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

Session Overview

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

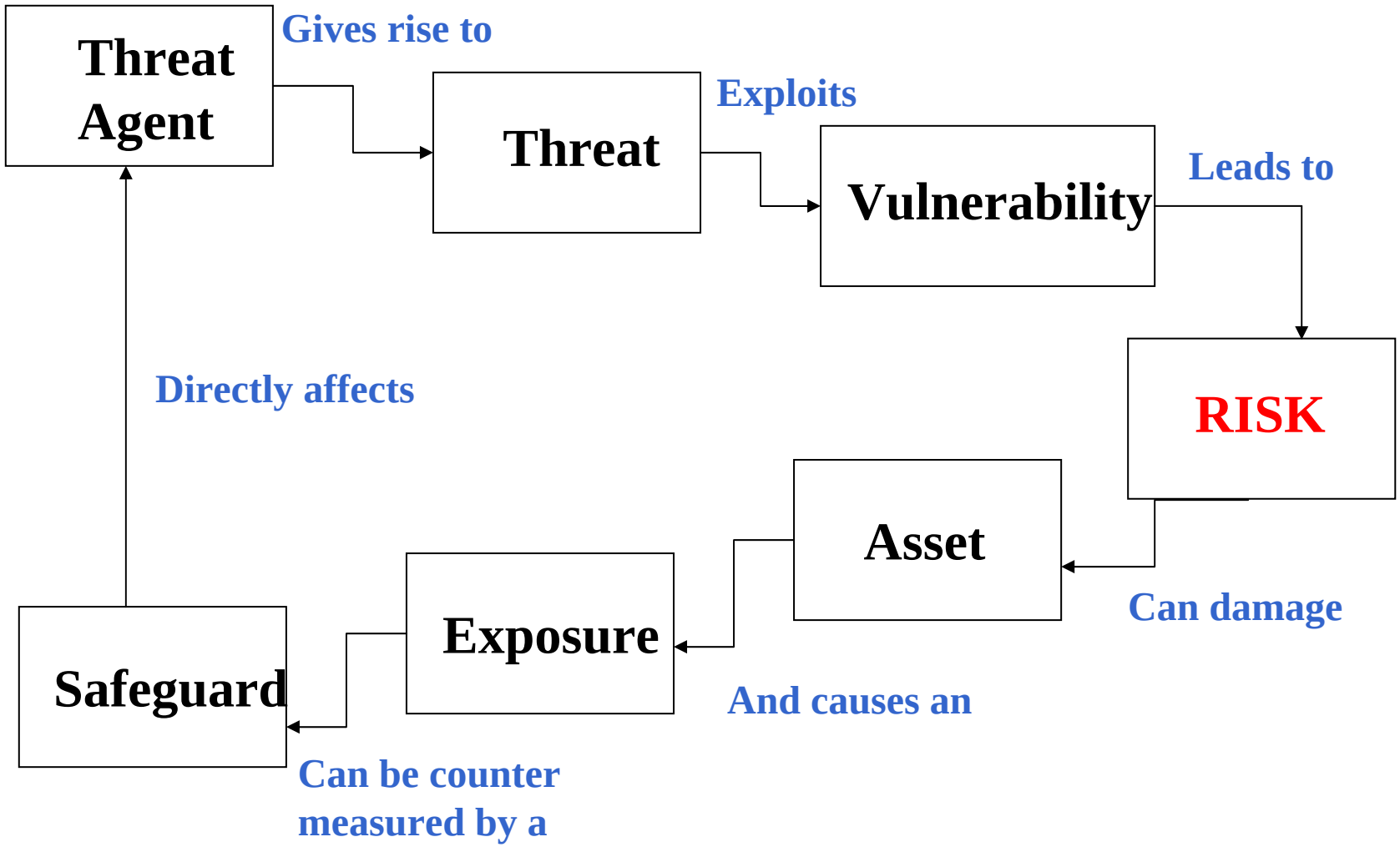
Security Risk Management Concepts

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

What is a security risk

- Threat – is any potential danger to information, or systems (e.g. fire)
- Vulnerability – is a software, hardware, or procedural weakness that may provide an attacker the open door to enter a system. (e.g. lack of water)
- Risk – loss potential (probability) that a threat will exploit a vulnerability.

Relationship among different security components

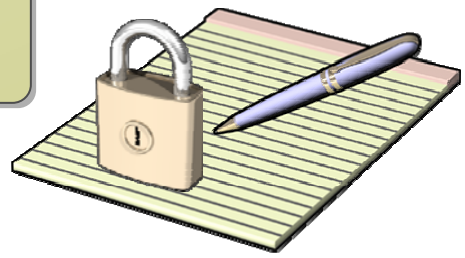


Why Develop a Security Risk Management Process?

Security risk management: A process for identifying, prioritizing, and managing risk to an acceptable level within the organization

Developing a formal security risk management process can address the following:

- Threat response time
- Regulatory compliance
- Infrastructure management costs
- Risk prioritization and management



Two key questions being asked today

- How much information security is enough and how do I know?
- How do I get my organization to consistently follow our security policies?

Identifying Success Factors That Are Critical to Security Risk Management

Key factors to implementing a successful security risk management program include:

- ✓ Executive sponsorship
- ✓ Well-defined list of risk management stakeholders
- ✓ Organizational maturity in terms of risk management
- ✓ An atmosphere of open communication and teamwork
- ✓ A holistic view of the organization
- ✓ Security risk management team authority

Comparing Approaches to Risk Management

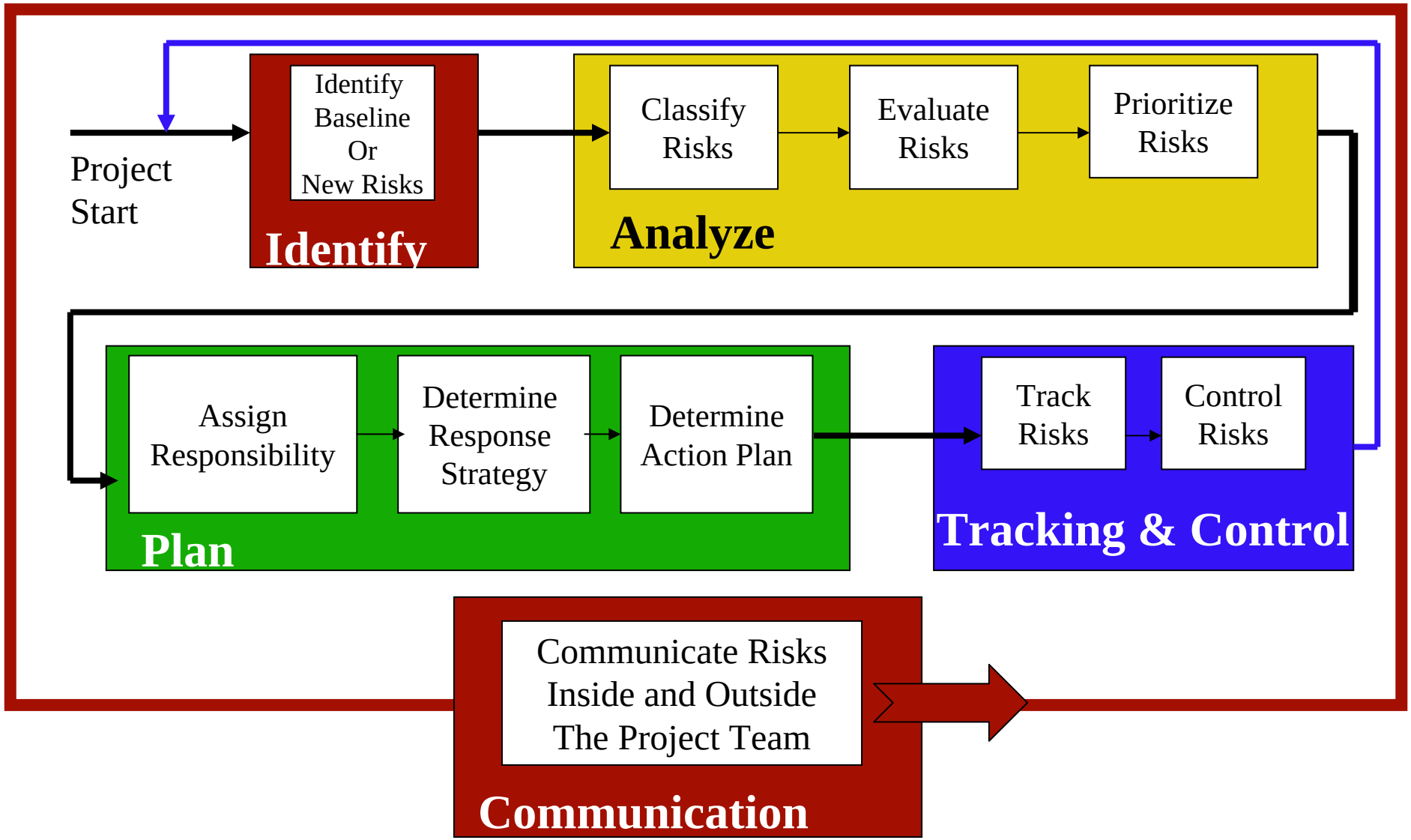
Many organizations have approached security risk management by adopting the following:

Reactive approach	A process that responds to security events as they occur
Proactive approach	The adoption of a process that reduces the risk of new vulnerabilities in your organization

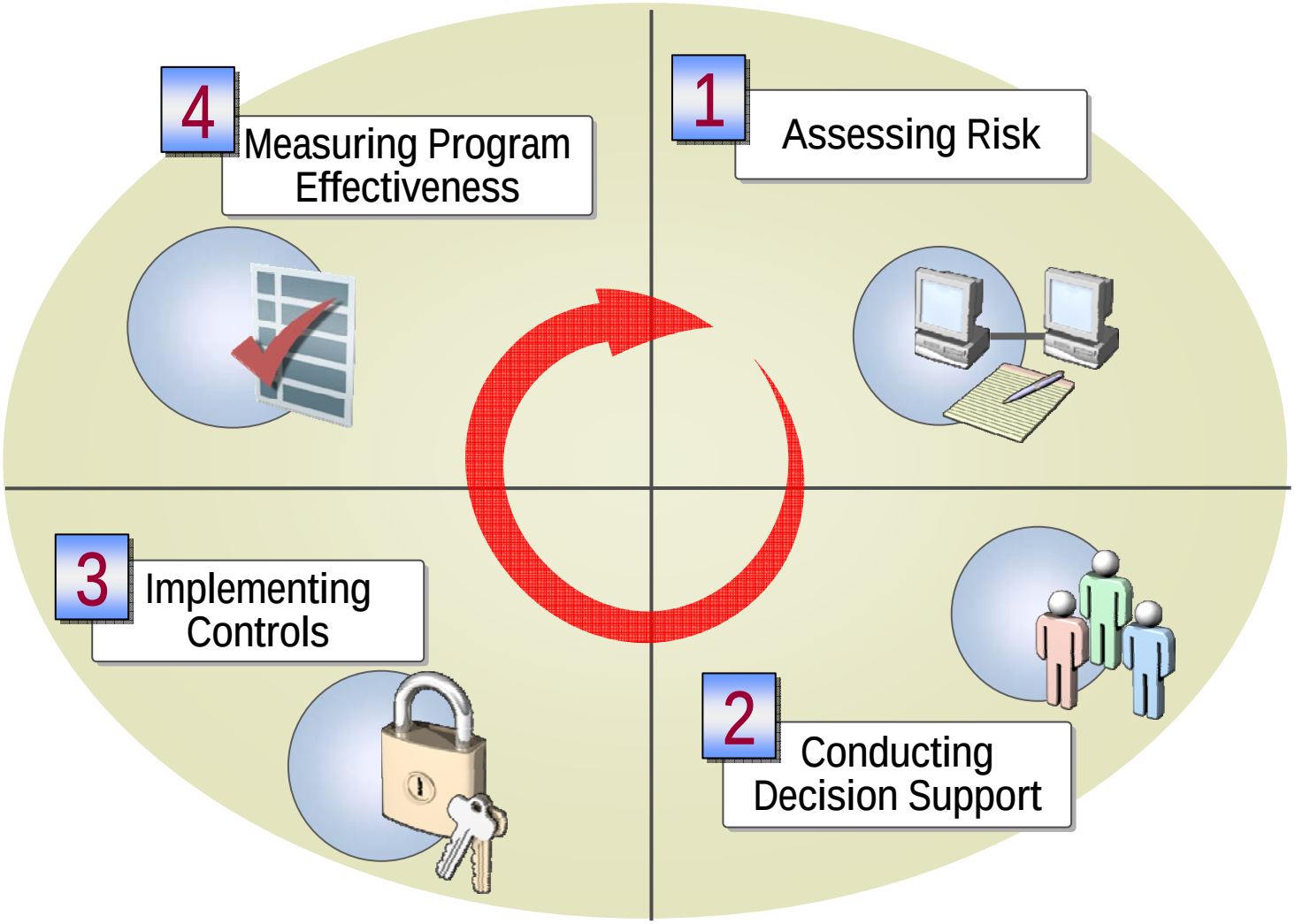
Comparing Approaches to Risk Prioritization

Approach	Benefits	Drawbacks
Quantitative	• **Risks prioritized by financial impact; assets prioritized by their financial values** • **Results facilitate management of risk by return on security investment** • **Results can be expressed in management-specific terminology**	• **Impact values assigned to risks are based upon subjective opinions of the participants** • **Very time-consuming** • **Can be extremely costly**
Qualitative	• **Enables visibility and understanding of risk ranking** • **Easier to reach consensus** • **Not necessary to quantify threat frequency** • **Not necessary to determine financial values of assets**	• **Insufficient granularity between important risks** • **Difficult to justify investing in control as there is no basis for a cost-benefit analysis** • **Results dependent upon the quality of the risk management team that is created**

Generic Security Risk Management Methodology



Introducing the Security Risk Management Process



Requirements continue to change …

DIRECTOR - CFO - CIO

Different Perspectives