

# 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

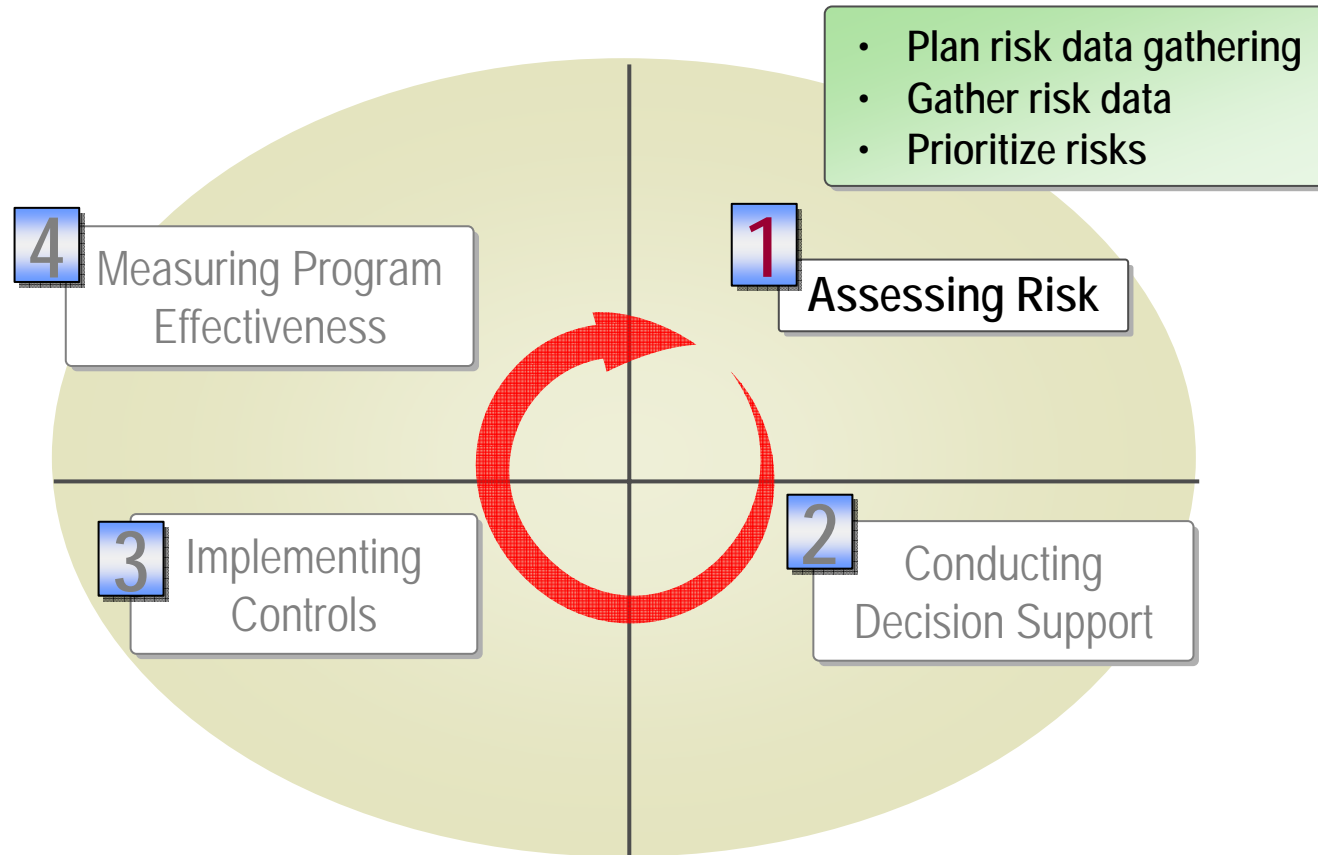
- Security is a **process**, not a product. Security products will not save you.
- **Process** is composed of technology, people, and tools. This is important because processes involve time and interaction between entities and many of the hard problems in security stem from this inherent interaction.

# 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

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

# Overview of the Assessing Risk Phase



# Understanding the Planning Step

The primary tasks in the planning step include the following:

- Alignment
- Scoping
- Stakeholder acceptance
- Setting expectations

# Understanding Facilitated Data Gathering

Elements collected during facilitated data gathering include:

- Organizational assets
- Asset description
- Security threats
- Vulnerabilities
- Current control environment
- Proposed controls

Keys to successful data gathering include:

- Meet collaboratively with stakeholders
- Build support
- Understand the difference between discussing and interrogating
- Build goodwill
- Be prepared

# Identifying and Classifying Assets

An asset is anything of value to the organization and can be classified as one of the following:

- ✓ High business impact
- ✓ Moderate business impact
- ✓ Low business impact

Use the following questions as an agenda during facilitated discussions:

- What asset are you protecting?
- How valuable is the asset to the organization?
- What are you trying to avoid happening to the asset?
- How might loss or exposures occur?
- What is the extent of potential exposure to the asset?
- What are you doing today to reduce the probability or the extent of damage to the asset?
- What are some actions that you can take to reduce the probability in the future?

# Estimating Asset Exposure

Exposure: The extent of potential damage to an asset

Use the following guidelines to estimate asset exposure:

High  
exposure

Severe or complete loss of the asset

Medium  
exposure

Limited or moderate loss

Low  
exposure

Minor or no loss

# Estimating Probability of Threats

Use the following guidelines to estimate probability for each threat and vulnerability identified:

High threat

Likely—one or more impacts expected within one year

Medium threat

Probable—impact expected within two to three years

Low threat

Not probable—impact not expected to occur within three years

The facilitated risk discussion meeting is divided into the following sections:

- 1 Determining Organizational Assets and Scenarios
- 2 Identifying Threats
- 3 Identifying Vulnerabilities
- 4 Estimating Asset Exposure
- 5 Estimating Probability of Exploit and Identifying Existing Controls
- 6 Meeting Summary and Next Steps

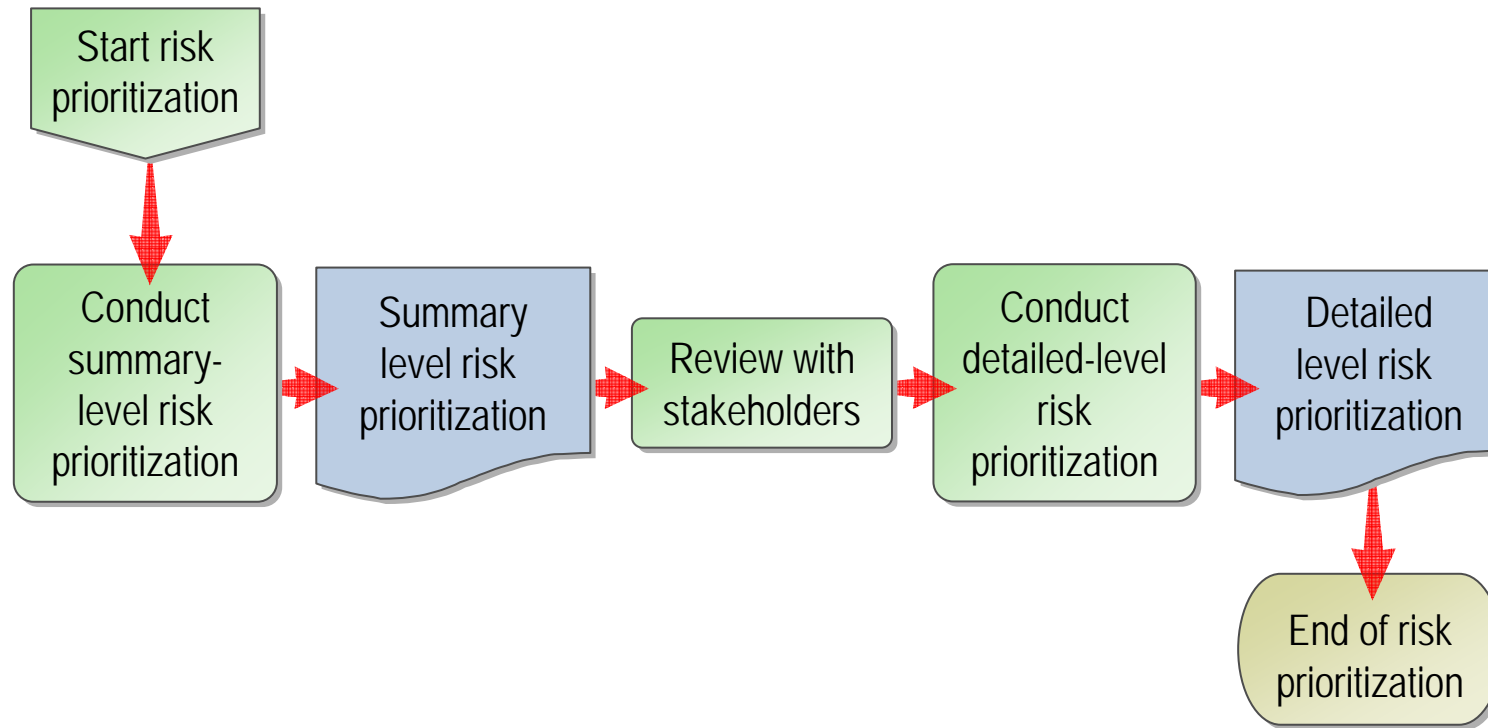
# Defining Impact Statements

Impact data includes the following information:

Information collected during Data Gathering process

Asset				Exposure			
Date Identified	Asset Name/Desc.	Asset Class	Applicable DiD Layer(s)	Threat Description	Vulnerability Description	Exposure Rating (H,M,L)	Impact Rating (H,M,L)

# Understanding Risk Prioritization



# Conducting Summary-Level Risk Prioritization

**1**

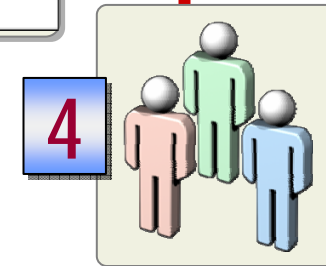
Asset Class	High	Moderate	High	High
	Med	Low	Moderate	High
Low	Low	Low	Moderate	
		Low	Medium	High
		Exposure Level		

**3**

Impact (from Impact Table above)	High	Moderate	High	High
	Med	Low	Moderate	High
Low	Low	Low	Moderate	
		Low	Medium	High
		Probability Value		

**2**

**High.** Likely—one or more impacts expected within one year  
**Medium.** Probable—impact expected within two to three years  
**Low.** Not probable—impact not expected to occur within three years



The summary-level prioritization process includes the following:

- 1** Determine impact level
- 2** Estimate summary-level probability
- 3** Complete the summary-level risk list
- 4** Review with stakeholders

# Conducting Detailed Level Risk Prioritization

The following four tasks outline the process to build a detailed-level list of risks:

**1** Determine impact and exposure

**2** Identify current controls

**3** Determine probability of impact

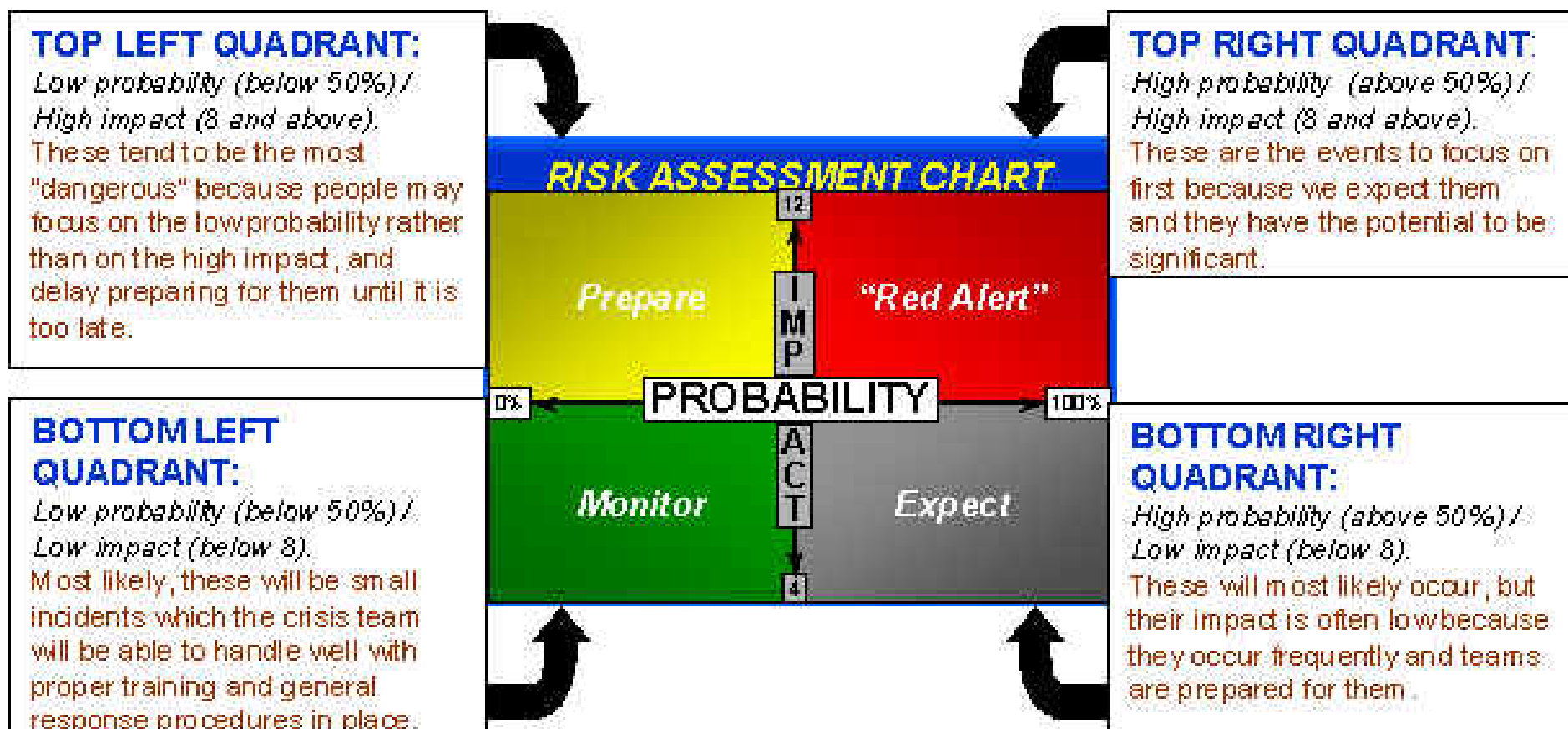
**4** Determine detailed risk level

Use the Detailed-Level Risk Prioritization template (SRJA3-Detailed Level Risk Prioritization.xls)

The following tasks outline the process to determine the quantitative value:

- 1 Assign a monetary value to each asset class
- 2 Input the asset value for each risk
- 3 Produce the single-loss expectancy value (SLE)
- 4 Determine the annual rate of occurrence (ARO)
- 5 Determine the annual loss expectancy (ALE)

# Qualitative Risks Matrix



# Assessing Risk: Best Practices

- ✓ Analyze risks during the data gathering process
- ✓ Conduct research to build credibility for estimating probability
- ✓ Communicate risk in business terms
- ✓ Reconcile new risks with previous risks