

Information Security Risk Management

Based on

ISO/IEC 17799

Houman Sadeghi Kaji

Spread Spectrum Communication System PhD. ,

Cisco Certified Network Professional Security Specialist

BS7799 LA

info@houmankaji.net



Target Audience

This session is primarily intended for:

- Systems architects and planners
- Members of the information security team
- Security and IT auditors
- Senior executives, business analysts, and business decision makers
- Consultants and partners

Motivation for this Presentation

- Security is a **process**, not a product. Security products will not save you.
- **Process** is composed of technology, people, and tools. This is important because processes involve time and interaction between entities and many of the hard problems in security stem from this inherent interaction.

What is a risk (generic)

- A definable event
- Probability of Occurrence
- Consequence (impact) of occurrence

- A risk is not a problem A problem is a risk whose time has come

Identifying Security Risk Management Prerequisites



- Security Risk Management Concepts
- Identifying Security Risk Management Prerequisites
- Assessing Risk
- Conducting Decision Support
- Implementing Controls and Measuring Program Effectiveness

- Risk Analysis is a method of identifying and assessing the possible damage that could be caused in order to justify security safeguards.
- Two types of risk analysis:
 - **Quantitative** – attempts to assign real numbers to the costs of safeguards and the amount of damage that can take place
 - **Qualitative** – An analysis that judges an organization's risk to threats, which is based on judgment, intuition, and the experience versus assigning real numbers to these possible risks and their potential loss

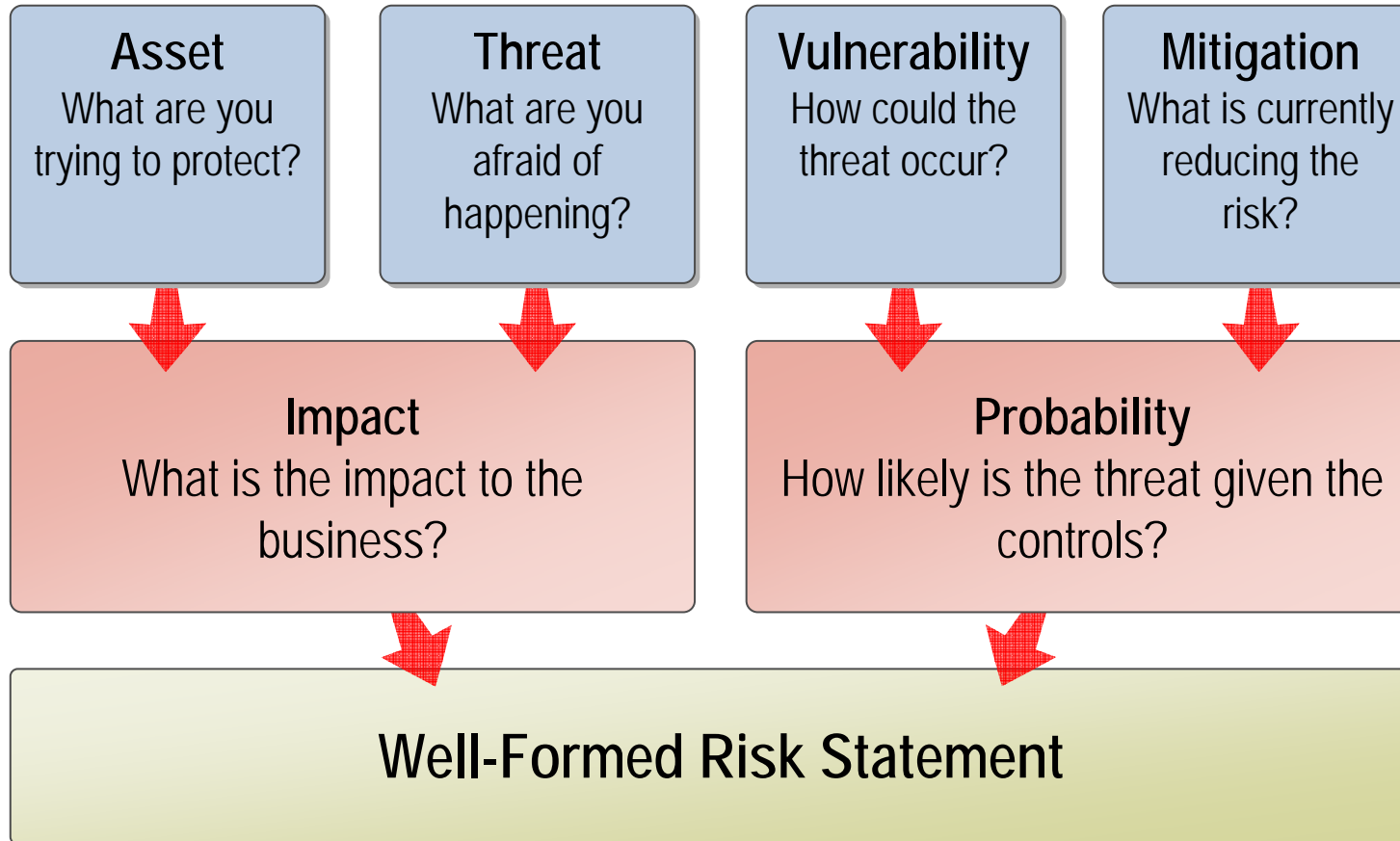


Risk Management vs. Risk Assessment

	Risk Management	Risk Assessment
Goal	<ul style="list-style-type: none">• Manage risks across business to acceptable level	<ul style="list-style-type: none">• Identify and prioritize risks
Cycle	<ul style="list-style-type: none">• Overall program across all four phases	<ul style="list-style-type: none">• Single phase of risk management program
Schedule	<ul style="list-style-type: none">• Scheduled activity	<ul style="list-style-type: none">• Continuous activity
Alignment	<ul style="list-style-type: none">• Aligned with budgeting cycles	<ul style="list-style-type: none">• Not applicable



Communicating Risk



Determining Your Organization's Risk Management Maturity Level



Publications to help you determine your organization's risk management maturity level include:

National Institute of Standards and Technology

Security Self-Assessment Guide for Information Technology Systems (SP-800-26)

IT Governance Institute

Control Objectives for Information and Related Technology (CobiT)

International Standards Organization

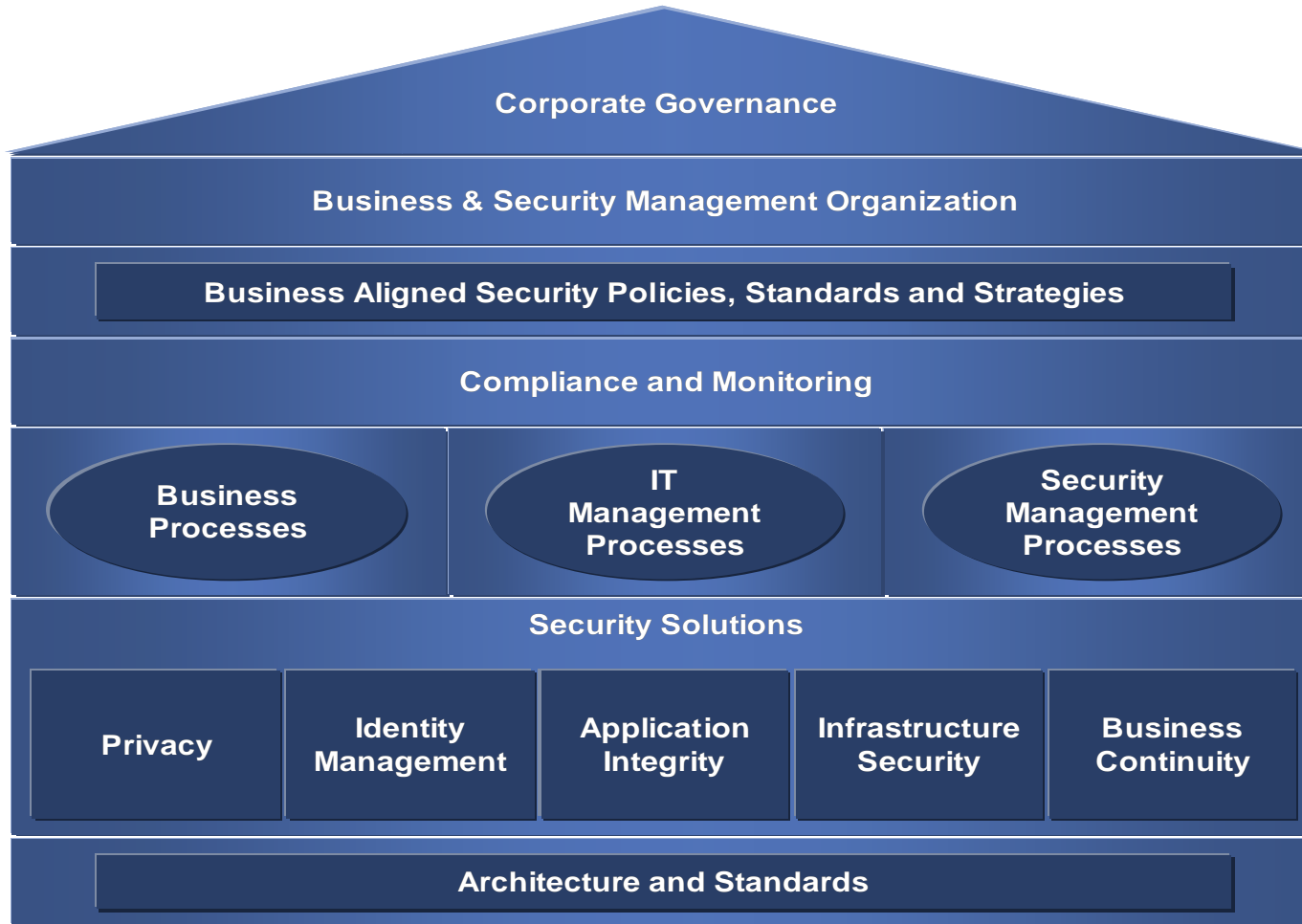
ISO Code of Practice for Information Security Management (ISO 17799)

Performing a Risk Management Maturity Self-Assessment

Level	State
0	Non-existent
1	Ad hoc
2	Repeatable
3	Defined process
4	Managed
5	Optimized



Enterprise Security Architecture Model



Defining Roles and Responsibilities

