Risk Management Program

An Introduction

Risk Management Program

Chris Hill

Acting Chief Information Security Officer

- Responsible for information security for entities operating under the Governor
- 64 Agencies, Boards and Commissions
- 50,000 state employees
- Compliance including FTI, HIPAA, PCI, CJIS, more

Risk Management Program

Risk:

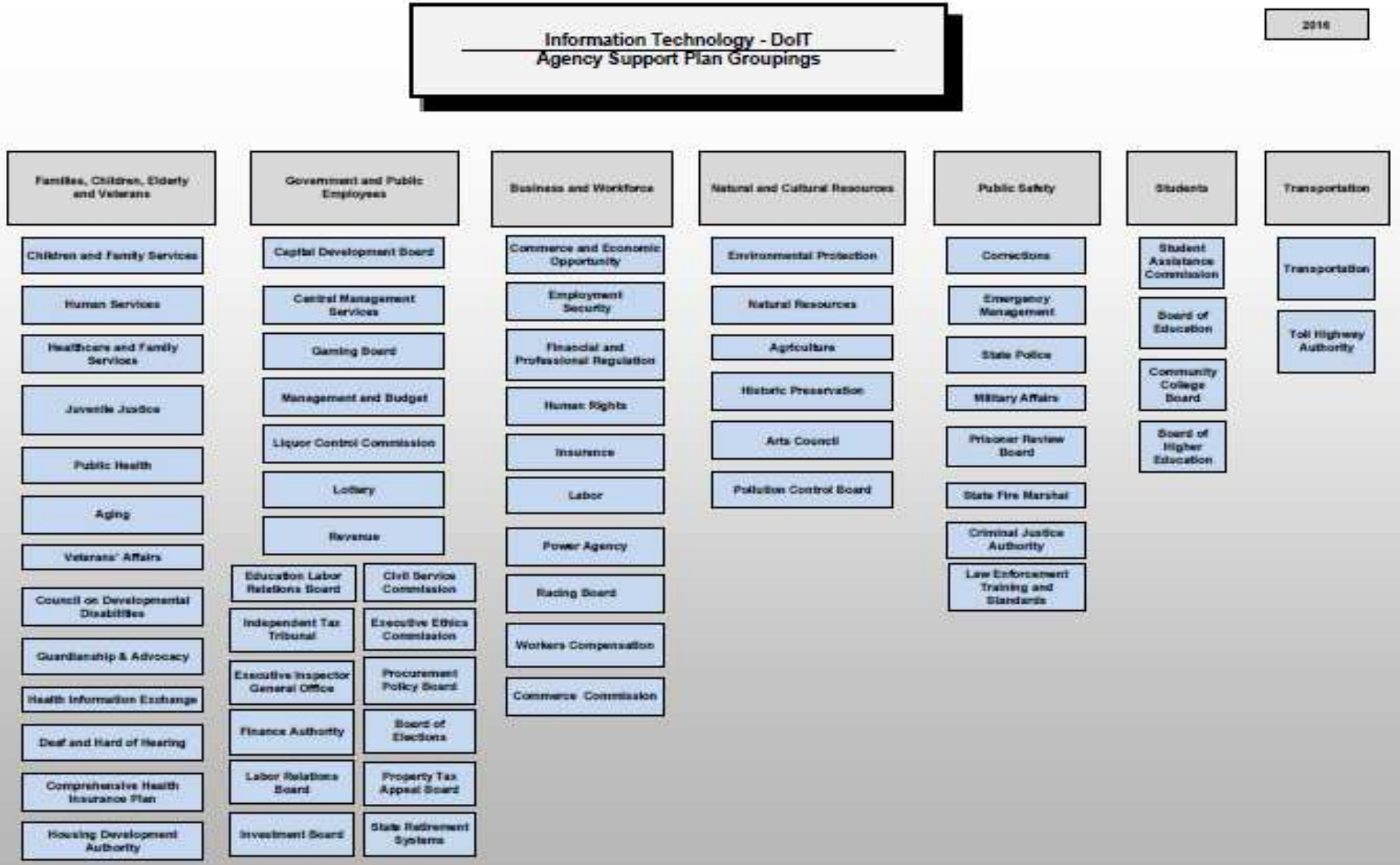
Incorporating risk management principles and best practices into organization-wide strategic planning considerations, core missions and business processes, and supporting organizational information systems.

Risk Assessment

1. Part of an overall Security Assessment
2. Incorporates threats and vulnerability intel
3. Considers mitigations provided by security controls

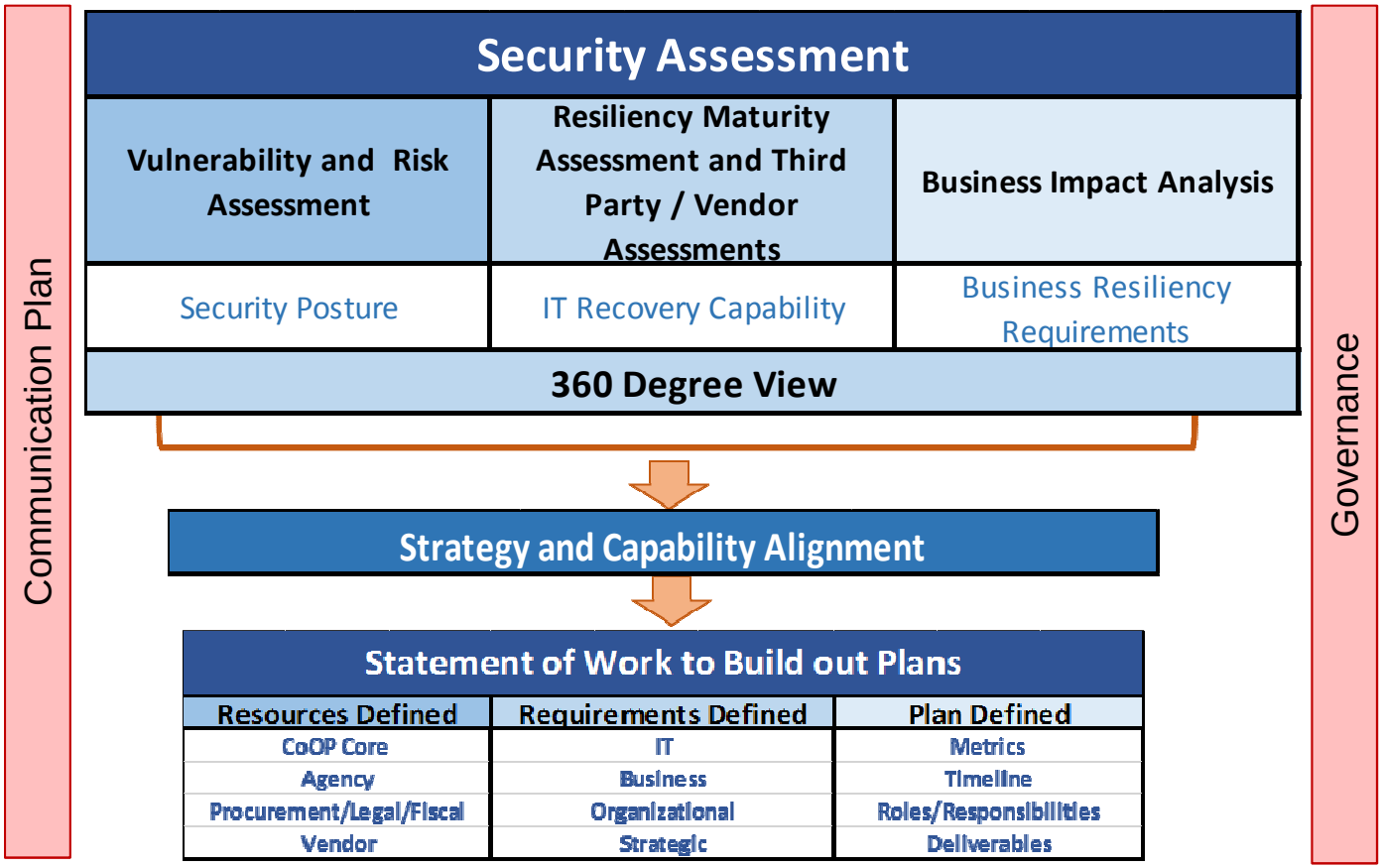
Why do Risk Assessments?

Our Challenge



Risk Management Program

Risk one of the Building Blocks of DoIT's Security Assessment Program



Current State

Future State

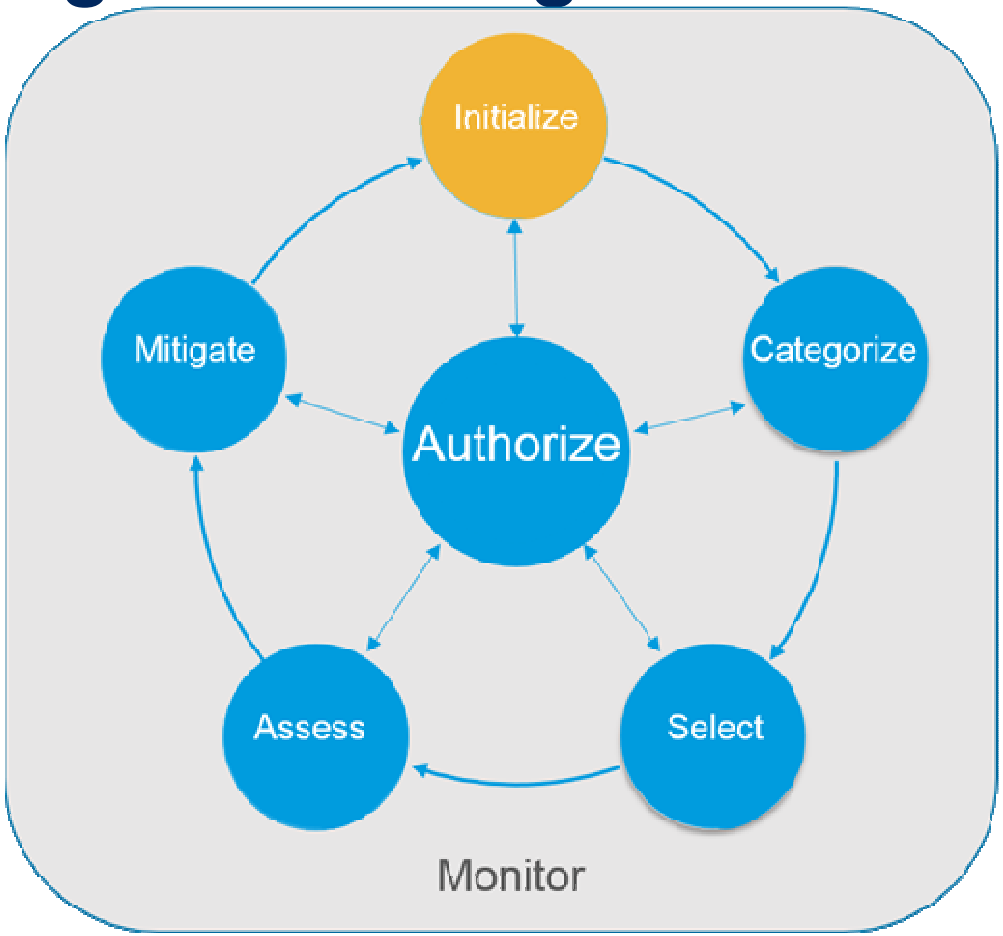
Path to Get there

End Game: Secure and Resilient IT

DR/Contingency/Continuity Plans in place, Tested and Executable for Information Systems, Infrastructure, Applications, Data, Personnel

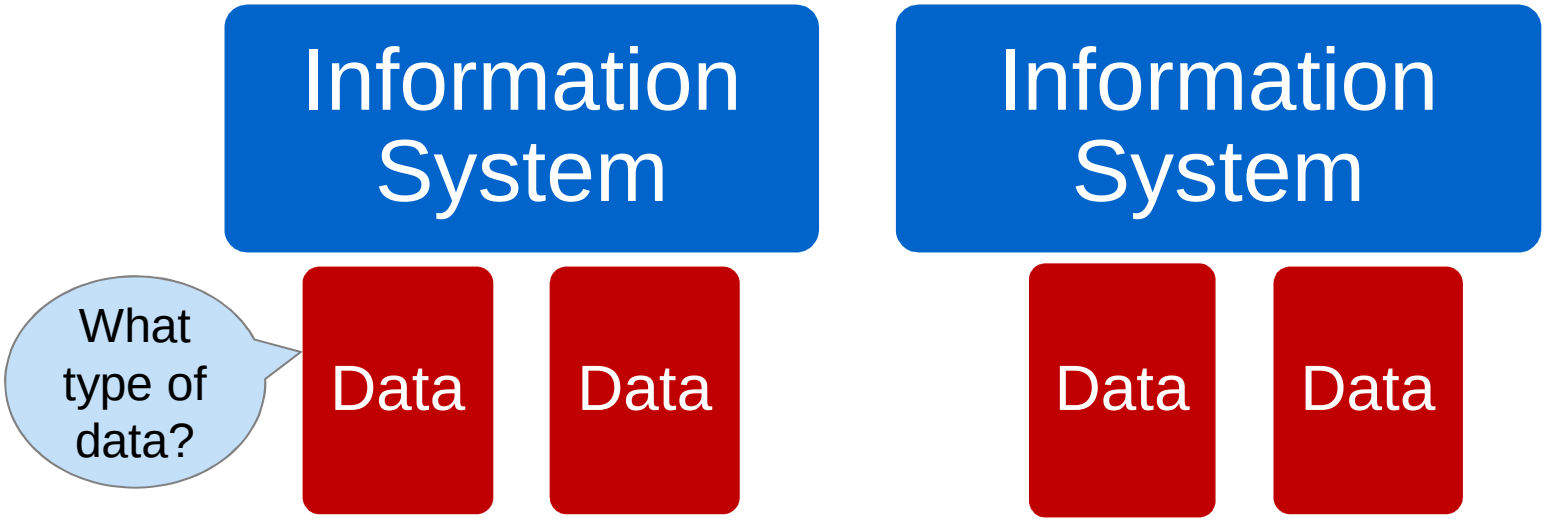
Risk Management Program

Risk Management Program Process



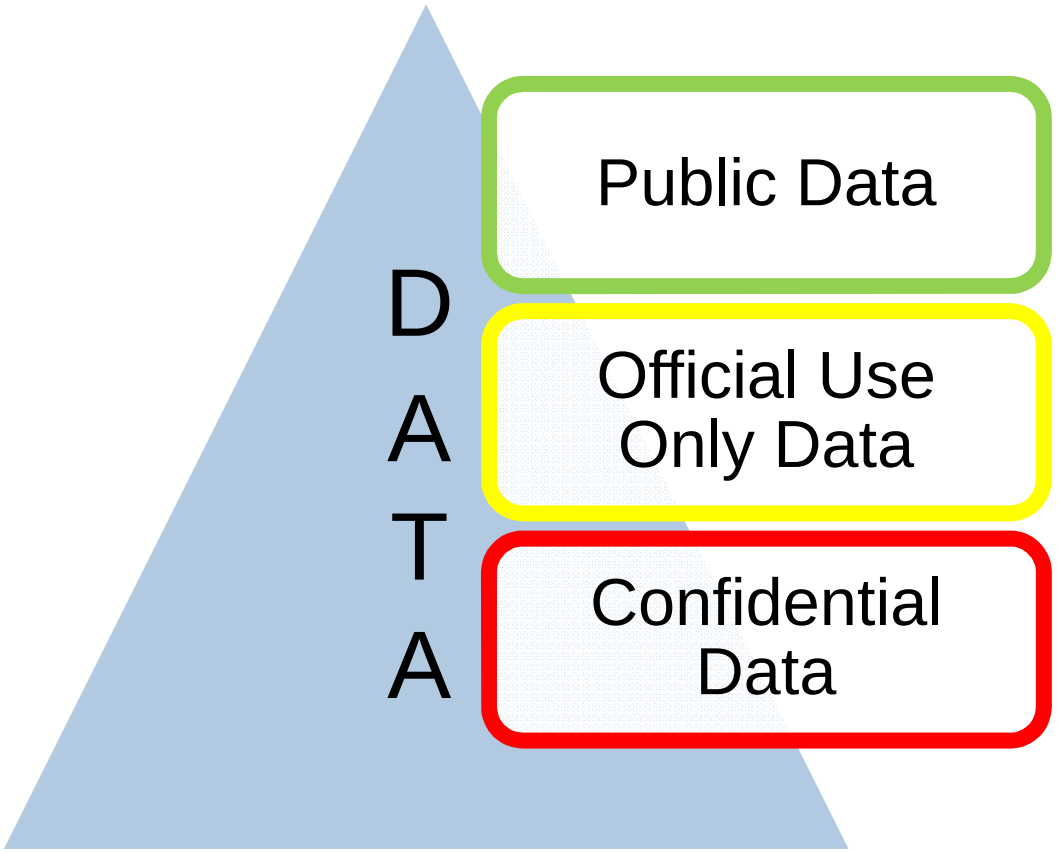
Risk Management Program

Classifying(Data) and Categorizing(Systems)



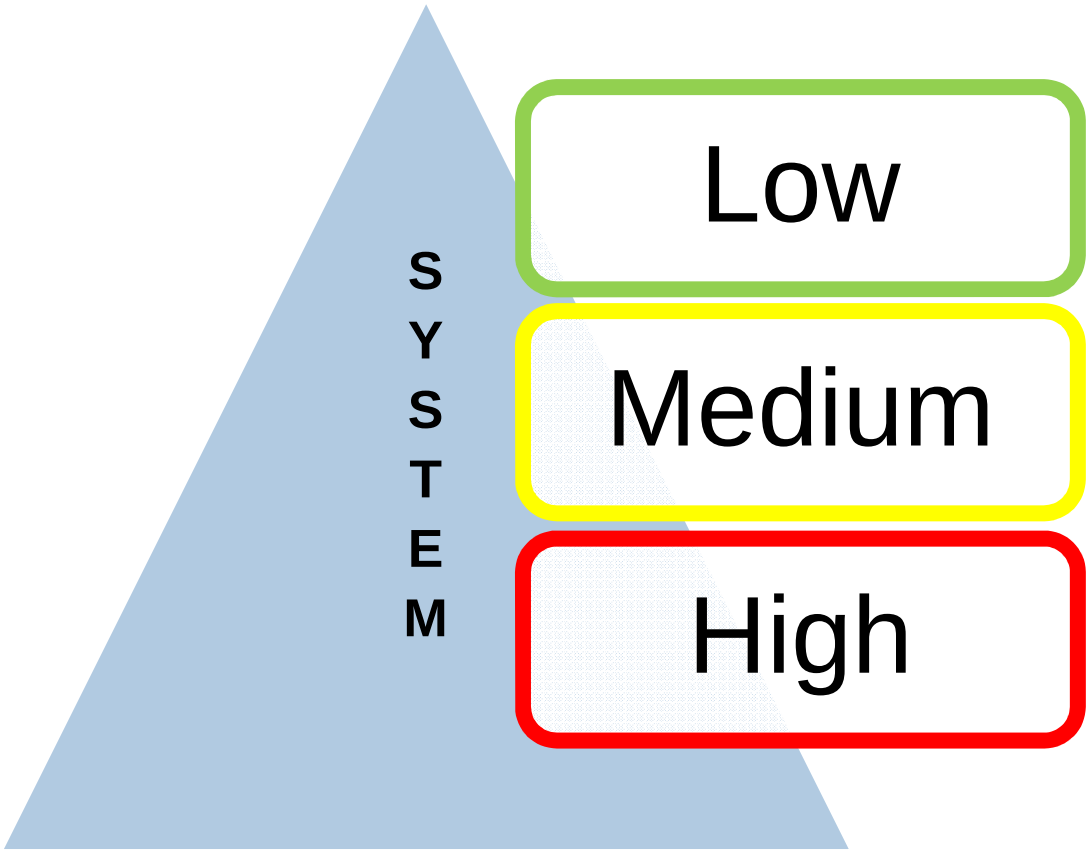
Risk Management Program

Data Classification



Risk Management Program

System Categorization



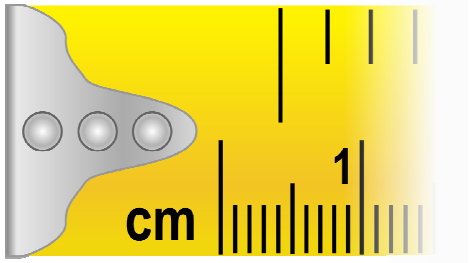
Risk Management Program

CIA

- Confidentiality
- Integrity
- Availability

Risk Management Program

Strength



Breadth

Rigor

Illinois Department of Innovation & Technology
Risk Assessment Framework

Score	Strength	Breadth	Rigor
1	Little to no protection	Little or no application across the organization	Ad-hoc process; not formally documented
2	No significant protection	Some application in selected areas across the organization	Repeatable process; not formally documented
3	Meaningful protection with little to no consistency in enforcement	Application in critical areas across the organization	Standard repeatable process; formally documented
4	Strong protection with consistent in enforcement	Application in most areas across the organization	Managed process with defined metrics driving toward control objectives
5	Maximum protection and consistent enforcement	Application in all possible areas across the organization	Optimized process; continuously improving; automated if possible

Risk Management Program

State of Illinois (Department of Information Technology)
Information Security organization Risk Assessment Framework: Self-Assessment Tool

Document Overview

This information security self-assessment tool provides an information security risk assessment framework for the State of Illinois (DoIT) by integrating control requirements and guidelines from National Institute of Standards and Technology (NIST) 800-53 Rev. 4.

Table of Contents

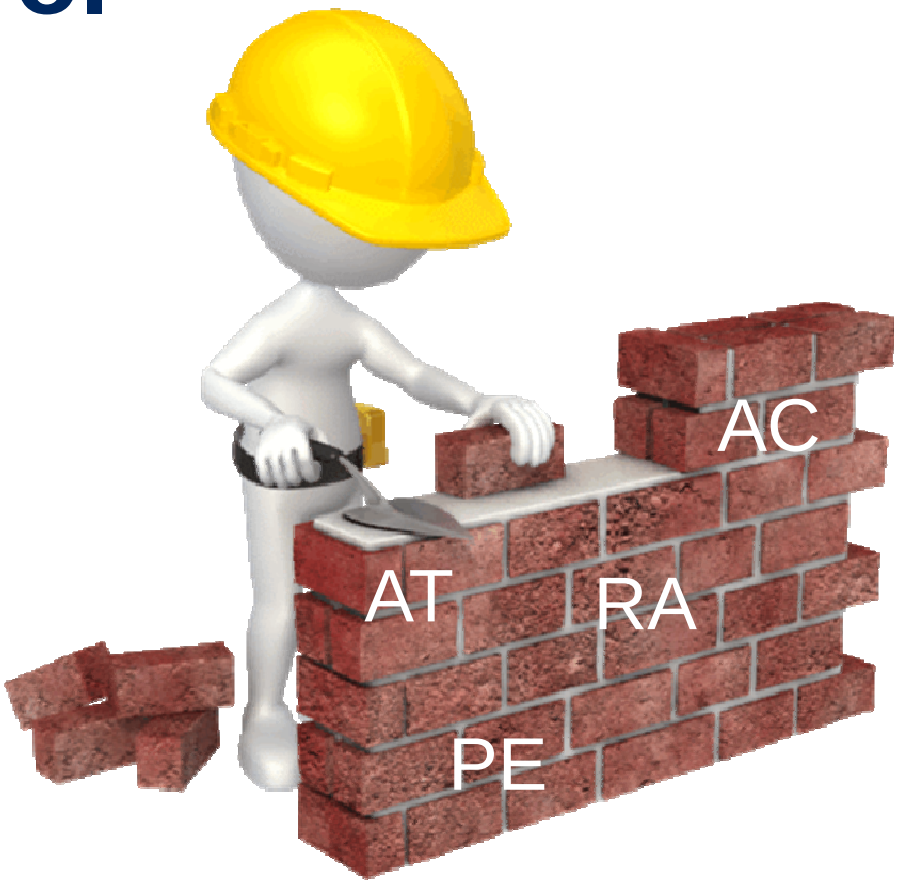
Page 1

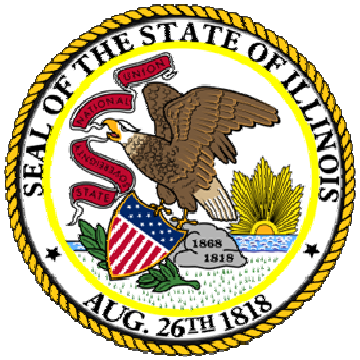
Version Control

Version	Updated by	Date modified	Change description
1.0		8/30/2016	Initial draft

Risk Management Program

NIST Control Families SP 800-37





Thank you,
Chris Hill
chris.hill@Illinois.gov