

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

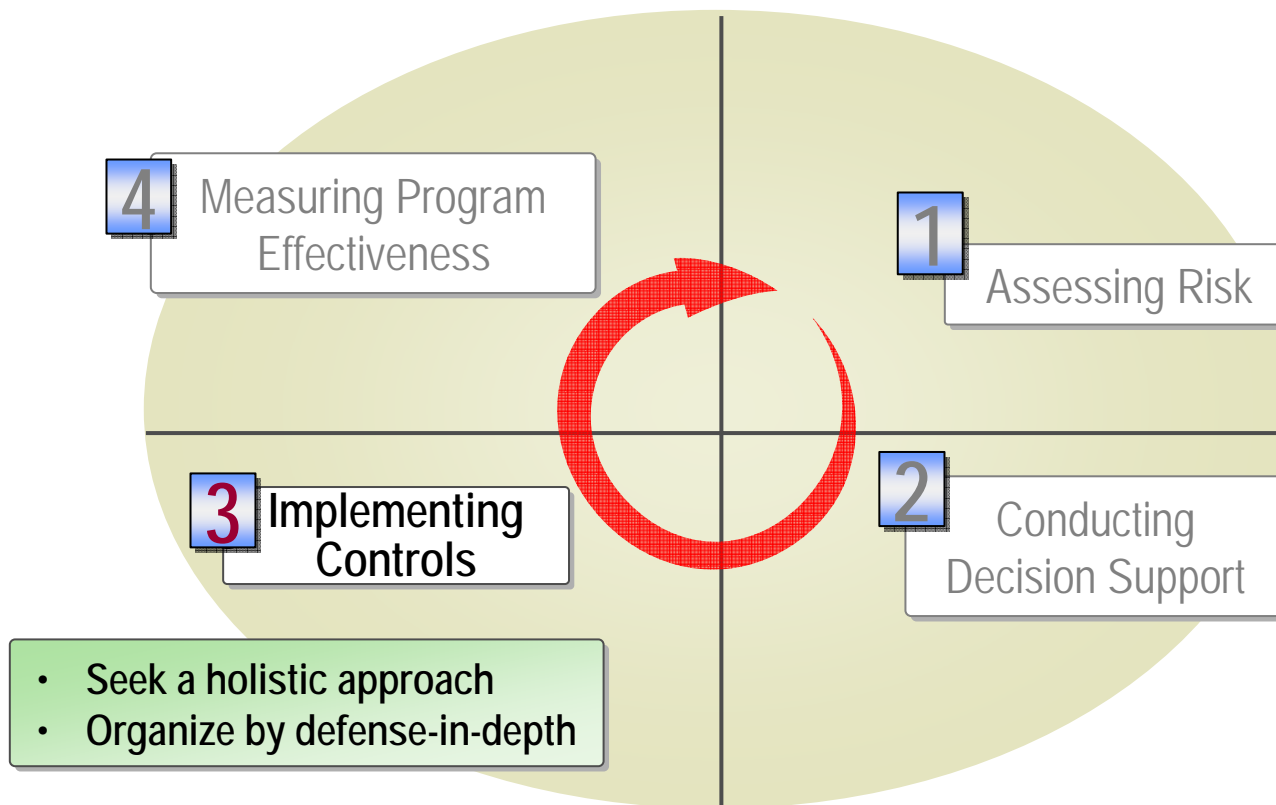
- A risk is not a problem A problem is a risk whose time has come

Implementing Controls and Measuring Program Effectiveness



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

Implementing Controls

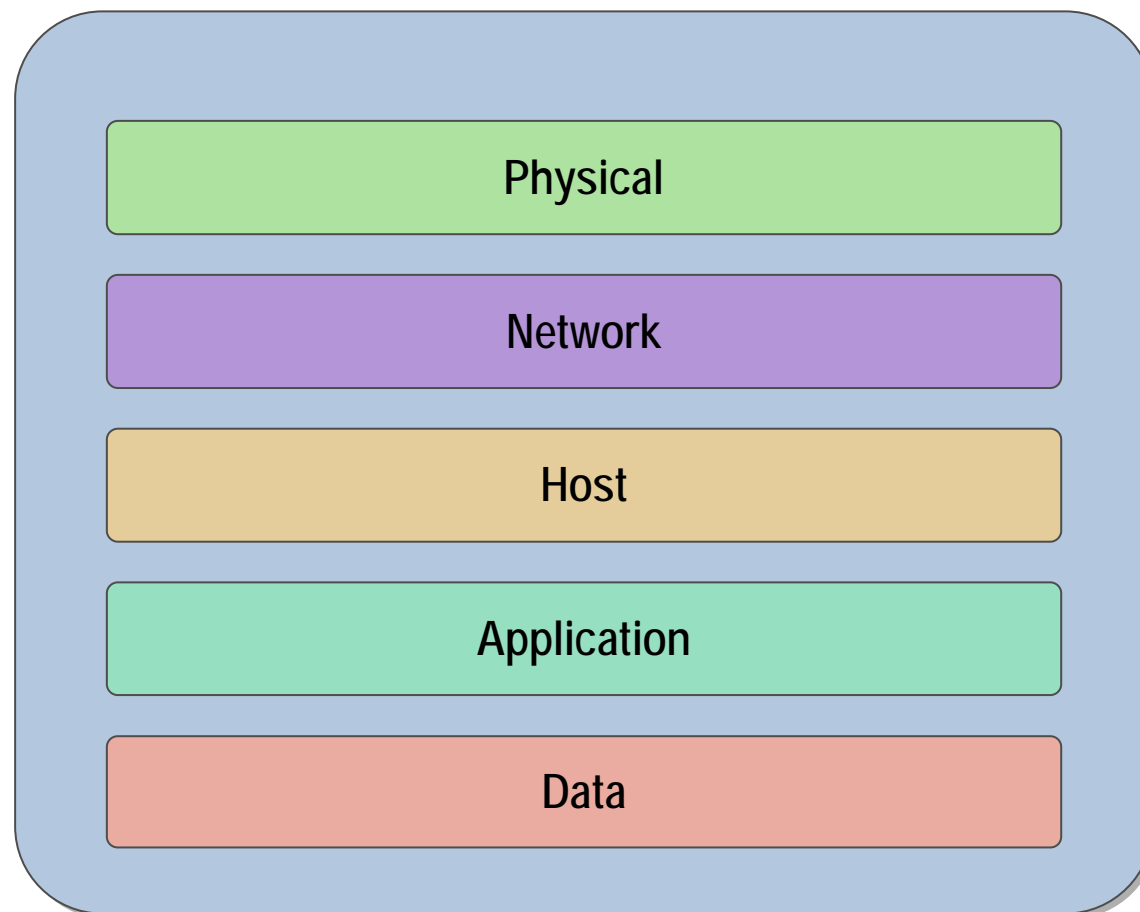


Organizing the Control Solutions

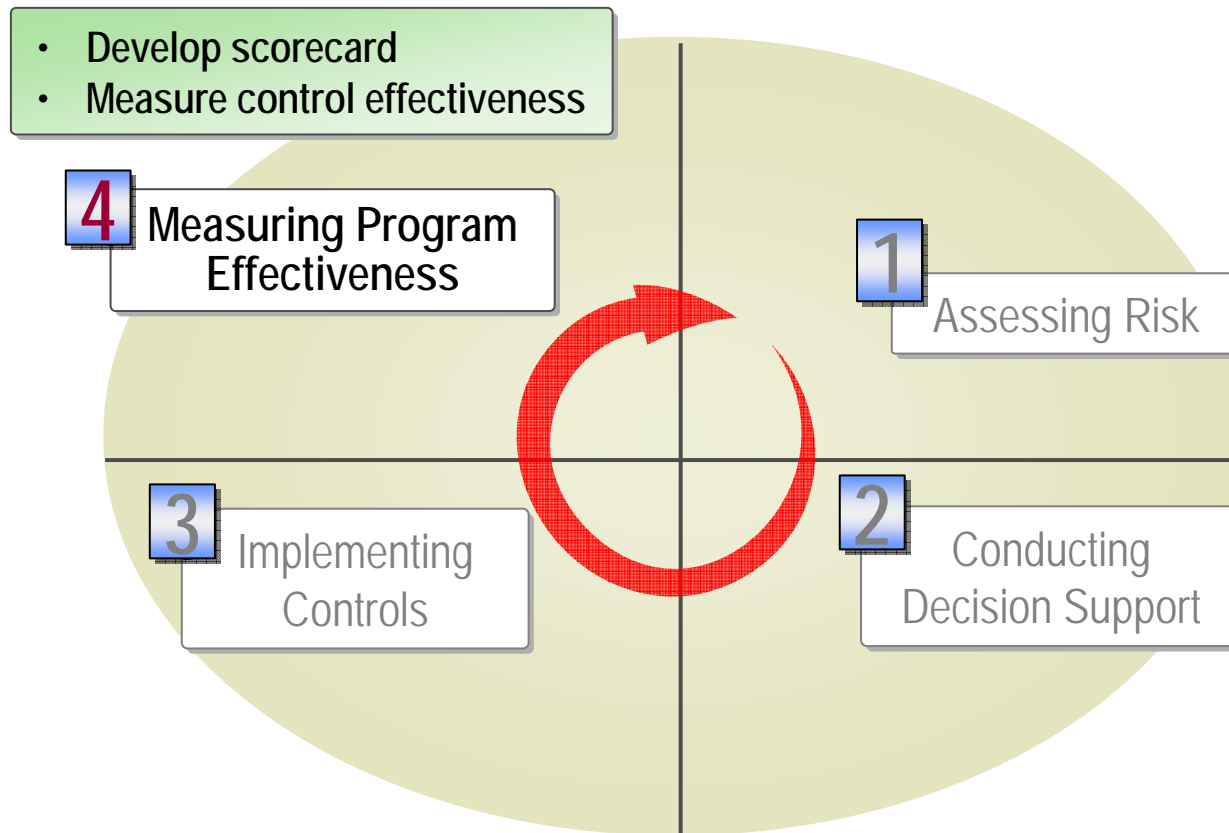
Critical success determinants to organizing control solutions include:

- ✓ Communication
- ✓ Team scheduling
- ✓ Resource requirements

Organizing by Defense-in-Depth



Measuring Program Effectiveness



Developing Your Organization's Security Risk Scorecard



A simple security risk scorecard organized by the defense-in-depth layers might look like this:

	FY05 Q1	FY05 Q2	FY05 Q3	FY05 Q4
Physical	H	M		
Network	M	M		
Host	M	M		
Application	M	H		
Data	L	L		
Risk Levels (H, M, L)				

Methods to measure the effectiveness of implemented controls include:

- ✓ Direct testing
- ✓ Submitting periodic compliance reports
- ✓ Evaluating widespread security incidents