

An Introduction



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

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:

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?



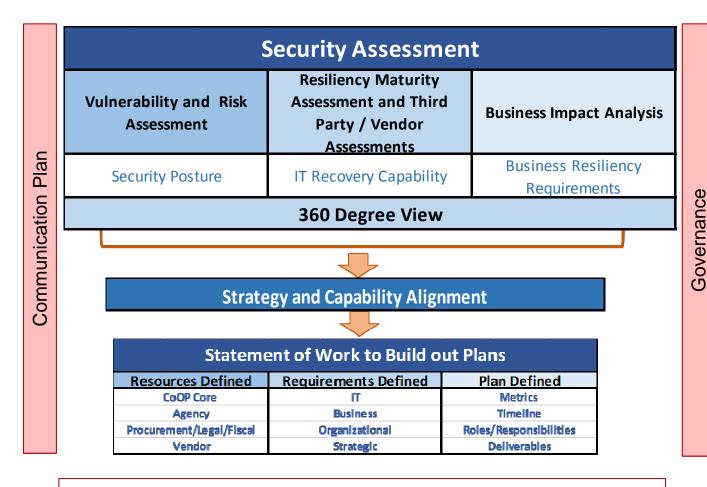
Our Challenge

Information Technology - DoIT Agency Support Plan Groupings 2016

12	. 102		G2 40		1 0	: Wr = ±0	165-
Fundles, Children, Elderly and Veterans	Government Emplo		Business and Workforce	Natural and Cultural Resources	Public Selety	Students	Transportati
Children and Family Services	Capital Develo	opment Board	Commerce and Economic Opportunity	Environmental Protection	Corrections	Student Assistance Commission	Transportati
Human Services	Central Management Services		Employment Security	Natural Resources	Emergency Management	Sound of	ř.
Healthcare and Family Services	Gaming Board		Financial and Professional Regulation		State Police	Education	Toll Highway Authority
Juvenile Justice	Management	and Budget	Human Sights	Historic Preservation	Military Affairs	Community College Board	7.5
Public Health	Liquor Control	Commission	Insurance	Arts Council	Prisoner Review Board	Sound of Higher Estucation	
	Lon	wy	Labor	Poliution Control Board	State Fire Marshall		
Aging Veterans' Affaira	Nevense		Power Agency		Criminal Justice Authority		
Veurans Amaris	Education Labor Ratellons Sound	Civil Service Commission	27777		Law Enforcement Training and		
Council on Developmental Disabilities	Independent Tax	Executive Ethics	Racing Doard		Diameterds		
Guardianahip & Advocacy	Tribunal	Commission	Workers Compensation				
Health Information Exchange	Esscutive inspector General Office	Procurement Policy Board	Commerce Commission				
Deaf and Hard of Hearing	Finance Authority	Board of Elections	12				
Comprehensive Health	Labor Relations Board	Property Tax Appeal Board					
Housing Development	Investment Sound	State Retirement Systems					

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





Current State

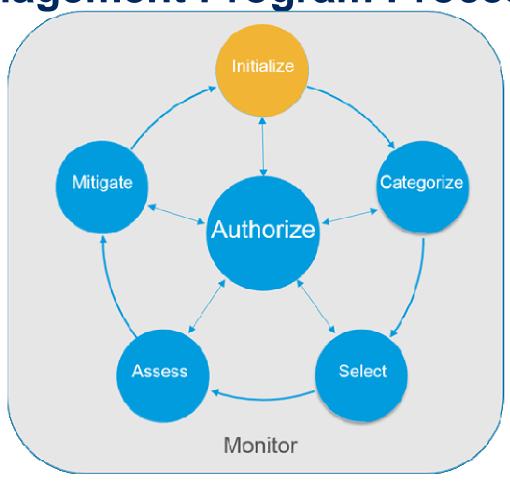
Future State

Path to Get there

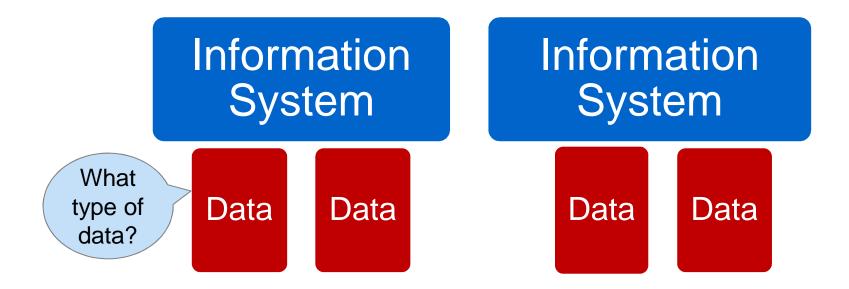
End Game: Secure and Resilient IT

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

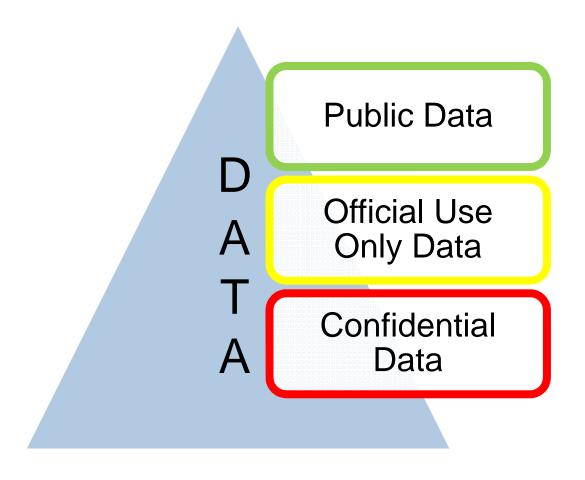
Risk Management Program Process



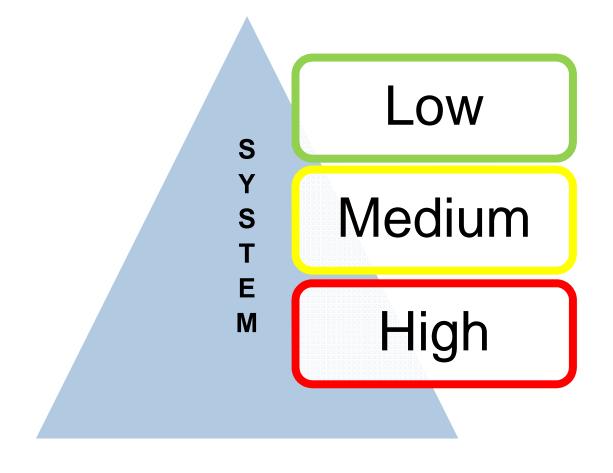
Classifying(Data) and Categorizing(Systems)



Data Classification



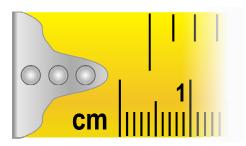
System Categorization





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	

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 DolT).

NIST Control

Families

SP 800-37





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