

California  
**TECHNOLOGY AGENCY**  
Office of Information Security

# Risk Management Overview

# Risk Management

## ■ What is Risk Management?

*“Risk management is the process of taking actions to avoid or reduce risk to acceptable levels. This process includes both the identification and assessment of risk through risk analysis and the initiation and monitoring of appropriate practices in response to that analysis through the agency's risk management program.”* -- **SAM Section 5305**

# Risk Management

## ■ Okay :-) What is it really?

- In your Personal Risk profile
  - Life, health, safety, financial, etc.
- During the Project Life Cycle
  - Scope, cost, & schedule
- Information Security Risk
  - Threats
  - Vulnerabilities
  - Probability
  - Impact

# Risk Management

- First, you must have something of value:
  - Your life
  - Your family
  - Your job
  - A processing system that determines eligibility and issues checks or EBT cards
  - The Supreme Court building in Washington D. C.
  - The BLT sandwich you left in your car last week

# Risk Management

## Identification and Analysis

### Simply put:

You have some **thing** of value you wish to protect. You determine what **threats** exist that are related to this thing. You then determine if your thing is **vulnerable** to these threats. You determine the **probability** of that particular threat, can use that particular vulnerability, and cause harm. If harm does occur, what is the **impact**.

# Risk Management



## Controls and Remediation Planning

Now that you have this risk identified and measured, you prepare by developing plans to deal with the risk, both before and after something bad happens.

### Before:

Remediation planning and building defenses

Contingency planning

### After:

Execute the plans or accept the consequences

# Risk Management

## ■ Risk – EXAMPLE #1

You live in Topeka Kansas in a double-wide mobile home and it's early spring.

- Thing (asset)
- Threat
- Vulnerability
- Probability
- Impact
- Mitigation
- Contingency

# Risk Management

## ■ Risk – EXAMPLE #2

In late 2013, a \$3.8 billion, 1776 feet skyscraper is opened for business. Its address is - 1 World Trade Center, NY, NY.

- Thing (asset)
- Threat
- Vulnerability
- Probability
- Impact
- Mitigation
- Contingency

# Risk Management

## ■ Risk – EXAMPLE #2

The Revenue Department currently collects over 63% of the state's income. Over the past 6 years, the tax collection process has gone from 85% paper to nearly 73% electronic. Everyone agrees, "*There's no going back to paper.*"

- Thing (asset)
- Threat
- Vulnerability
- Probability
- Impact
- Mitigation
- Contingency

## SAM 5305-Risk Management

Risk management is the process of taking actions to avoid or reduce risk to acceptable levels. This process includes both the identification and assessment of risk through risk analysis (SAM Section 5305.1) and the initiation and monitoring of appropriate practices in response to that analysis through the agency's risk management program.

## SAM 5305.1 Risk Analysis

Risk analysis is an essential aspect of a risk management program. Risk analysis is a process (commonly referred to as a risk assessment) that identifies and assesses risks associated with information assets and defines a cost-effective approach to managing such risks. Specific risks that must be addressed include, but are not limited to; those associated with accidental and deliberate acts on the part of agency employees and outsiders; fire, flooding, and electric disturbances; and, loss of data communications capabilities.

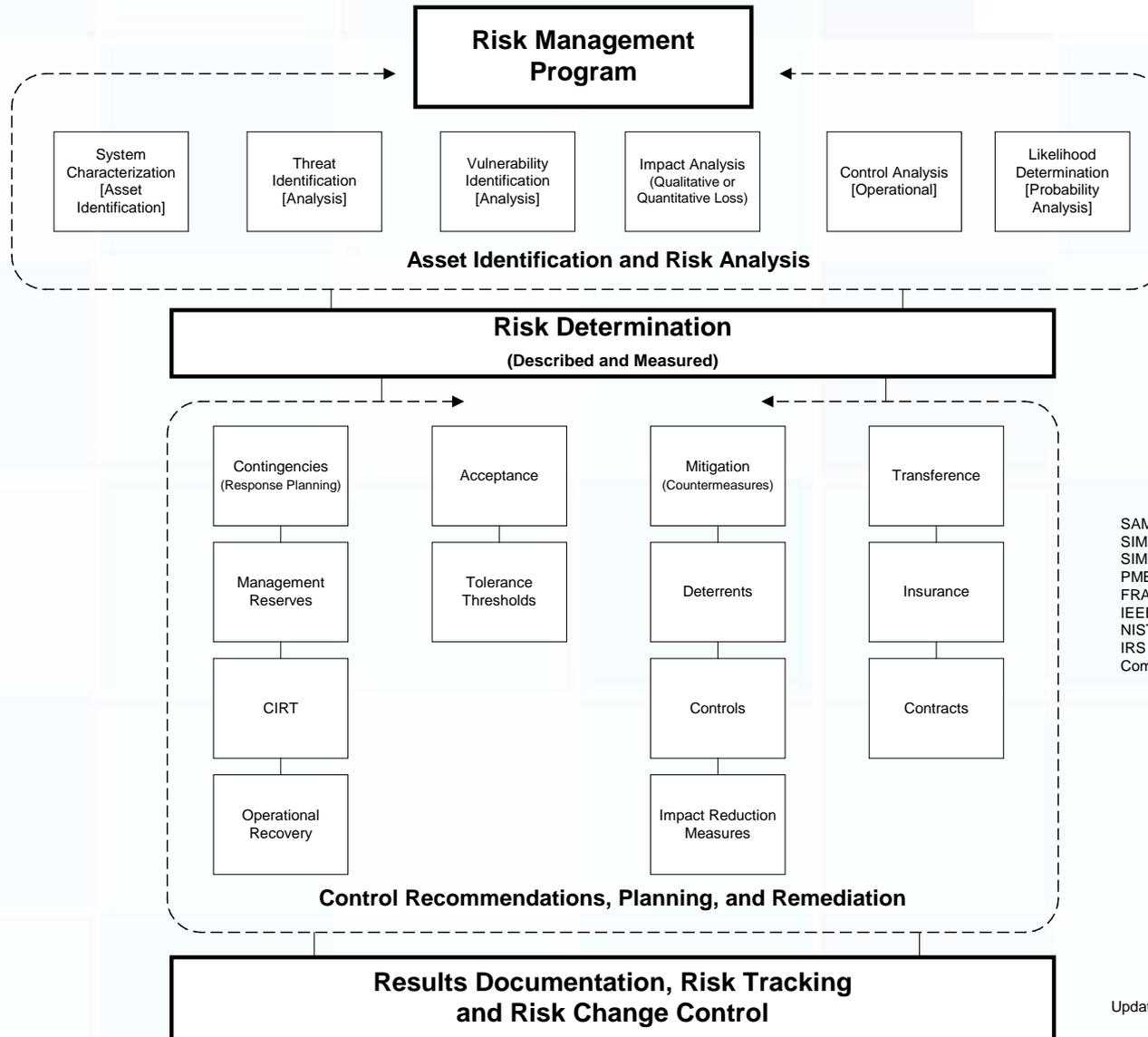
# Risk Assessment Toolkit



**INFORMATION SECURITY  
ASSESSMENT TOOL  
FOR STATE AGENCIES**

April 2008

# Risk Management



## SOURCES

SAM Section 4842  
 SIMM Section 70  
 SIMM Section 200  
 PMBOK Chapter 11  
 FRAP - Thomas Peltier  
 IEEE  
 NIST SP 800-30  
 IRS Pub. 1075, Sec. 5.6  
 Common Criteria

Update: December 22, 2003

# Risk Management steps that are shared by the Disaster Recovery function?



- Asset identification and valuation
- Impact analysis
- System Development Life Cycle
- Change Control
- Contingency Planning

# Questions?