Carnegie Mellon
Software Engineering Institute

Pittsburgh, PA 15213-3890

Rethinking Risk Management

Christopher Alberts
Audrey Dorofee

Sponsored by the U.S. Department of Defense

HIPAA Data Security

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 establishes a standard of due care for data security in healthcare organizations.

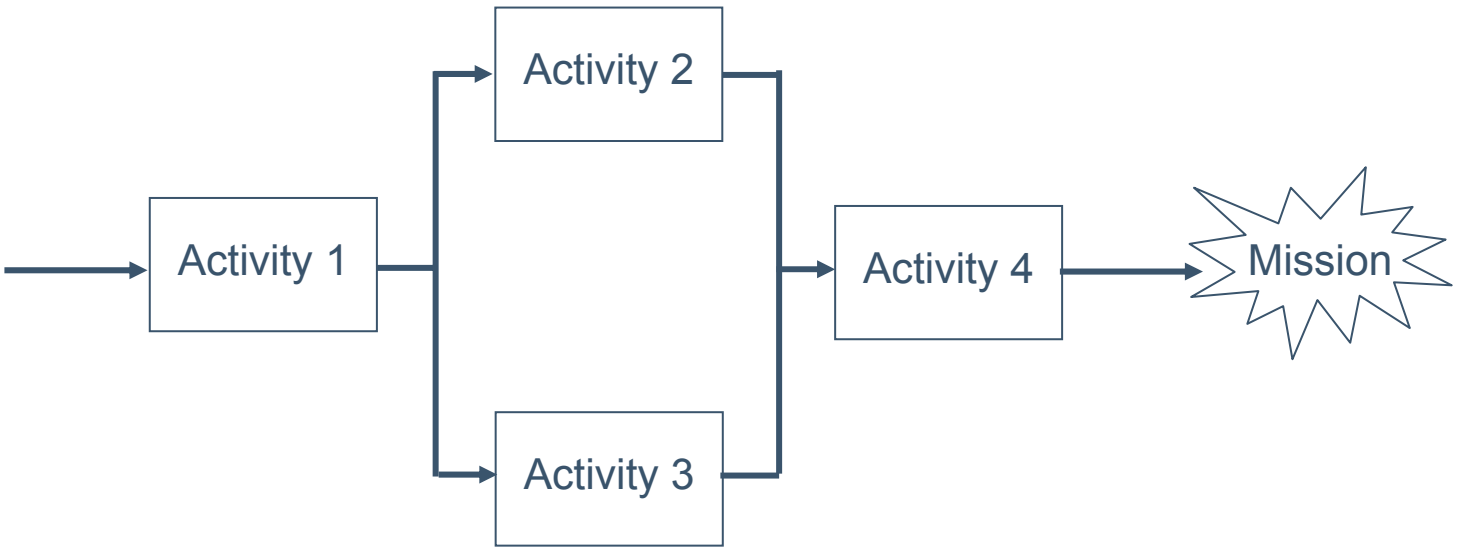
The regulation requires each healthcare organization to conduct a security risk assessment to ensure that its security program effectively mitigates its risk.

Key Questions

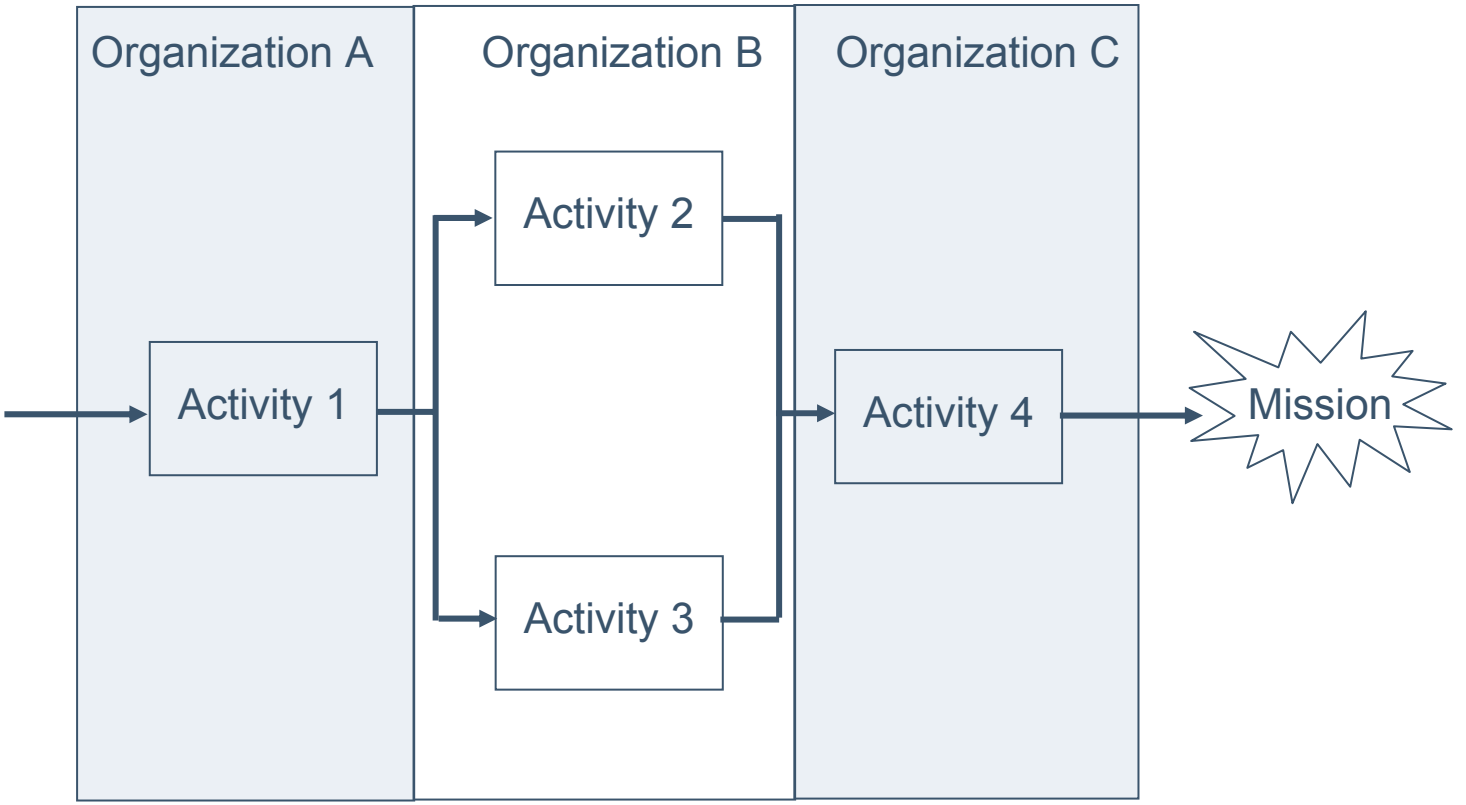
Do state-of-the-practice risk assessments accurately characterize the security risk confronting healthcare organizations?

Are some risks overlooked by state-of-the-practice risk assessments?

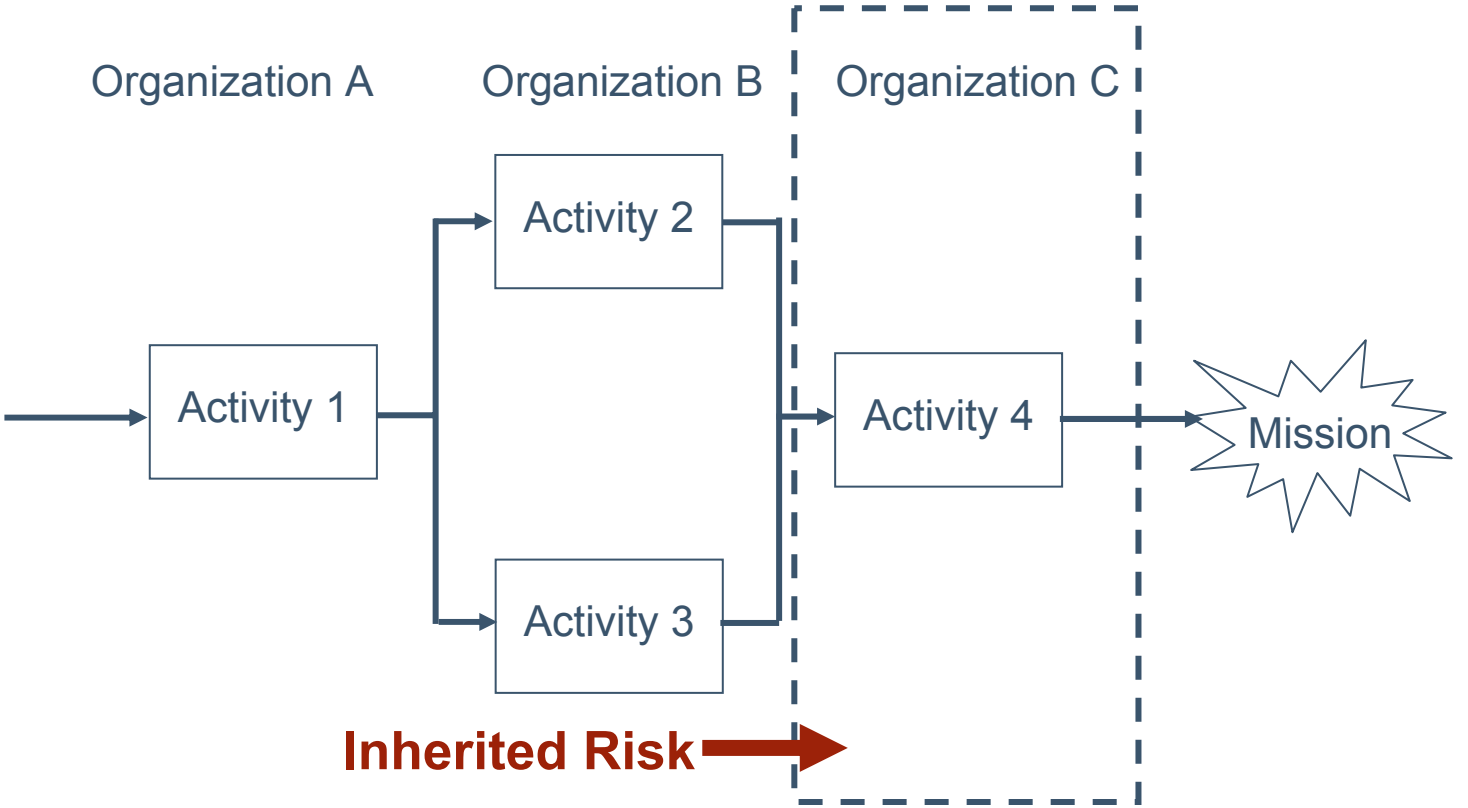
Example: Work Process



Example: Organizational Control



Example: Inherited Risk



Organization C's risk analysis only considers what happens within its organizational boundaries. However, risk is inherited from activities performed earlier in the process.

Current Reality

Outsourcing requires work products to move across organizational borders.

Distributed computing enables information to flow outside of defined system boundaries.

Current Risk Assessment Practices

State-of-the-practice risk assessments begin by drawing boundaries around the entity "being analyzed" (i.e., a technology or an organization).

These assessment techniques view risk as a static entity.

They cannot address the

- flow of work and information outside of artificially defined boundaries
- complex interrelationships among processes and technologies

The Dynamic Nature of Risk

Risk must be viewed as being dynamic in nature, moving with the workflow or the information flow.

Failure to account for the dynamic nature of risk precludes development of an accurate risk profile, because much of the risk is inherited from the surrounding environment.

Common Risk Assessment Deficiencies

The operational context is not sufficiently established.

Dependencies and interrelationships among risks and risk factors are not identified.

There is a tendency for local optimization of risk mitigation efforts.

- Only a subset of mission-related risk factors are examined at any given time.
- Inherited risk is not considered during the analysis.

What Is Needed

A risk analysis designed for the complexities of the modern business environment, where

- outsourcing of business processes are commonplace
- distributed technologies have become ubiquitous

Multi-Dimensional Risk Analysis

Defines a set of objects, rules, and heuristics used to model and analyze risk

Can be tailored to many different domains and many different types of risk

Focuses on assuring the completion of defined missions

Addresses common risk assessment deficiencies

Addressing the Deficiencies

An operational model with the following attributes is developed

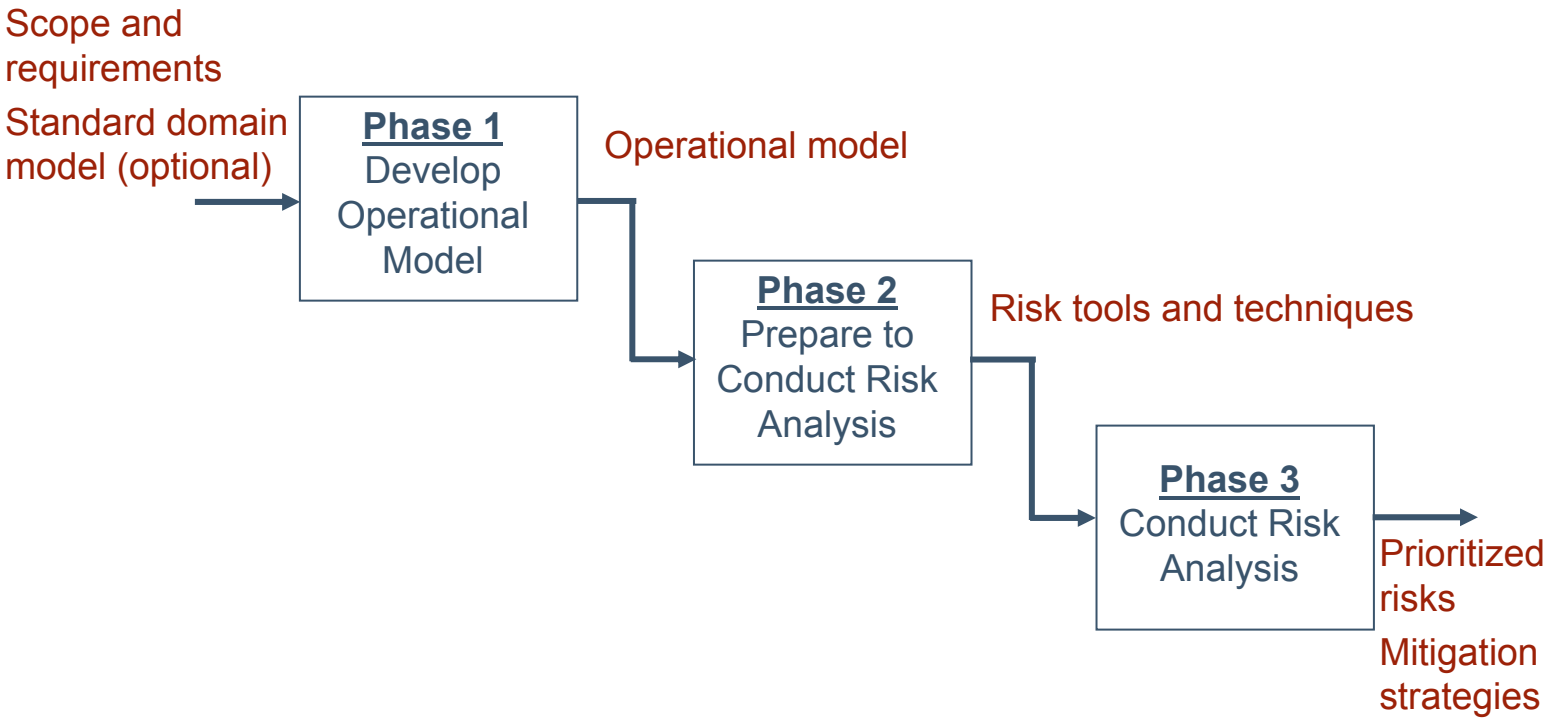
- flow of work or information
- sequencing of activities
- timing of activities

Risk factors are mapped to the operational model, enabling analysis of combinatorial effects among risk factors.

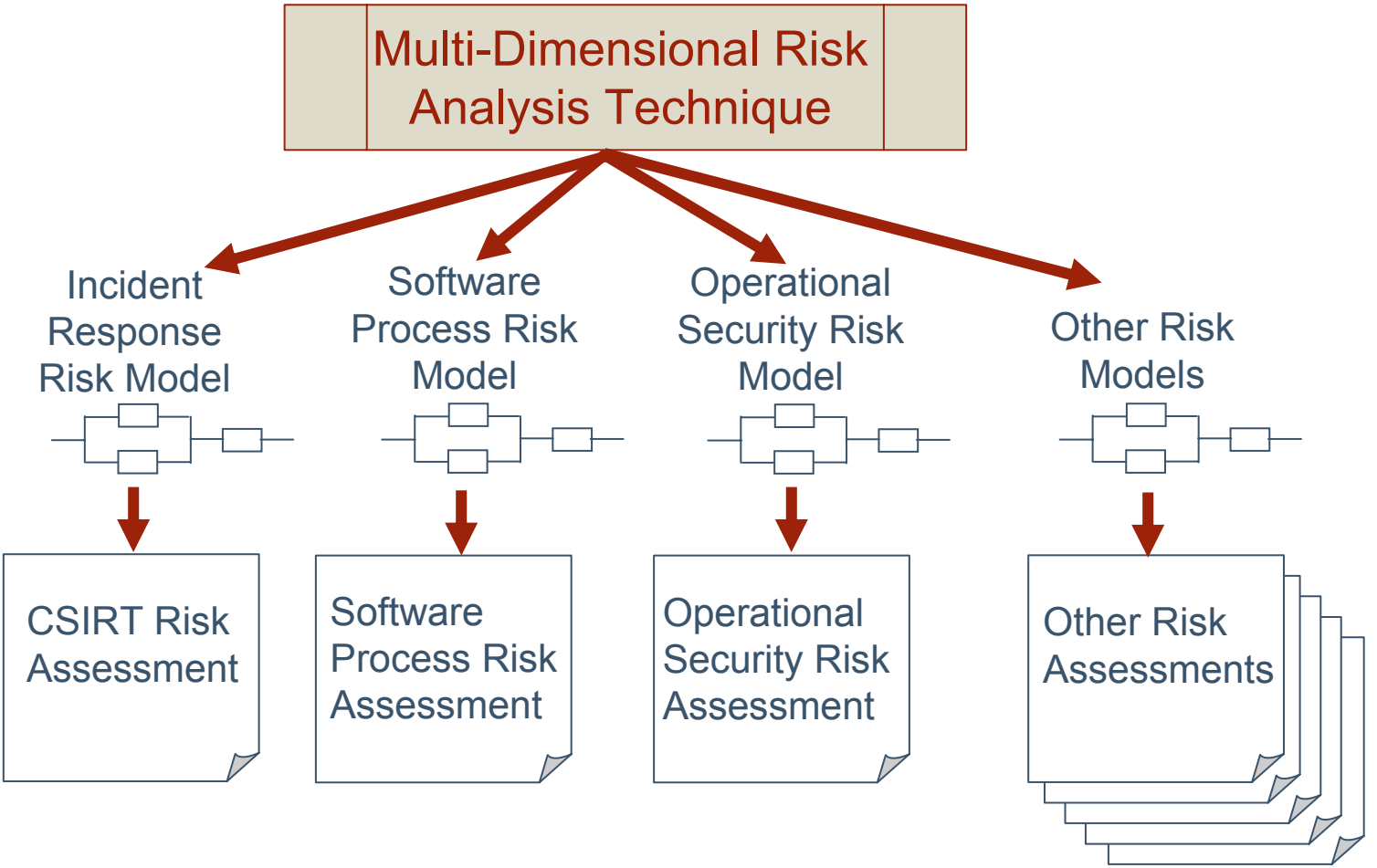
Risk reduction strategies are globally optimized.

- A range of mission-related risk factors are examined, providing a balanced view of risk.
- Inherited risk is integral to the analysis.

Multi-Dimensional Risk Analysis Framework



A Common Basis for Analyzing Risk



Four Dimensions of Risk

Mission Risk

Architecture Risk

Activity Risk

Event Risk

Depth of Analysis

Type I	Gap Analysis
Type II	Basic Risk Analysis
Type III	Advanced Risk Analysis
Type IV	Measured Risk Analysis

Why Focus on Incident Response?

1. Experience has shown that many organizations initially focus on incident response when developing a cyber-security capability.

2. An incident-response capability is a requirement of the HIPAA data security regulations.

3. An incident-response capability is typically distributed across multiple departments or organizations.

Project Status

First pilot analyzing risk to a CSIRT capability is underway.

- The operational model has been developed.
- Evaluations of CSIRT capabilities are beginning.

Currently looking for a second pilot in another domain.

- operational security risk (HIPAA risk assessment)
- software acquisition risk
- unique problems (e.g., risk in operating weapons systems, critical infrastructure risks)