INTRODUCTION OF INFORMATION SECURITY

AfNOG 2011 - Tanzania

By
Marcus K. G. Adomey

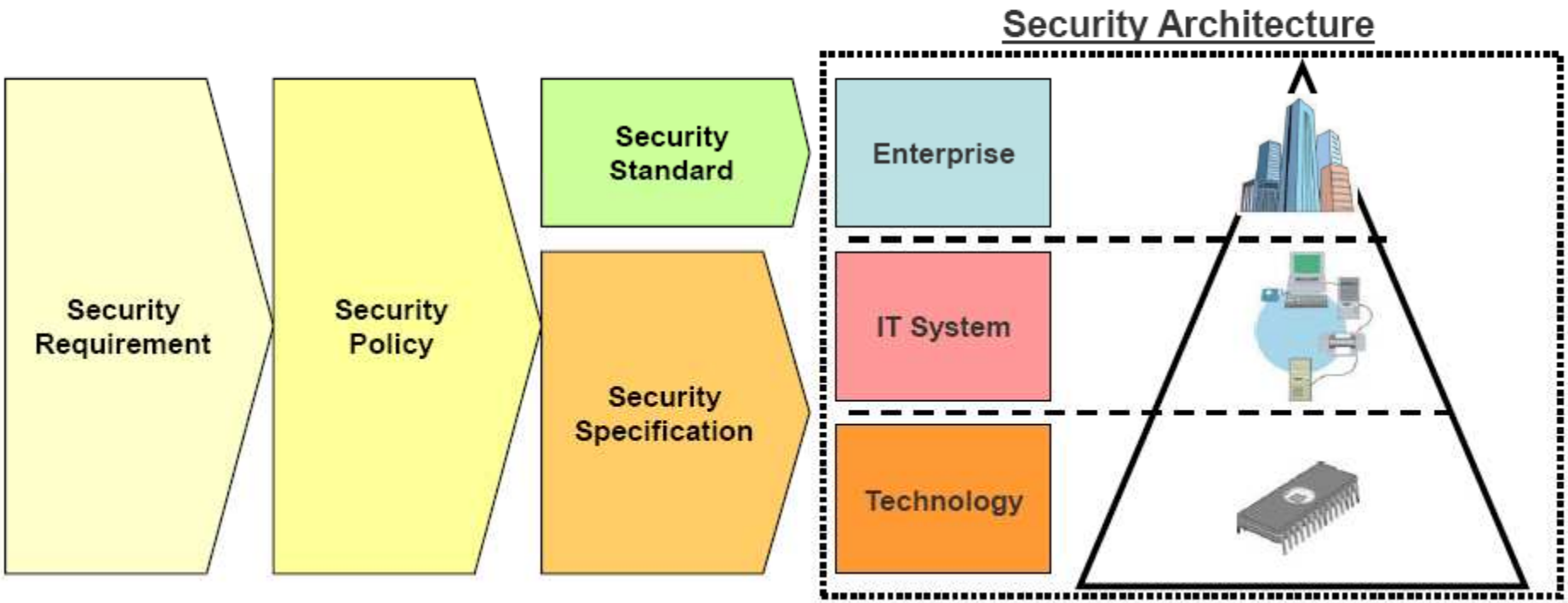
Presentation adapted from JPCERT presentation
During AfriNic meeting in South Africa – Nov 2010

Overview

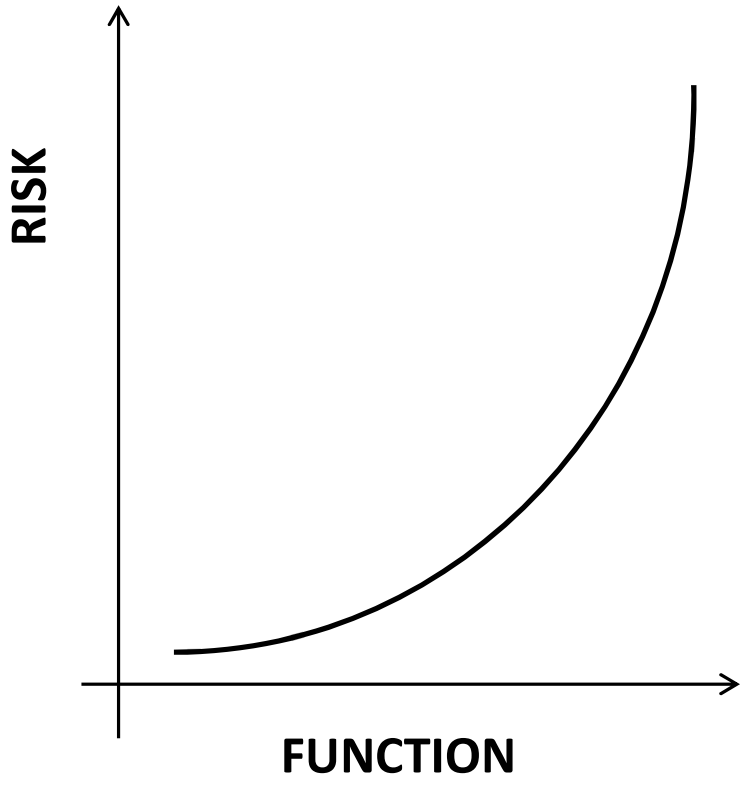
- ✓ Security Architecture
- ✓ Nature of Information Security Risk
- ✓ Principles of Information Security
- ✓ Security Process

Security Architecture

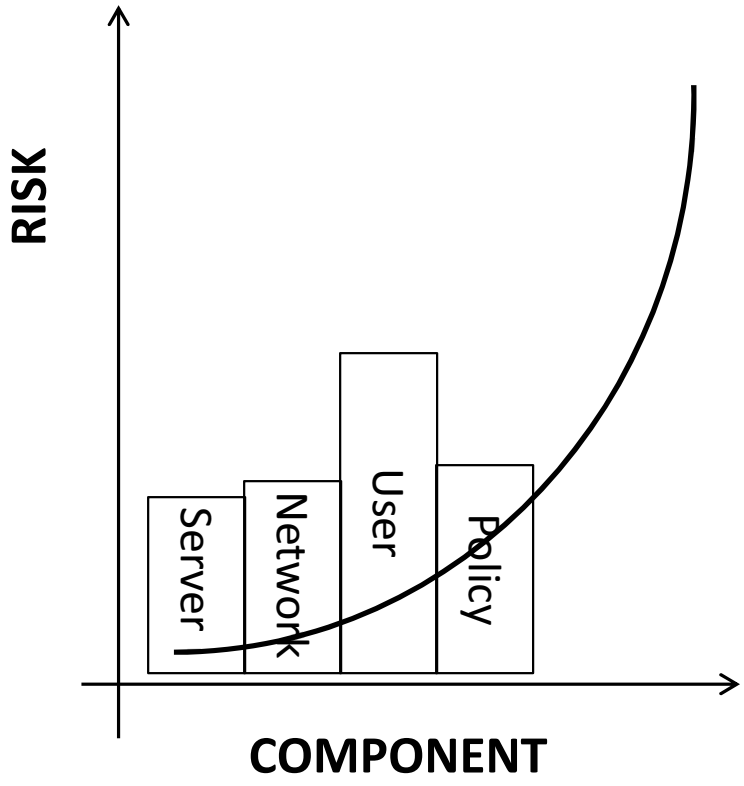
Design of systems to satisfy security requirements.



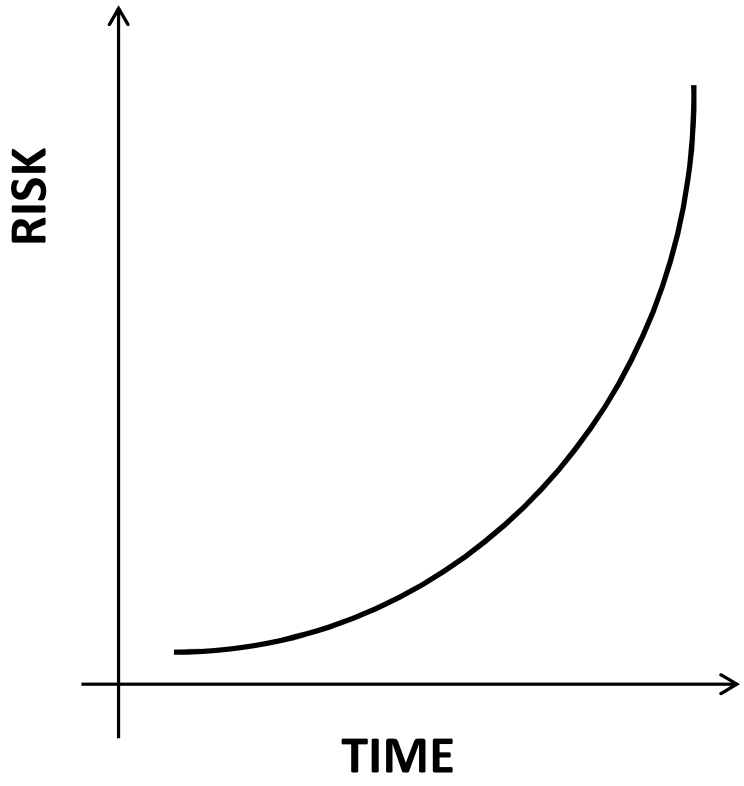
Nature of Information Security Risk



As number or usefulness of functions increase, information security risks also increase.



Security is only as strong as the weakest link.



As time goes by,

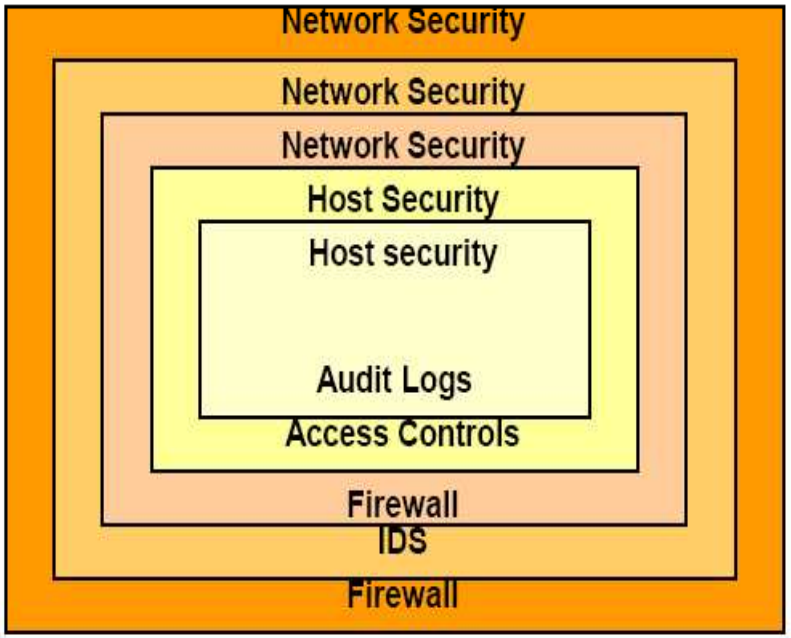
information security risks

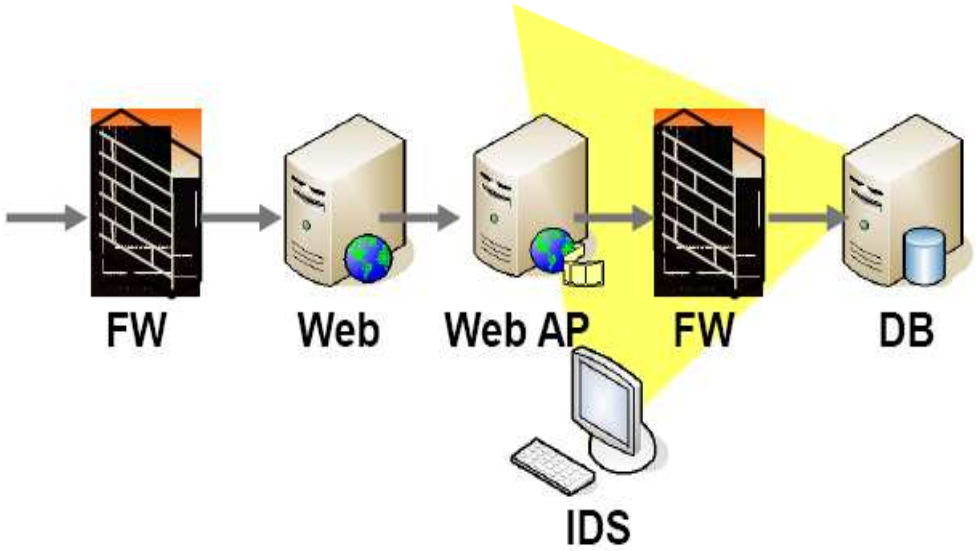
of a system increase.

Principles of Information Security

Layered Security / Defense in Depth

- ✓ Avoid single point of failure.
- ✓ "Make the effort for compromise more costly than it is worth to a potential attacker."(Conklin et.al., Principles of Computer Security)
- ✓ Maintenance cost increases. (drawback)





Typical 3 Layer Web-App Architecture

Least Privilege

"A subject(user, applications, or process) should have only the necessary rights and privileges to perform its task with no additional permissions.)"

"Limiting an object's privileges limits the amount of harm that can be caused, thus limiting an organization's exposure to damage." (Conklin et.al.)

Compartmentalize

- ✓ Divide assets into separate sections.
- ✓ Limit the access of a successful intruder.
- ✓ Increase layers of security.
- ✓ Increases complexity and costs (drawback).

Secure the Weakest Link

"A system is only as secure as the weakest link."

"Find the weakest link and secure it. Then worry about the next weakest link." (Schneier, Secrets & Lies)

Keep It Simple

If you do not understand something, you cannot truly secure it.

"Complexity is the worst enemy of security." (Schneier)

"A system with fewer links is easier to secure."

Make systems, applications and processes as simple as possible.

Halt services that you do not use.

Diversity of Defense

Mix products from different vendors.

Increase layers of security.

Increases complexity and costs (drawback).

Fail Secure

When a system fails, it must retain secure state.

Design systems as default secure.

Security Through Obscurity

"Approach of protecting by hiding it."

Make it difficult to attack, but "does not prevent anyone from eventually succeeding."

"Security through obscurity is considered a poor approach, especially if it is the only approach to security." (Conklin et.al.)

"Not in products, but in how products are used. I call this unpredictability." (Schneier)

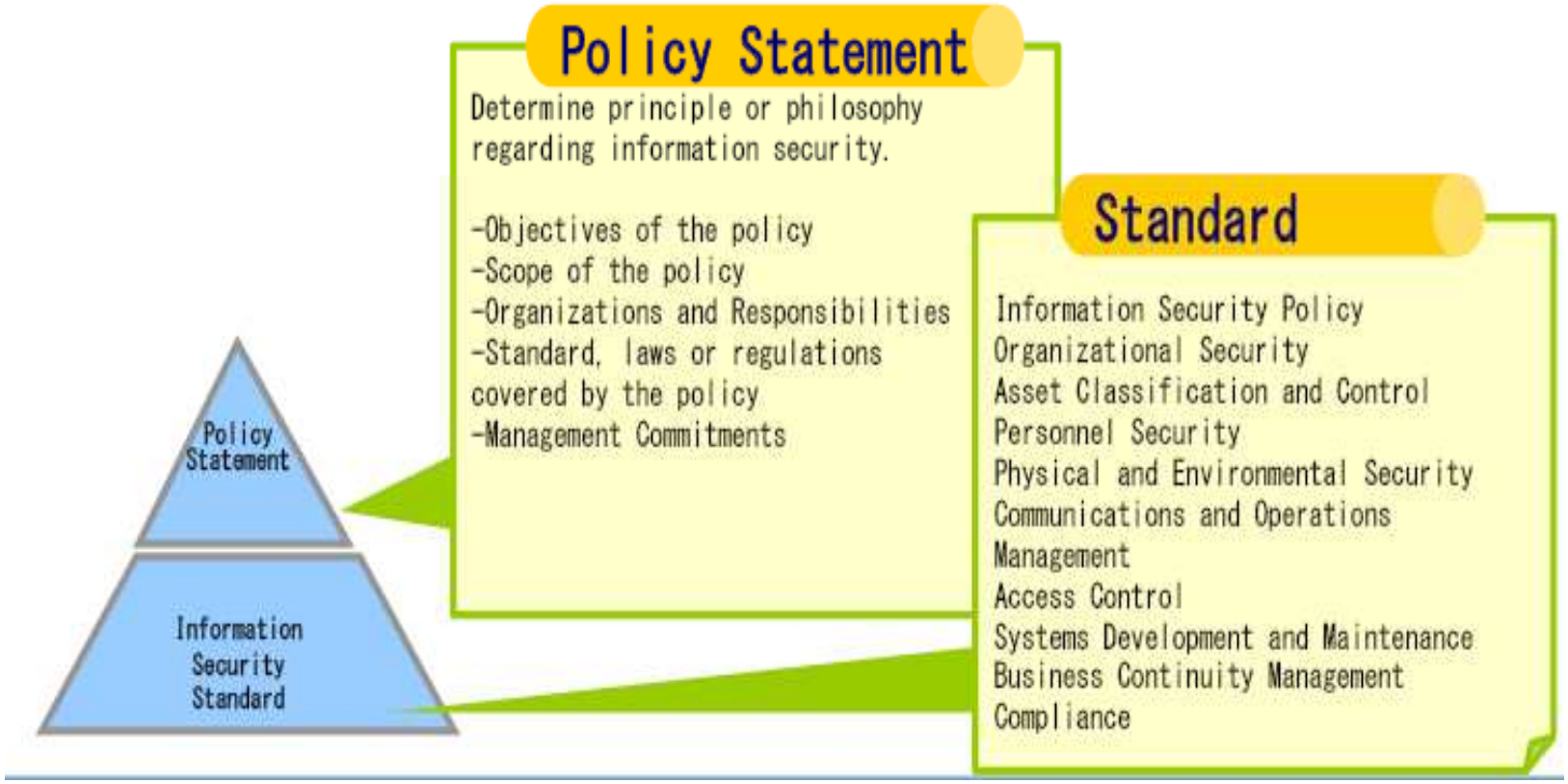
Security Proceed through

- ✓ Countermeasure Strategy
- ✓ Risk Analysis and Management Process
- ✓ Information Policy

Security Countermeasure Strategy

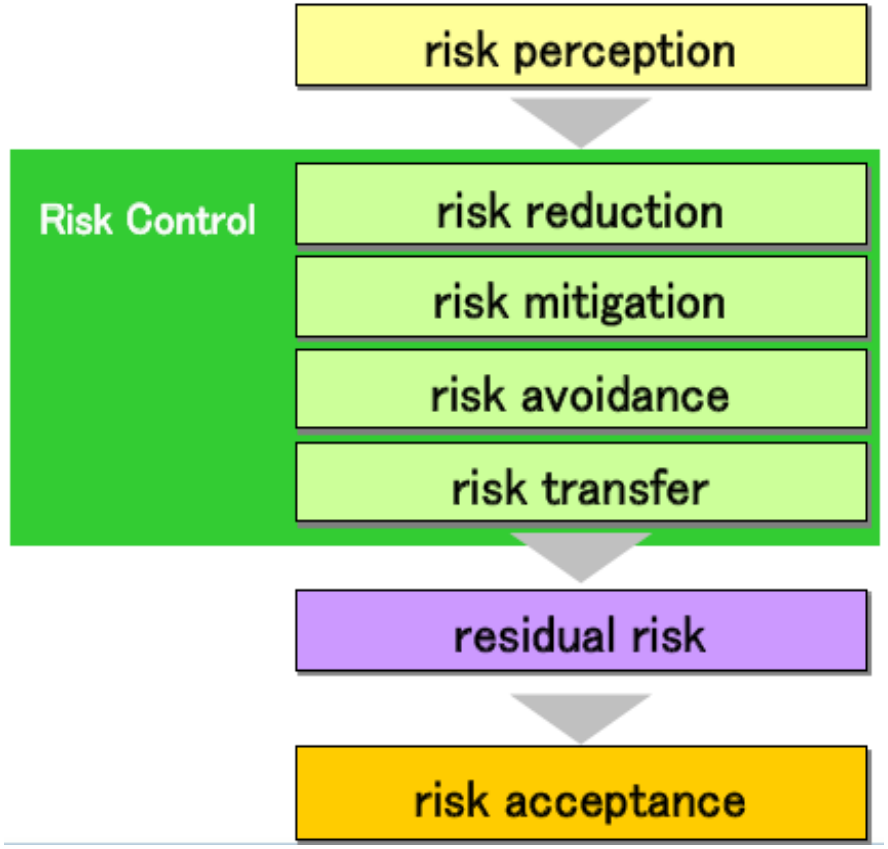
Strategy	Description	Implementation
Resistance	capability of a system to repel attacks	firewall, recognition, access control, cryptography etc.
Recognition	capability to detect attacks as they occur and to evaluate the extent of damage and compromise	Intrusion Detection System, audit trail analysis, integrity check etc.
Recovery	capability to maintain essential services and assets during attack, limit the extent of damage, and restore full services following attack	Back up and recovery, Incident Response etc.

Information Security Policy



Risk Management

Risk management is the identification, assessment, and prioritization of risks



Assets Analysis

Identification of Assets

- ✓ Hardware (Servers, Network Equipment)
- ✓ Software
- ✓ Data
- ✓ People
- ✓ Documentation
- ✓ Supplies

Classification of Asset Values

- ✓ High
- ✓ Mid
- ✓ Low

Definition of Responsibility for the Assets

Asset	Value	Owner
Accounting Data	High	A
Config Data	Mid	B
Marketing Data	High	C
Customer Data	High	A
Router	Mid	A
Hub	Low	B
Web Server	High	D
...	...	...

Risk analysis

It a systematic use of information to identify sources and to estimate the risk

Risk Analysis Approaches

- ✓ Baseline Approaches
- ✓ Informal Approaches
- ✓ Detailed Risk Analysis
- ✓ Combined Approaches

Threat Analysis

- ✓ Network Intrusion
- ✓ Malware
- ✓ Power Outage
- ✓ Theft
- ✓ Insider Abuse
- ✓ Earthquake

Classification

Threat	Level
Network Intrusion	MID
Malware	HIGH
Power Outage	MID
Theft	MID
Insider Abuse	MID
Earthquake	LOW
Missoperation	MID
...	...

Vulnerability Analysis

- ✓ Mis-configuration
- ✓ Un-patched software
- ✓ Inappropriate access control
- ✓ Physical weakness of facility

Vulnerability	Level	Threat
Misconfiguration	MID	Network Intrusion
Unpatched Software	HIGH	Malware
Inappropriate access control	MID	Network Intrusion
		Insider Abuse
Physical weakness	MID	Theft
		Earthquake
Weak password	MID	Network Intrusion
...	...	...

Risk Analysis

Asset	Class	Threat	Level	Vulnerability	Level	Control
Accounting Data	Top Secret	Insider abuse	MID	Misconfiguration	MID	Auditing
Configuration Data	Top Secret	Network Intrusion	MID	Bad access control	MID	Auditing
Web Server	Important	Network Intrusion	MID	Misconfiguration	MID	Auditing
Router	Important	Earthquake	LOW	Physical weakness	MID	Backup
e-mail message	Secret	Network Intrusion	MID	Weak password	MID	Log monitoring
...	...	...	...	...	...	...

Residual Risk Analysis

- ✓ Defined the acceptable

	Threat								
	Low			Mid			High		
	Vulnerability								
Asset Value	Low	Mid	High	Low	Mid	High	Low	Mid	High
Low	LLL	LLM	LLH	LML	LMM	LMH	LHL	LHM	LHH
Mid	MLL	MLM	MLH	MML	MMM	MMH	MHL	MHM	MHH
High	HLL	HLM	HLH	HML	HMM	HMM	HHL	HHM	HHH

... Acceptable Risk

... Unacceptable Risk (Require some control measure to reduce the risk)