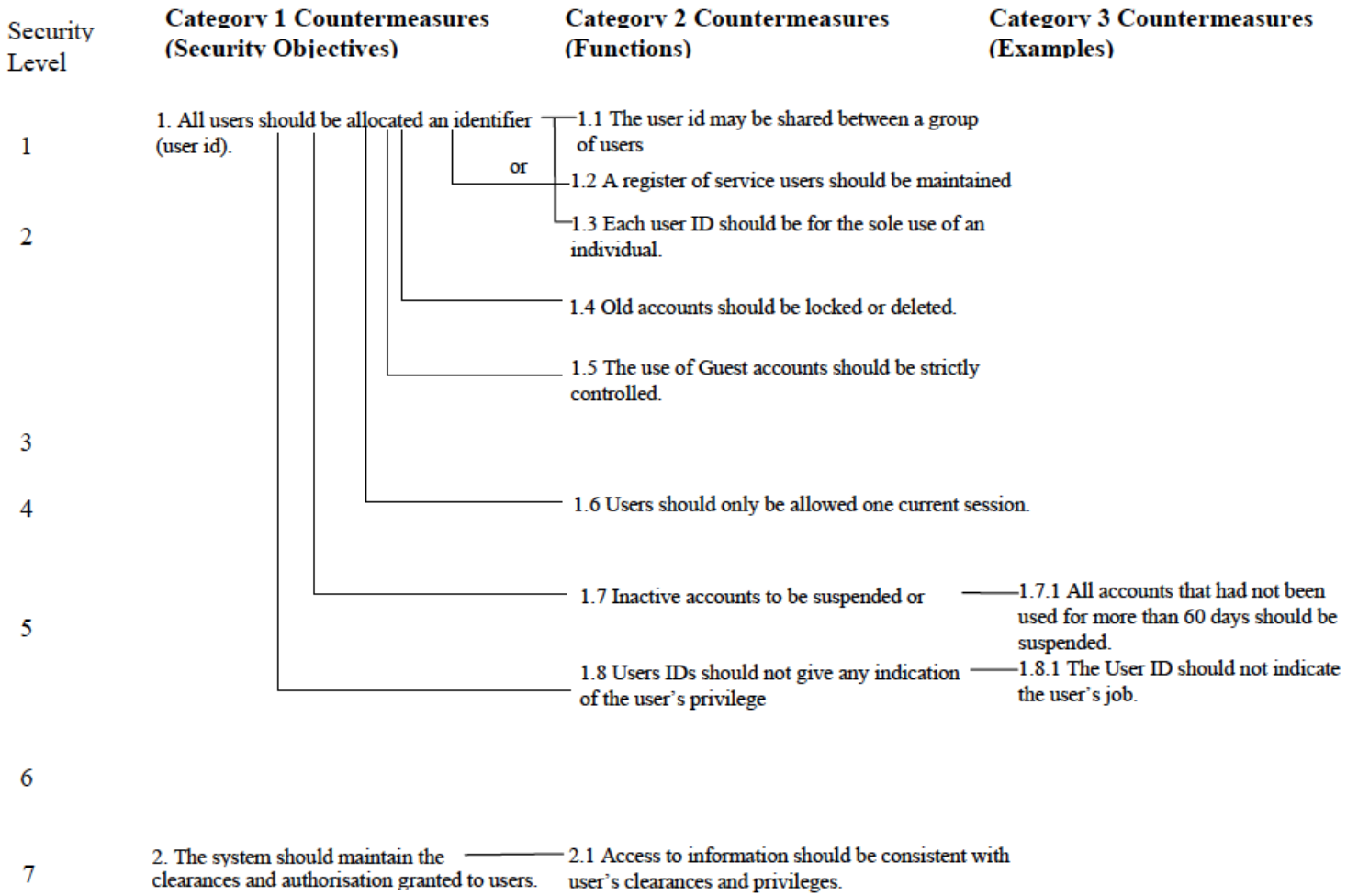
CRAMM Stage 3 - Step 1



CRAMM Stage 3 - Step 1: Countermeasure Selection

- Countermeasure library
  - Countermeasure groups (63)
  - Sub-groups (181)

CRAMM Stage 3 - Step 1: Example of the controls library



CRAMM Stage 3 - Step 1: Countermeasure Selection

- By comparison of the measure of risk of a «triple» with the security level of each countermeasure
- By matching the threat to the countermeasure group
- By matching the asset to the countermeasure group
- By matching the impact to the countermeasure group

CRAMM Stage 3 - Step 2: Countermeasure Status

- Installed
- To be implemented
- Implementing Recommendation
- Implemented Recommendation
- Already covered
- Accept level of risk
- Under discussion
- Not installed

CRAMM Stage 3 - Step 3: Design Treatment Plan

- Consultation / Approval Interviews
  - acceptability
  - background history
  - other constraints
- Trade Offs
  - requirement vs culture
  - requirement vs budget
  - requirement vs degree of change
  - prioritisation method
  - implementation strategy

CRAMM Stage 3 - Step 4: Management Report

- Management Report
  - Skeleton headings
- Countermeasure Library
  - Measure of risk values for each impact type
- Countermeasure Priorities
  - Details of priority values
- Countermeasure Costs
  - Status of recommendations plus costs
- Backtrack
  - Which impacts led to which countermeasures being selected

CRAMM Stage 3 - Step 4: Management Report

- Threats
- Assets
- Threat/Assets
- Countermeasure groups
- Justification
- Alternatives
- Costs and products
- Recommendations

Case

A Hospital

- Legal drivers due to personal and sensitive data being processed
- Scientific selection of countermeasures
- Communication between the stakeholders:
  - Doctors
  - Administrative personnel
  - IT personnel
  - Contractors (e.g., cleaning company)

The hardware

- 1 Server hosting the Document Management application
- 1 Server hosting the Blood Results application
- 1 Server hosting the Human Resources and Payroll application
- 1 Server hosting the Patients' Management application and the Logistics application
- 1 webserver

The software

- The Document Management application
- The Blood Results application
- The Human Resources and Payroll application
- The Patients' Management application
- The Logistics application
- The MS Office

How about the Data?

The Categories of data

Categories of data:

- Blood Results
- Medicine
- Human Resources
- Payroll
- Suppliers
- Finance
- Patient Appointments
- Health Expenditures
- Document Management

Assessing the Value of Data

	Availability Loss					Integrity Loss			Confidentiality Loss
	1 hour	12 hours	1 day	2 days	1 week	Total Loss	Part Loss	Malicious Changes	
Blood Results Data	1	3		5		3	6	6	6
Medicine Data	2	2	5			4	5	6	6
Human Resources Data		3	3		5	5	5	5	6
Payroll Data	1		1		3	3	3	3	3
Suppliers Data		1	3		3	3	3	5	2
Finance Data	1	2	5			6	4	5	1
Patient Appointments Data	1	3	5			5	5	5	4
Health Expenditures Data		1	2		5	4	3	4	3
Document Management Data		1		4	4	5	5	5	1

Assessing Threats and Vulnerabilities

Asset	Impact in Case of Masquerading by Insiders Threat	Threat Assessment	Vulnerability Assessment
Blood Results Data, Personnel Data	Availability Loss (up to 2 days), Part Loss, Loss of Confidentiality to Outsiders	High	Medium
	Malicious Modifications	High	High
Medicine Data	Availability Loss (up to 2 days), Part Loss, Loss of Confidentiality to Insiders	Very High	Medium
	Malicious Modifications	Very High	High
Patient Appointments Data	Availability Loss (up to 2 days), Part Loss, Loss of Confidentiality to Insiders	High	Low
	Malicious Modifications	High	Medium
Finance Data	Availability Loss (up to 2 days), Part Loss, Loss of Confidentiality to Insiders	High	Low
	Malicious Modifications	Very High	Medium
Payroll Data	Malicious Modifications	High	High
Health Expenditures Data	Availability Loss (up to 2 days), Part Loss, Loss of Confidentiality to Insiders	Very High	Low
	Malicious Modifications	Very High	Medium
Suppliers Data	Malicious Modifications	High	Medium

The Higher Level Threats

- Masquerading by Insiders
- Masquerading by Outsiders
- Application Failure, particularly for Payroll Application
- User Error
- Electivity loss
- Theft

Assessing Risks (The higher ones)

Masquerading by Insiders Threat		
Asset	Impact	Risk Level
Medicine Data	Malicious Modifications	6
	Availability Loss from 1 to 2 days	5
Blood Results Data, Finance Data, Human Resources Data	Malicious Modifications	5

Masquerading by Outsiders Threat		
Asset	Impact	Risk Level
Medicine Data, Blood Results Data, Patient Appointments Data	Loss of Confidentiality to Outsiders	5
Medicine Data	Malicious Modifications	5

Assessing Risks (The higher ones)

Malicious Code Threat		
Asset	Impact	Risk Level
Workstations	Total Loss of Data, Partial Loss of Data, Malicious Modifications	5