



Risk Management Program

An Introduction

CONFIDENTIAL – PROPRIETARY AND PRE-DECISIONAL
Any use of this material without specific permission is strictly prohibited



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 Management Program

Risk Assessment

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



Risk Management Program

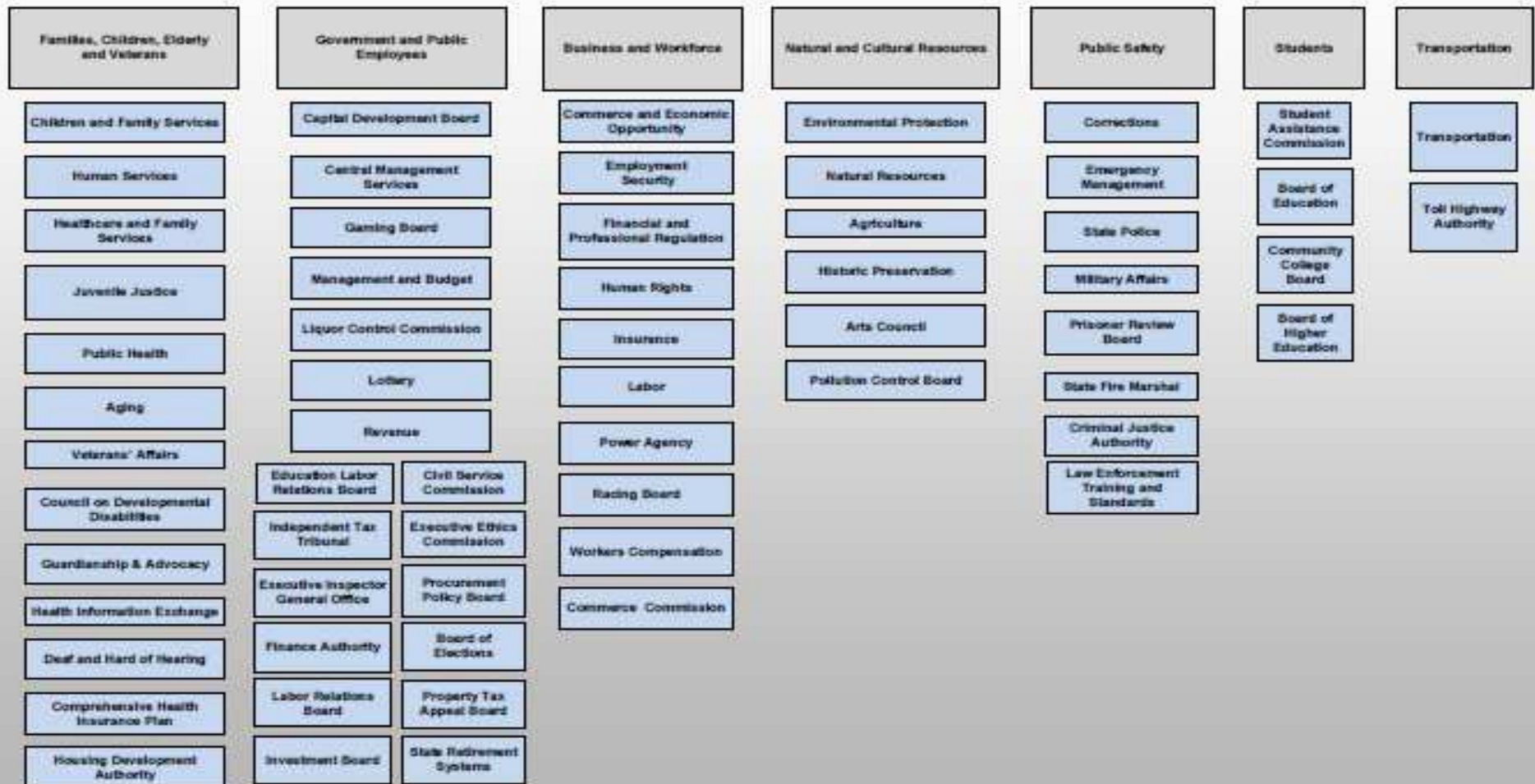
Why do Risk Assessments?



Our Challenge

Information Technology - DoIT Agency Support Plan Groupings

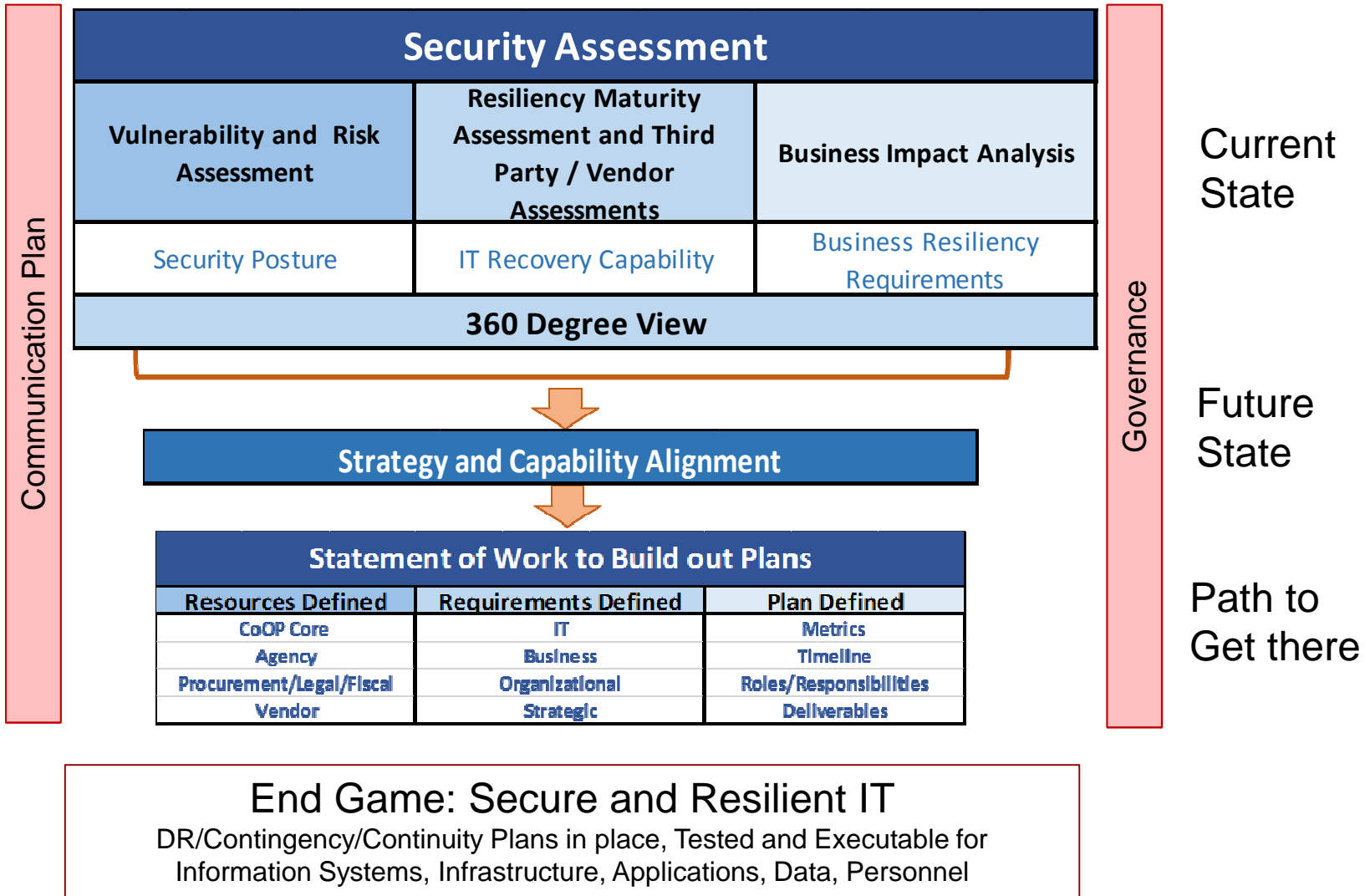
2016



Risk Management Program

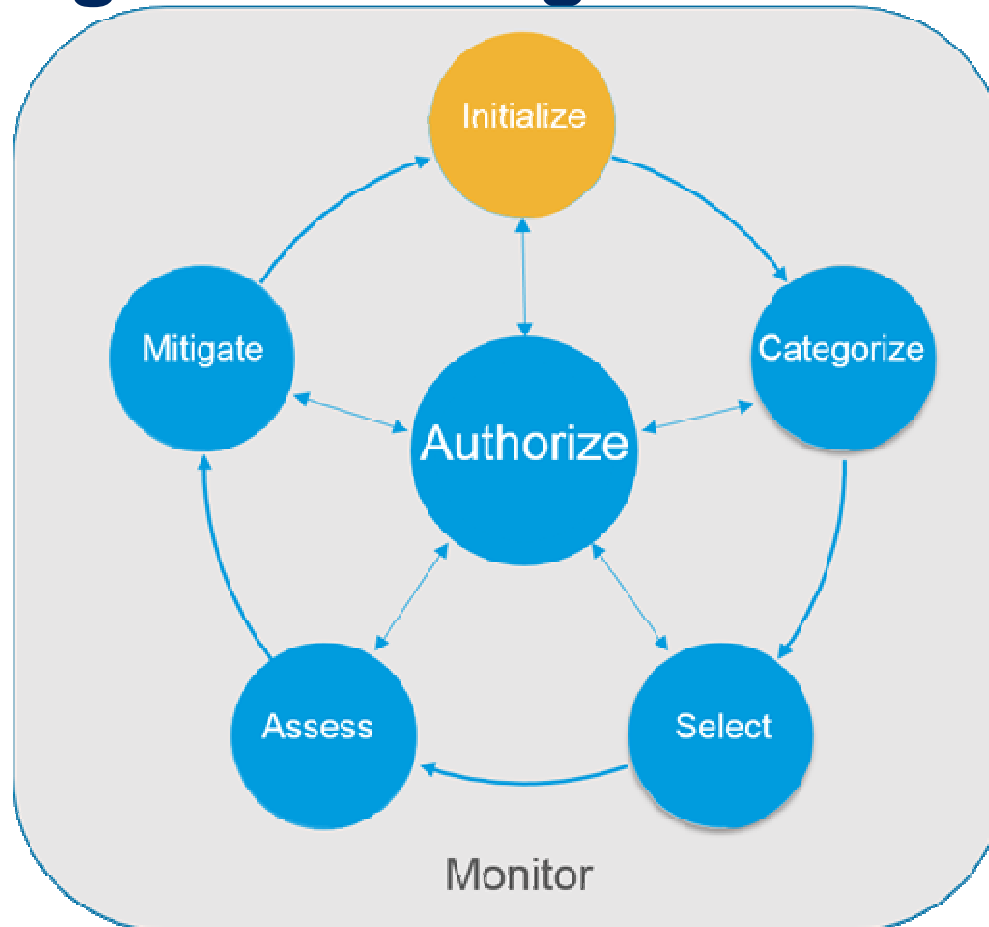
Risk one of the Building Blocks of DoIT's Security Assessment Program





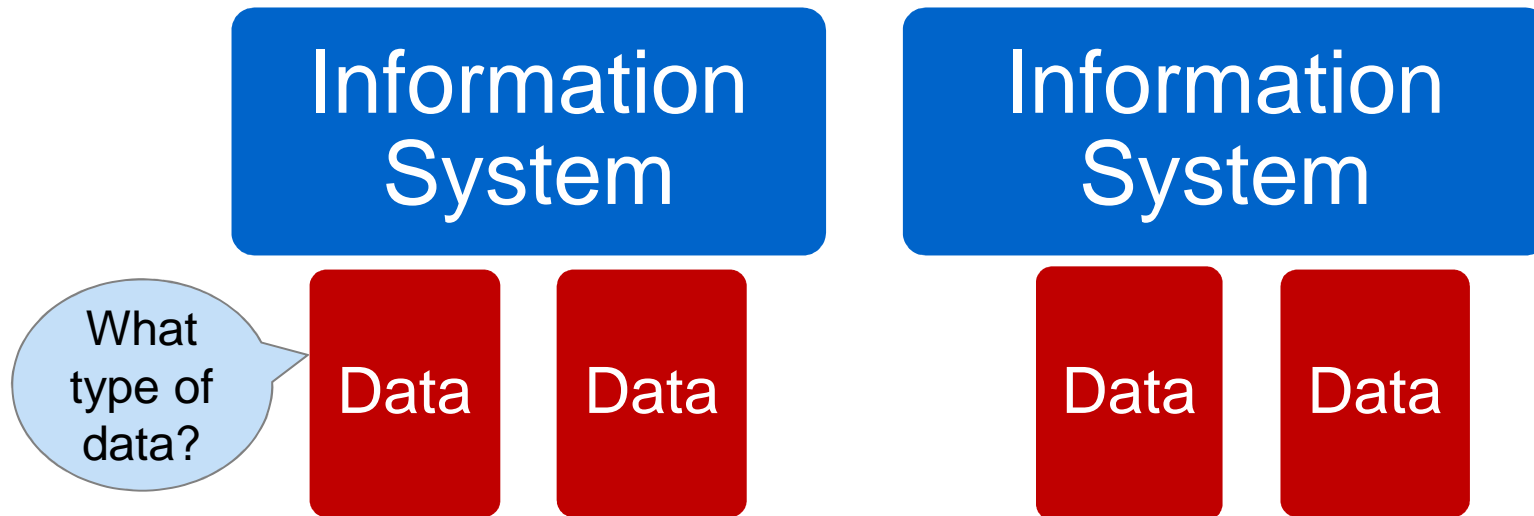
Risk Management Program

Risk Management Program Process



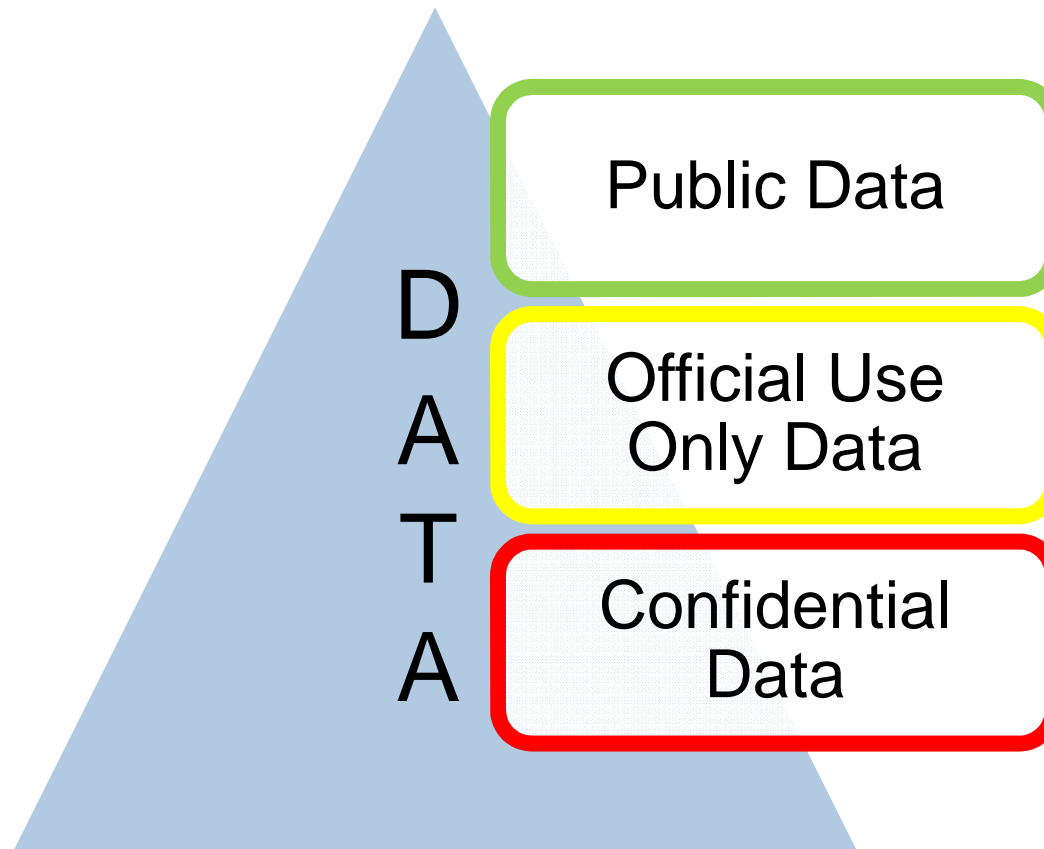
Risk Management Program

Classifying(Data) and Categorizing(Systems)



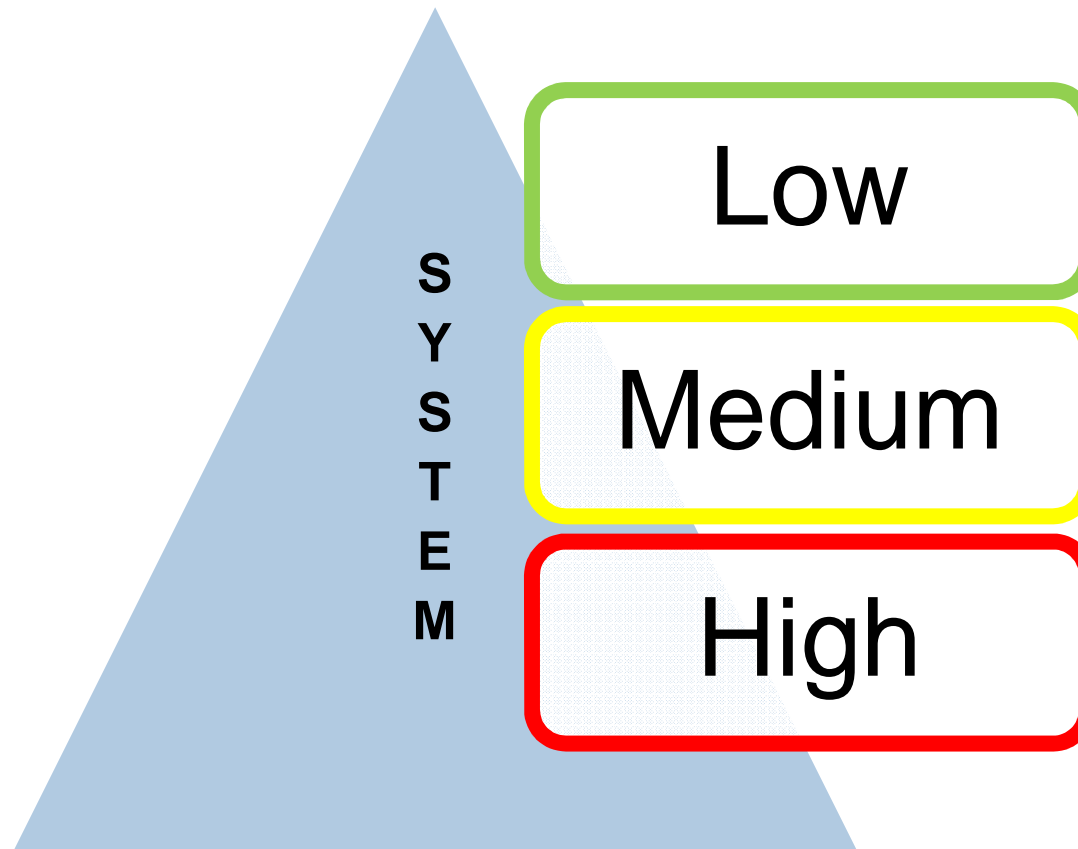
Risk Management Program

Data Classification



Risk Management Program

System Categorization



Risk Management Program

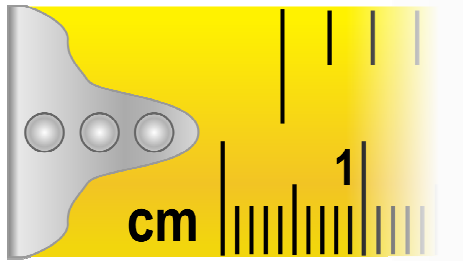
CIA

- Confidentiality
- Integrity
- Availability



Risk Management Program

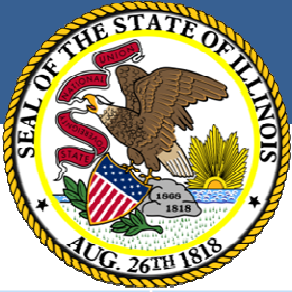
Strength



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

- 1. Risk Assessment Framework Overview
- 2. Roles & Responsibilities (Phase Approvals)
- 3. Information Security Domains
- 4. Information Security Control Matrix
- 5. Risk Dashboard
- 5. Data Summary
- 7.1 Governance Organization
- 7.2 IT Risk Strategy
- 7.3 IT Risk Management
- 7.4 Asset Management
- 7.5 Data Protection & Privacy
- 7.6 Security Operations
- 7.7 Vulnerability Management
- 7.8 Identity Access Management
- 7.9 Training & Awareness
- 7.10 Monitoring, Communication & Reporting
- 8. Reference
- 9. New System Assessment
- 10. NIST 800-53 Rev4 Control List

Page 1

Version Control

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

All Rights Reserved

This tool is intended solely for the use of the State of Illinois and is not intended to be and should not be used by any other person or entity. Content may not be reproduced, altered, or transferred in any form or by any means, except with the prior written permission of DoIT.

Risk Management Program

NIST Control

Families

SP 800-37





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