Virginia Information Technologies Agency

Welcome and Opening Remarks

Mike Watson

March 4, 2020

ISOAG March Agenda

- Welcome and Opening Remarks - Mike Watson
- NIST Publications 800-37 Risk Management- Eduardo Takamura, NIST Framework For Systems and Organizations
- How to Improve Cybersecurity – Servio F Medina, Health Information Technology
- Quantitative Risk Analysis – Mark Martens, VITA

NIST Risk Management Framework (RMF) Overview

Eduardo Takamura

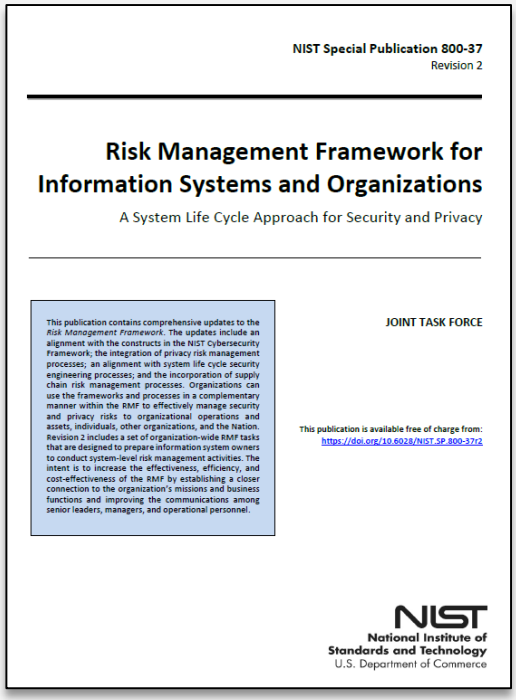
FISMA Implementation Project
National Institute of Standards and Technology (NIST)
Information Technology Laboratory (ITL)
Computer Security Division (CSD)

Virginia Information Technologies Agency (VITA) Information Security Officer Advisory Group (ISOAG)
March 4, 2020 Meeting, Chester, VA

Outline

- Introduction
- **NIST RMF Overview**
- **NIST RMF Steps**
- Featured Publications
- Resources and Engagement Opportunities
- Q&A and Open Discussion

DISCLAIMER: any mention of entities, equipment, materials, or services throughout this talk is for information only; it does not imply recommendation or endorsement by NIST, nor is it intended to imply best available solution for any given purpose.


NIST Special Publication 800-37
Revision 2

Risk Management Framework for Information Systems and Organizations

A System Life Cycle Approach for Security and Privacy

This publication contains comprehensive updates to the *Risk Management Framework*. The updates include an alignment with the constructs in the NIST Cybersecurity Framework; the integration of privacy risk management processes; an alignment with system life cycle security engineering processes; and the incorporation of supply chain risk management processes. Organizations can use the frameworks and processes in a complementary manner within the RMF to effectively manage security and privacy risks to organizational operations and assets, individuals, other organizations, and the Nation. Revision 2 includes a set of organization-wide RMF tasks that are designed to prepare information system owners to conduct system-level risk management activities. The intent is to increase the effectiveness, efficiency, and cost-effectiveness of the RMF by establishing a closer connection to the organization's missions and business functions and improving the communications among senior leaders, managers, and operational personnel.

JOINT TASK FORCE

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-37r2

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

NIST, FISMA Implementation Project, RMF

The **National Institute of Standards and Technology (NIST)** is a non-regulatory bureau of the U.S. Department of Commerce responsible for developing **information security standards and guidelines**, including **minimum requirements for federal systems** (except national security systems unless otherwise approved by appropriate federal officials exercising policy authority over such systems)

The **Federal Information Security Modernization Act (FISMA)** publications are developed by NIST in accordance with its statutory responsibilities under the Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. § 3551 et seq., Public Law (P.L.) 113-283.

The **Risk Management Framework (RMF)** developed by NIST effectively brings together all of the **FISMA-related security standards and guidance to promote the development of comprehensive and balanced information security programs by agencies**.

Photo credit: Courtesy HDR Architecture, Inc./Steve Hall © Hedrich Blessing

The NIST Risk Management Framework

A flexible model for developing, implementing, and maintaining a risk management process for IT security and privacy

Described in **NIST SP 800-37 Revision 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy* (December 2018)**

Provides a holistic risk management process (disciplined and structured)

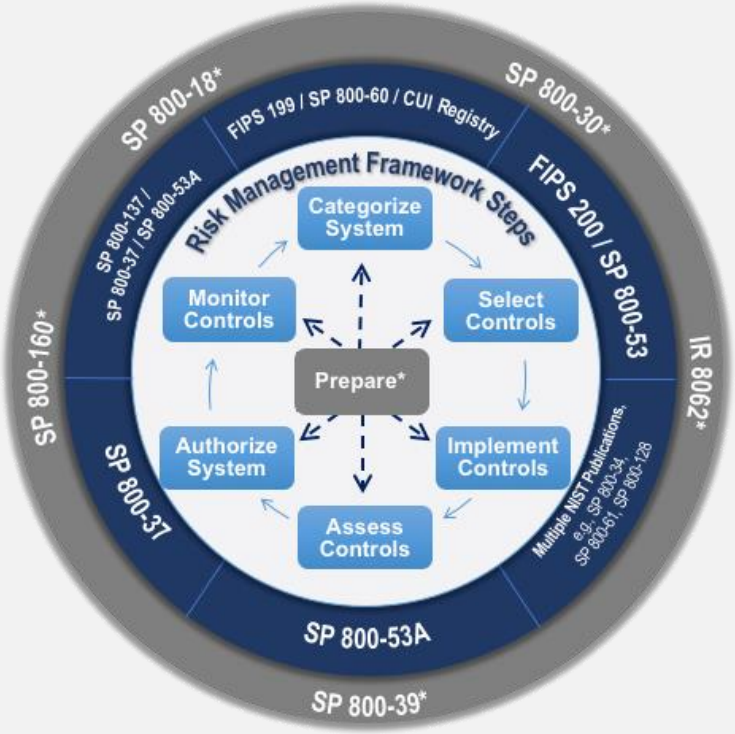
Integrates information security and risk management activities into the system development life cycle

"to guide and inform the **CATEGORIZATION** of Federal information and information systems; the **SELECTION**, **IMPLEMENTATION**, and **ASSESSMENT** of security and privacy controls; the **AUTHORIZATION** of information systems and common controls; and the continuous **MONITORING** of information systems." (Office of Management and Budget Circular A-130, *Managing Information as a Strategic Resource*)

NIST Special Publication 800-37 Revision 2

HIGHLIGHTS	NEW GUIDANCE	UPDATED GUIDANCE
Provide closer links and **improve communication** between C-Suite/Governance-level to system/operational-level	Privacy, supply chain, Cybersecurity Framework (CSF), security engineering	Authorization boundaries
Integrates **privacy**, **supply chain**, and **security engineering** into the Risk Management Framework (RMF)	New Prepare Step	Authorization decisions and types
Aligns the **Cybersecurity Framework** and the RMF	All RMF tasks include potential inputs and expected outputs	Ongoing authorization
Demonstrates how the RMF is implemented in the **system development life cycle**	"New" tasks in existing steps	Roles and responsibilities

NIST RMF Steps

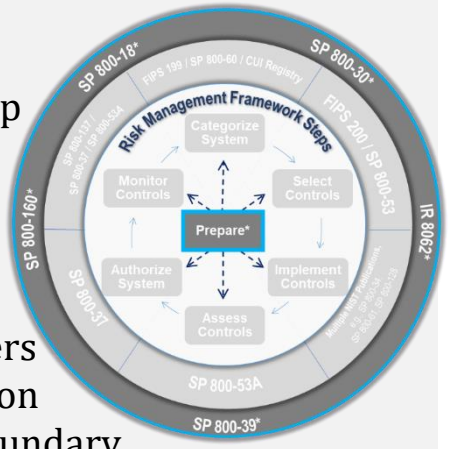


PREPARE Step
CATEGORIZE Step
SELECT Step
IMPLEMENT Step
ASSESS Step
AUTHORIZE Step
MONITOR Step

Prepare Step

New *

Purpose: Carry out essential activities at all three risk management levels to help prepare the organization to manage its security and privacy risks using the RMF.



Organization- & Mission/Business Process-Level Tasks

P-1: Risk Management Roles
P-2: Risk Management Strategy
P-3: Risk Assessment – Organization
P-4: Organizationally-tailored Control Baselines and Cybersecurity Framework Profiles (optional)
P-5: Common Control Identification
P-6: Impact Level Prioritization (optional)
P-7: Continuous Monitoring Strategy – Organization
P-8: Mission or Business Focus

System-Level Tasks

P-9: System Stakeholders
P-10: Asset Identification
P-11: Authorization Boundary
P-12: Information Types
P-13: Information Life Cycle
P-14: Risk Assessment – System
P-15: Requirements Definition
P-16: Enterprise Architecture
P-17: Requirements Allocation
P-18: System Registration

See Kelley Dempsey's ISOAG June 7, 2017 presentation on ISCM

Task Structure

Task abbreviation

"Prepare Step Task 11"

Associated **SDLC** phase(s)/ process(es) when task is typically executed (not in Prepare)

Related publications/ resources

AUTHORIZATION BOUNDARY

TASK P-11 Determine the authorization boundary of the system.

Potential Inputs: System design documentation; network diagrams; system stakeholder information; asset information; network and/or enterprise architecture diagrams; organizational structure (charts, information).

Expected Outputs: Documented authorization boundary.

Primary Responsibility: Authorizing Official.

Supporting Roles: Chief Information Officer; System Owner; Mission or Business Owner; Senior Agency Information Security Officer; Senior Agency Official for Privacy; Enterprise Architect.

System Development Life Cycle Phase: New – Initiation (concept/requirements definition).
Existing – Operations/Maintenance.

Discussion: Authorization boundaries establish the scope of protection for information systems (i.e., what the organization agrees to protect under its management control or within the scope of its …

References: [SP 800-18]; [SP 800-39] (System Level); [SP 800-47]; [SP 800-64]; [SP 800-160 v1] (System Requirements Definition Process); [NIST CSF] (Core [Identify Function]).

Information that **may** be needed to complete the task

Artifacts, **results**, or conditions after task execution

Roles within the organization that may help with or provide input for task completion

Explanatory **information** to facilitate understanding

Prepare Tasks and Outcomes: Organization Level

TASKS	OUTCOMES
TASK P-1: RISK MANAGEMENT ROLES	Individuals are identified and assigned key roles for executing the RMF.
TASK P-2: RISK MANAGEMENT STRATEGY	A risk management strategy for the organization that includes a determination and expression of organizational risk tolerance is established.
TASK P-3: RISK ASSESSMENT – ORGANIZATION	An organization-wide risk assessment is completed or an existing risk assessment is updated.
TASK P-4: ORGANIZATIONALLY-TAILORED CONTROL BASELINES AND CSF PROFILES (OPT)	Organizationally-tailored control baselines and/or CSF profiles are established and made available.
TASK P-5: COMMON CONTROL IDENTIFICATION	Common controls that are available for inheritance by organizational systems are identified, documented, and published.
TASK P-6: IMPACT-LEVEL PRIORITIZATION (OPT)	A prioritization of organizational systems with the same impact level is conducted.
TASK P-7: CONTINUOUS MONITORING STRATEGY – ORGANIZATION	An organization-wide strategy for monitoring control effectiveness is developed and implemented.

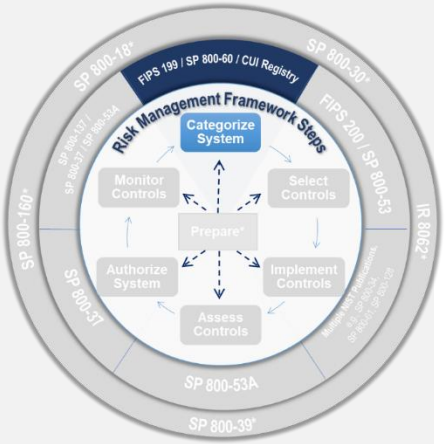
Prepare Tasks and Outcomes: System Level

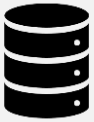
TASKS	OUTCOMES
TASK P-8: MISSION OR BUSINESS FOCUS	Missions, business functions, and mission/business processes that the system is intended to support are identified.
TASK P-9: SYSTEM STAKEHOLDERS	The stakeholders having an interest in the system are identified.
TASK P-10: ASSET IDENTIFICATION	Stakeholder assets are identified and prioritized.
TASK P-11: AUTHORIZATION BOUNDARY	The authorization boundary (i.e., system) is determined.
TASK P-12: INFORMATION TYPES	The types of information processed, stored, and transmitted by the system are id'd.
TASK P-13: INFORMATION LIFE CYCLE	All stages of the information life cycle are identified and understood for each information type processed, stored, or transmitted by the system.
TASK P-14: RISK ASSESSMENT – SYSTEM	A system-level risk assessment is completed or an existing risk assessment is updated.
TASK P-15: REQUIREMENTS DEFINITION	Security and privacy requirements are defined and prioritized.
TASK P-16: ENTERPRISE ARCHITECTURE	The placement of the system within the enterprise architecture is determined.
TASK P-17: REQUIREMENTS ALLOCATION	Security and privacy requirements are allocated to the system and to the environment in which the system operates.
TASK P-18: SYSTEM REGISTRATION	The sys. is registered for purposes of management, accountability, coord. & oversight.

Categorize Step

Purpose: Inform organizational risk management processes and tasks by determining the adverse impact of the loss of confidentiality, integrity, and availability of organizational systems and information to the organization.

C-1: System Description
C-2: Security Categorization
C-3: Security Categorization Review and Approval New*





Categorize Tasks and Outcomes

TASKS	OUTCOMES
TASK C-1: SYSTEM DESCRIPTION	The characteristics of the system are described and documented.
TASK C-2: SECURITY CATEGORIZATION	• A security categorization of the system, including the information processed by the system represented by the organization-defined information types, is completed • Security categorization results are documented in the security, privacy, and SCRM plans • Security categorization results are consistent with the enterprise architecture and commitment to protecting organizational missions, business functions, and mission/business processes. • Security categorization results reflect the organization's risk management strategy
TASK C-3: SECURITY CATEGORIZATION REVIEW AND APPROVAL	The security categorization results are reviewed and the categorization decision is approved by senior leaders in the organization

Security Objectives

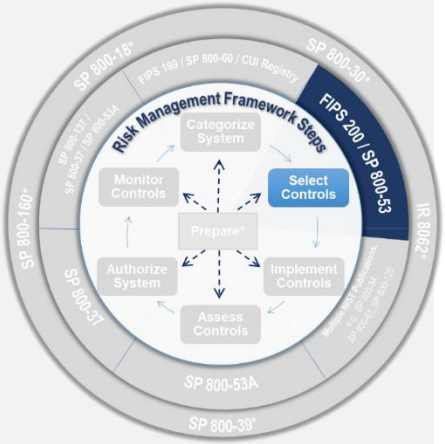
CONFIDENTIALITY
INTEGRITY
AVAILABILITY

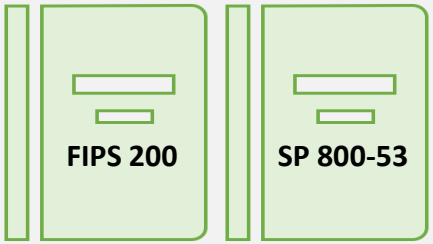
Impact Level
Low: loss has limited adverse impact
Moderate: loss has serious adverse impact
High: loss has catastrophic adverse impact

Select Step

Purpose: Select, tailor, and document the controls necessary to protect the information system and organization commensurate with risk to organizational operations and assets, individuals, and the Nation.

S-1: Control Selection
S-2: Control Tailoring — New*
S-3: Control Allocation — Revised
S-4: Documentation of Planned Control Implementations — New*
S-5: Continuous Monitoring Strategy – System — Revised
S-6: Plan Review and Approval





Select Tasks and Outcomes

TASKS	OUTCOMES
TASK S-1: CONTROL SELECTION	Control baselines necessary to protect the system commensurate with risk are selected.
TASK S-2: CONTROL TAILORING	Controls are tailored producing tailored control baselines.
TASK S-3: CONTROL ALLOCATION	• Controls are designated as system-specific, hybrid, or common controls. • Controls are allocated to the specific system elements (i.e., machine, physical, or human elements).
TASK S-4: DOCUMENTATION OF PLANNED CONTROL IMPLEMENTATIONS	Controls and associated tailoring actions are documented in security and privacy plans or equivalent documents.
TASK S-5: CONTINUOUS MONITORING STRATEGY – SYSTEM	A continuous monitoring strategy for the system that reflects the organizational risk management strategy is developed.
TASK S-6: PLAN REVIEW AND APPROVAL	Security and privacy plans reflecting the selection of controls necessary to protect the system and the environment of operation commensurate with risk are reviewed and approved by the authorizing official.

Select Step: SP 800-53 Control Families

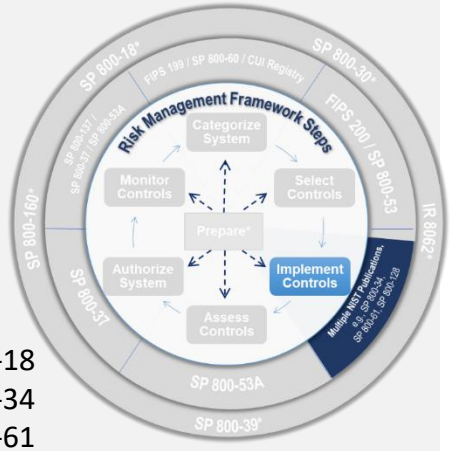
AC – Access Control	**PE – Physical and Environmental Protection**
AT – Awareness and Training	**PL – Planning**
AU – Audit and Accountability	**PM – Program Management**
CA – Assessment, Authorization, and Monitoring	**PS – Personnel Security**
CM – Configuration Management	***PT – PII Processing and Transparency***
CP – Contingency Planning	**RA – Risk Assessment**
IA – Identification and Authentication	**SA – System and Services Acquisition**
IR – Incident Response	**SC – System and Communications Protection**
MA – Maintenance	**SI – System and Information Integrity**
MP – Media Protection	***SR – Supply Chain Risk Management***

Implement Step

Purpose: Implement the controls as specified in security and privacy plans for the system and for the organization, and update the plans with the as-implemented details.

I-1: Control Implementation
I-2: Update Control Implementation Information Revised

800-18
800-34
800-61
800-128

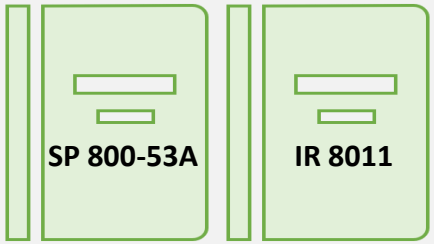


TASKS	OUTCOMES
TASK I-1: CONTROL IMPLEMENTATION	• Controls specified in the security and privacy plans are implemented. • System security and privacy engineering methodologies are used to implement the controls in the system security and privacy plans.
TASK I-2: UPDATE CONTROL IMPLEMENTATION INFORMATION	• Changes to the planned implementation of controls are documented. • The security and privacy plans are updated based on information obtained during the implementation of the controls.

Assess Step

Purpose: Determine if the controls selected for implementation are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security and privacy requirements for the system and organization.

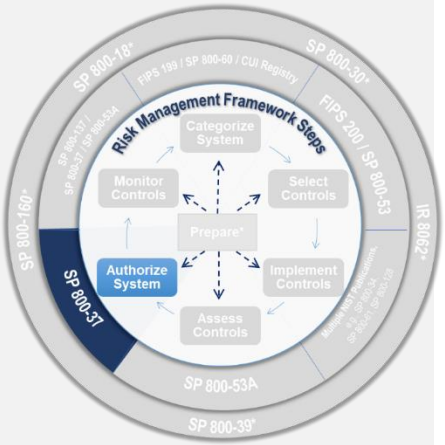
A-1: Assessor Selection New*
A-2: Assessment Plan
A-3: Control Assessments
A-4: Assessment Reports
A-5: Remediation Actions
A-6: Plan of Action and Milestones Moved



Assess Tasks and Outcomes

TASKS	OUTCOMES
TASK A-1: ASSESSOR SELECTION	• An assessor or assessment team is selected to conduct the control assessments. • The appropriate level of independence is achieved for the assessor or assessment team selected.
TASK A-2: ASSESSMENT PLAN	• Documentation needed to conduct the assessments is provided to the assessor or assessment team. • Security and privacy assessment plans are developed and documented. • Security and privacy assessment plans are reviewed and approved to establish the expectations for the control assessments and the level of effort required.
TASK A-3: CONTROL ASSESSMENTS	• Control assessments are conducted in accordance with the security and privacy assessment plans. • Opportunities to reuse assessment results from previous assessments to make the risk management process timely and cost-effective are considered. • Use of automation to conduct control assessments is maximized to increase speed, effectiveness, and efficiency of assessments.
TASK A-4: ASSESS. REPORTS	Security and privacy assessment reports that provide findings and recommendations are completed.
TASK A-5: REMEDIATION ACTIONS	• Remediation actions to address deficiencies in the controls implemented in the system and environment of operation are taken. • Security and privacy plans are updated to reflect control implementation changes made based on the assessments and subsequent remediation actions.
TASK A-6: PLAN OF ACTIONS AND MILESTONES	A plan of action and milestones detailing remediation plans for unacceptable risks identified in security and privacy assessment reports is developed.

Authorize Step

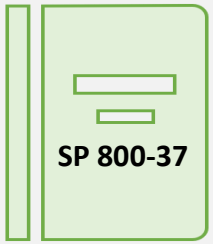


Purpose: Provide accountability by requiring a senior management official to determine if the security and privacy risk to organizational operations and assets, individuals, other organizations, or the Nation of operating a system or the use of common controls, is acceptable.

R-1: Authorization Package
R-2: Risk Analysis and Determination — Revised
R-3: Risk Response
R-4: Authorization Decision
R-5: Authorization Reporting — New*

Decisions:

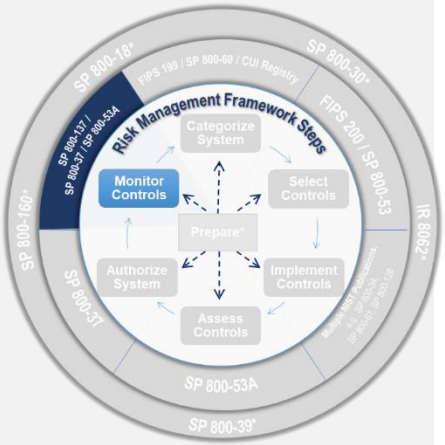
- Authorization To Operate
- Common Control Authorization
- Authorization To Use — New*
- Denial of Authorization



Authorize Tasks and Outcomes

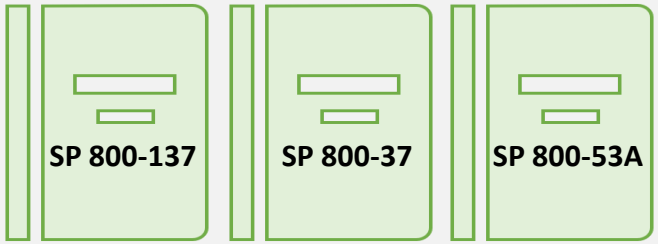
TASKS	OUTCOMES
TASK R-1: AUTHORIZATION PACKAGE	An authorization package is developed for submission to the authorizing official.
TASK R-2: RISK ANALYSIS AND DETERMINATION	A risk determination by the authorizing official that reflects the risk management strategy including risk tolerance, is rendered.
TASK R-3: RISK RESPONSE	Risk responses for determined risks are provided.
TASK R-4: AUTHORIZATION DECISION	The authorization for the system or the common controls is approved or denied.
TASK R-5: AUTHORIZATION REPORTING	Authorization decisions, significant vulnerabilities, and risks are reported to organizational officials.

Monitor Step



Purpose: Maintain an ongoing situational awareness about the security and privacy posture of the system and the organization in support of risk management decisions.

M-1: System and Environment Changes
M-2: Ongoing Assessments
M-3: Ongoing Risk Response
M-4: Authorization Package Updates
M-5: Security and Privacy Reporting
M-6: Ongoing Authorization
M-7: System Disposal



Monitor Tasks and Outcomes

TASKS	OUTCOMES
TASK M-1: SYSTEM AND ENVIRONMENT CHANGES	The information system and environment of operation are monitored in accordance with the continuous monitoring strategy.
TASK M-2: ONGOING ASSESSMENTS	Ongoing assessments of control effectiveness are conducted in accordance with the continuous monitoring strategy.
TASK M-3: ONGOING RISK RESPONSE	The output of continuous monitoring activities is analyzed and responded to appropriately.
TASK M-4: AUTHORIZATION PACKAGE UPDATES	Risk management documents are updated based on continuous monitoring activities.
TASK M-5: SECURITY AND PRIVACY REPORTING	A process is in place to report the security and privacy posture to the authorizing official and other senior leaders and executives.
TASK M-6: ONGOING AUTHORIZATION	Authorizing officials conduct ongoing authorizations using the results of continuous monitoring activities and communicate changes in risk determination and acceptance decisions.
TASK M-7: SYSTEM DISPOSAL	A system disposal strategy is developed and implemented, as needed.

Final Thoughts

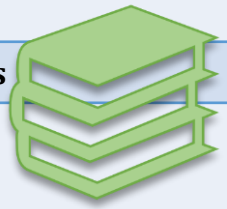
- RMF steps, tasks and supporting guidance facilitate and provide flexibility in the risk management process
- Not a one-size-fits-all approach or a compliance checklist
- Each organization is unique (i.e., may have different risks, threats, vulnerabilities, risk tolerance, and other attributes)
- RMF development a product of collaboration; NIST public comment process (2 public comment periods); public workshops with industry; ever evolving
- Know what you have & know the risks
- Risks cannot be eliminated, they need to be reduced and managed
- Tips for streamlining RMF implementation on page 25 of NIST SP 800-37 Revision 2

Featured Publications

FIPS 199	Standards for Security Categorization of Federal Information and Information Systems
FIPS 200	Minimum Security Requirements for Federal Information and Information Systems
SP 800-18	Guide for Developing Security Plans for Federal Information Systems
SP 800-30	Guide for Conducting Risk Assessments
SP 800-34	Contingency Planning Guide for Federal Information Systems
SP 800-37	Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy
SP 800-39	Managing Information Security Risk: Organization, Mission, and Information System View
SP 800-53	Security and Privacy Controls for Federal Information Systems and Organizations
SP 800-53A	Assessing Security and Privacy Controls in Federal IS and Organizations
SP 800-53B	Control Baselines and Tailoring Guidance for Federal Information Systems and Organizations *(planned)*
SP 800-60 Vol. 1	Guide for Mapping Types of Information and Information Systems to Security Categories
SP 800-60 Vol. 2	Guide for Mapping Types of Information and Information Systems to Security Categories: Appendices

Featured Publications

SP 800-128	Guide for Security-Focused Configuration Management of Information Systems
SP 800-137	Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations
SP 800-137A	Assessing Information Security Continuous Monitoring (ISCM) Programs: Developing an ISCM Program Assessment *(planned)*
SP 800-160 Vol. 1	Systems Security Engineering: Considerations for Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems
SP 800-160 Vol. 2	Developing Cyber Resilient Systems: A Systems Security Engineering Approach
SP 800-161	Supply Chain Risk Management Practices for Federal Information Systems and Organizations
IR 8011	Automation Support for Security Control Assessments • Vol. 1: *Overview* • Vol. 2: *Hardware Asset Management* • Vol. 3: *Software Asset Management* • Vol. 4: *Software Vulnerability Management* (est. March 2020)



Resources and Engagement Opportunities

FISMA Implementation Project Website
https://csrc.nist.gov/Projects/risk-management

LEARN

General mailbox
sec-cert@nist.gov

PARTICIPATE

FISMA Implementation Project Mailing List
https://csrc.nist.gov/Projects/risk-management/mailing-list

CONTRIBUTE

NIST Cybersecurity Publications
https://csrc.nist.gov

Computer Security Resource Center (CSRC) email updates
https://public.govdelivery.com/accounts/USNIST/subscriber/new?qsp=USNIST_3

NIST Privacy Engineering Program
https://www.nist.gov/privacy-engineering

Resources and Engagement Opportunities

RMF 2.0 webcast
https://go.usa.gov/xENcs

LEARN

RMF Training (2-hour, on-demand CBT)
https://csrc.nist.gov/Projects/risk-management/rmf-training

PARTICIPATE

Federal Computer Security Managers (FCSM) Forum
https://csrc.nist.gov/Projects/Forum

CONTRIBUTE

NIST Security Control Overlay Repository (SCOR)
https://csrc.nist.gov/Projects/Risk-Management/scor

FCSM Forum Quarterly Meeting (April 21 & July 23, 2020, Gaithersburg, MD) (webcast option)
FCSM Forum 2-Day Conference (October 28-29, 2020, Gaithersburg, MD)
https://csrc.nist.gov/Projects/Forum/events

Advancing Cybersecurity Risk Management Conference (May 27-28, 2020, Gaithersburg, MD)
https://go.usa.gov/xdqnx

STAY IN TOUCH

CONTACT US

sec-cert@nist.gov
privacyeng@nist.gov

@NISTcyber

Backup Slides

OMB Circular A-130

Office of Management and Budget (OMB) Circular A-130, *Managing Information as a Strategic Resource:*

- requires executive agencies with the federal government to **implement the RMF** that is described in NIST Special Publication 800-37
- requires agencies to **integrate privacy** into the RMF process
- addresses **responsibilities** for protecting federal information resources and for managing personally identifiable information (PII)
- requires agencies to: **plan** for security; ensure that appropriate officials are assigned security **responsibility**; periodically **review** the security controls in their systems; **authorize** system processing prior to operations and, periodically, thereafter

Risk

- A measure of the extent to which an entity is threatened by a potential circumstance or event

- A function of:
  - **Adverse impact that would occur**
  - **Likelihood of occurrence**

- Four Risk Factors:
  - **Threat**
  - **Vulnerability**
  - **Impact**
  - **Likelihood**

RISK CAN NEVER BE ELIMINATED

RISK NEEDS TO BE MANAGED

MANAGING RISK DOESN'T MEAN FIXING EVERYTHING, NOR DOES IT MEAN NOT FIXING ANYTHING

Organizational Risk

Risk Management Definitions

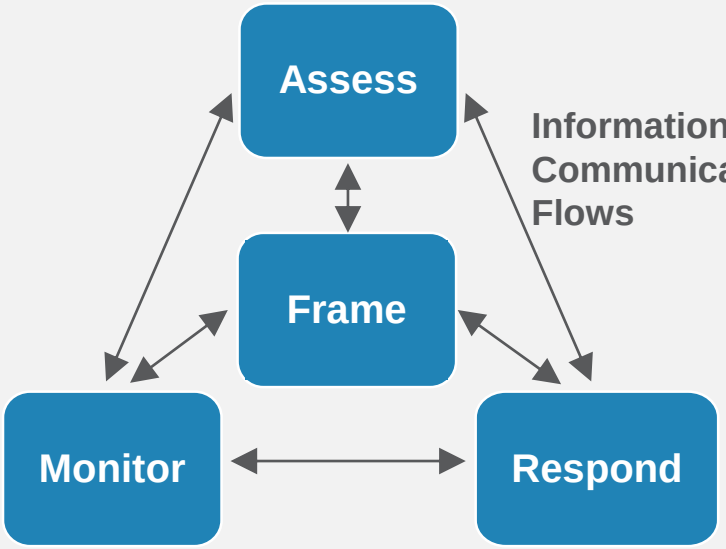
"**Risk Management**: the program and supporting processes to **manage risk** to agency operations (including mission, functions, image, reputation), agency assets, individuals, other organizations, and the Nation, and includes: **(i) establishing the context for risk-related activities; (ii) assessing risk; (iii) responding to risk once determined; and (iv) monitoring risk over time.**" (from NIST Special Publication 800-37, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*)

"**Risk Management** addresses **protecting** [Commonwealth of Virginia] information and IT systems **commensurate with sensitivity and risk**, including system availability needs. Accordingly, Risk Management is a central component of an agency information security program and allows each agency to determine how these factors apply to its IT systems and data." (from *Commonwealth of Virginia Information Technology Resource Management - Information Security Policy*)

Risk Management Process

FRAME:
- Assumptions
- Constraints
- Tolerance
- Priorities & Tradeoffs

ASSESS:
- Threat & Vulnerability Identification
- Risk Determination



Risk Management Process

RESPOND:
- Response identification
- Evaluation of alternatives
- Response decision
- Response implementation

MONITOR:
- Monitoring strategy
- Monitoring

Organization-Wide Risk Management

Three Levels of Organization-Wide Risk Management

RMF Purpose

To ensure that managing risk from systems is consistent with mission/business objectives and the overall risk strategy established by the senior leadership through the risk executive (function)

To ensure that security and privacy requirements, including necessary controls, are integrated into the organization's enterprise architecture and system development life cycle processes

To achieve more secure information and systems through the implementation of appropriate risk response strategies

To establish **responsibility and accountability** for the security and privacy of organizational systems/information/environments of operation

To provide senior leaders the necessary information to take credible, risk-based decisions with regard to the security and privacy of systems supporting organizational missions and business functions

Roles and Responsibilities

Authorizing Official	Risk Executive (Function)
Authorizing Official Designated Representative	Security or Privacy Architect
Chief Acquisition Officer	Senior Accountable Official for Risk Management
Chief Information Officer	Senior Agency Information Security Officer
Common Control Provider	Senior Agency Official for Privacy
Control Assessor	System Administrator
Enterprise Architect	System Owner
Head of Agency	System Security or Privacy Officer
Information Owner or Steward	System Security or Privacy Engineer
Mission or Business Owner	System User

Authorization Types, Options & Decisions

AUTHORIZATION TYPE
Initial Authorization
Ongoing Authorization
Reauthorization

OTHER OPTIONS
Type Authorization
Facility Authorization
Traditional or Joint Authorization

AUTHORIZATION DECISION
Authorization To Operate (ATO)
Common Control Authorization
Authorization To Use
Denial of Authorization

NIST Frameworks

RISK MANAGEMENT FRAMEWORK (RMF)	CYBERSECURITY FRAMEWORK (RMF)	PRIVACY FRAMEWORK
Originally developed for federal information systems	Originally developed for Industrial Control Systems (ICS)	Established to meet the need for a common language and practical tool to address privacy needs.
Required for federal systems (per OMB A-130); **can be adopted by any organization**	Required for federal systems (per EO 13800); **can be adopted by any organization**	Voluntary framework**; can be adopted by any organization**
Seven steps: • Prepare • Categorize • Select • Implement • Assess • Authorize • Monitor	Five concurrent and continuous functions: • Identify (ID) • Protect (PR) • Detect (DE) • Respond (RS) • Recover (RC)	Five functions for managing privacy risks arising from data processing: • Identify-P • Govern-P • Control-P • Communicate-P • Protect-P
SP 800-53 control catalog is integrated into the framework (SELECT step)	Categories equivalent to control families in SP 800-53	Mapping to SP 800-53 controls (and to other informative references)
Flexible (customizable)	Adaptive to provide a flexible and risk-based implementation that can be used with a broad array of risk management (RM) processes	Flexible, modeled after the CSF

NIST Frameworks

RISK MANAGEMENT FRAMEWORK (RMF)	CYBERSECURITY FRAMEWORK (RMF)	PRIVACY FRAMEWORK
	Use of tiers to describe an increasing degree of rigor and sophistication in RM practices	Use of tiers to describe current (privacy) risk management practices, the degree of integration of privacy risk into the organization's enterprise risk management portfolio, the organization's data processing ecosystem relationships, and the organization's workforce composition and training program.
In-depth methodology	High(er) level of abstraction (comp. to the RMF)	High(er) level of abstraction (comp. to the RMF)
Aligned with CSF • Inputs & outputs reference CSF as applicable; • Task outcome tables reference CSF sections, categories or subcategories as applicable; • References for tasks indicate relevant CSF sections (if any) Addresses security, privacy and supply chain risks	Provides a **common taxonomy** and mechanism for organizations to: • Describe their current cybersecurity posture; • Describe their target state for cybersecurity; • Identify and prioritize opportunities for improvement within the context of a continuous and repeatable process; • Assess progress toward the target state; • Communicate among internal and external stakeholders about cybersecurity risk.	Provides a **common language** to communicate privacy requirements with entities within the data processing ecosystem (particularly important when the data processing ecosystem crosses national boundaries such as international data transfers).
"Version 2.0" released December 2018	Version 1.1 released April 2018	Version 1.0 released in January 2020

NIST
CYBER


NIST Risk Management Framework (RMF) Overview
Tabassi


Outline


NIST, FISMA Implementation Project, RMF


The NIST Risk Management Framework

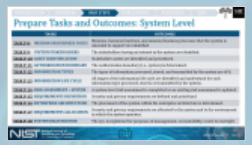

NIST Special Publication 800-37 Revision 2


NIST RMF Steps
PREPARE Step
CATEGORIZE Step
SELECT Step
IMPLEMENT Step
ASSESS Step
AUTHORIZE Step
MONITOR Step


Prepare Step


Task Structure


Prepare Tasks and Outcomes: Organization Level


Prepare Tasks and Outcomes: System Level


Categorize Step


Categorize Tasks and Outcomes


Select Step


Select Tasks and Outcomes


Select Step: SP 800-53 Control Families


Implement Step


Assess Step


Assess Tasks and Outcomes


Authorize Step


Authorize Tasks and Outcomes


Monitor Step


Monitor Tasks and Outcomes


Final Thoughts

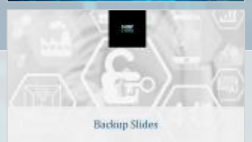

Featured Publications


Featured Publications

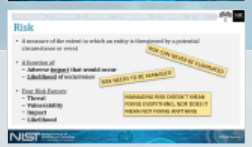

Resources and Engagement Opportunities


Resources and Engagement Opportunities

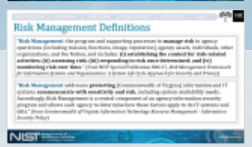

STAY IN TOUCH
CONTACT US


Backup Slides


OMB Circular A-130


Risk


Organizational Risk
organizational risk

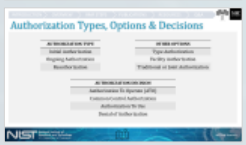

Risk Management Definitions


Risk Management Process


Organization-Wide Risk Management


RMF Purpose


Roles and Responsibilities


Authorization Types, Options & Decisions


NIST Frameworks

Servio Medina
Cybersecurity Oversight, Governance, & Strategy
Defense Health Agency, DAD IO/J-6

When Cybersecurity Impacts Healthcare: How to Get to Yes

March 4, 2020

Presented to The Virginia Information Technologies Agency

About me

- Worked cybersecurity: ~18 years
- Taught college math: ~10 years
- Federal employee since 2013
- Three kids since 2013

Photo credit: Robyn Vaughan

UNCLASSIFIED

Disclaimer

Content and opinions shared in this presentation, both written and verbal, are my own and not necessarily that of the Defense Health Agency or the Department of Defense

UNCLASSIFIED

Impacts to Healthcare

- Legally correct? *Yes*.
- Impacts healthcare? *Also yes*.

https://wreg.com/news/ambulance-gets-the-boot/

- Better?
- Necessary?

Recall WannaCry and cancelled NHS heart surgeries

https://www.mirror.co.uk/news/uk-news/fury-london-traffic-wardens-ticket-13222918

Example: 15-Minute Timeout/Screenlock

- Ticket for violation?
  - Control vulnerability: exploitation *has potential*
  - DoDIG finding
- Impact to healthcare?
  - Locked out during treatment
  - “Creative” workarounds
- How we got to yes
  - Conferred with PMO leadership
  - CIO/AO signed memo, *MHS Guidance on 15-Minute Automatic Timeout*, 3/18/2019

Photo credit: Servio Medina

Why Does this Happen?

Situation	COA	Tenure
Have an ailment?	Call the doc	Hippocrates (c.**460 - 370 BCE**), "father of modern medicine"
Got a legal concern?	Consult OGC	**1190 to 1230:** folks began to practice canon law as a lifelong profession in itself
Impacted by Cybersecurity?	Maybe we aren't really impacted…	The Morris Worm in **1983**

Not to mention

- IT/Cyber: "*you can't patch stupid*"
- Provider: "*we're saving lives – that's my job*"
- PEO: "*can't transform a user with 8 hours of training…in a classroom*"

DISCLAIMER

All events described herein actually happened, though on occasion I’ve taken certain, very small, liberties with details, chronology, etc.

Examples

Possibly okay	NOT OKAY
15-Minute screen timeout	Wiggle mouse with elbow
Removing files when departing	20G of .PST and 3 years of files
Transmitting files *to/from* .mil, .gov, .com	*from/to* non-GFE, including PII/PHI
Transfer files to/from government equipment	With flash drive
Saving files to the local shared drive; to cloud	Including PHI/PII
Transcription services	On CTR laptop, at CTR home
Using free/public web services	For healthcare scheduling
Defibrillator pulled from use in MTF	Because it had built-in, unauthorized WI-FI
Access DoD data/EHR	With personal device
Use Amazon Echo or Google Home	On your work desk (NOT kidding)
Text and email PHI	With personal equipment/account
Lab Analyzer kept on loading dock	No ATO (no RMF/assessment of risk)
Student Intern cannot access network/EHR	Background investigation takes too long; no CAC
Cybersecurity training	Sometimes the question doesn't even make sense

Impact to Yes

- Lab Analyzer kept on loading dock - did not have an ATO or any RMF effort
- Saving PII/PHI to the local shared drive; to cloud
- DoD (MIL/CIV) official removing .PST and shared drive files when departing or retiring
- Student Intern (and even visiting provider) cannot access network “because” background investigation takes too long, no CAC

How to Get to Yes…*After* *Impact*

- **See Something? Say Something!**
  - Let someone know before trying a workaround: CIO, CMIO, ISSM…a Functional or other leader's attention

- Report functional impacts of operational and technical issues that prevent full implementation and compliance
- Establish/Promote processes to support

How to Get to Yes…*Before* *Impact*

- **Do something before it happens**
  - Bake cybersecurity into healthcare
  - Equate poor cyber behavior with poor clinical care
  - Make the right choice an easier choice
  - Bake healthcare into cybersecurity

Do Something	How Do Something
Bake cybersecurity in	What do providers need a year from now?
Poor cyber = Poor care	Cybersecurity part of patient safety - even after treatment
Right = Informed choice	Knowledge Base: https://info.health.mil/dadio/infosec/Pages/KnowledgeBase.aspx
Bake healthcare in	Get providers involved in messaging

Impact of Training?

If someone plugs in their personal smartphone to charge, should their network privileges be suspended?

Should the violator be required to take the same annual, cyber awareness training – you know, the same training they already took?

Should you have to take the driver's license test again if you are caught speeding?

What's the Point of Training?

Risky Behavior

Risky Driving	Curb Risky Behavior
Reckless	Quick/frequent ticket
Texting	Increase risk awareness
W/o Seatbelt	Click it or Ticket
Fatigued	Rumble strips

Photo credit: Servio Medina

Nudge Them to Do the Right Thing

A nudge is any noncoercive alteration in the context in which people make decisions

- placing fruit at eye level in school cafeterias: enhances its popularity by as much as 25%

- a fly etched into the wells of urinals, giving male patrons something to aim at: spillage was reduced by 80%

Source: The Chronicle Review on Sunstein's *Nudge: Improving Decisions About Health, Wealth, and Happiness,* May 9, 2008

Nudge Example

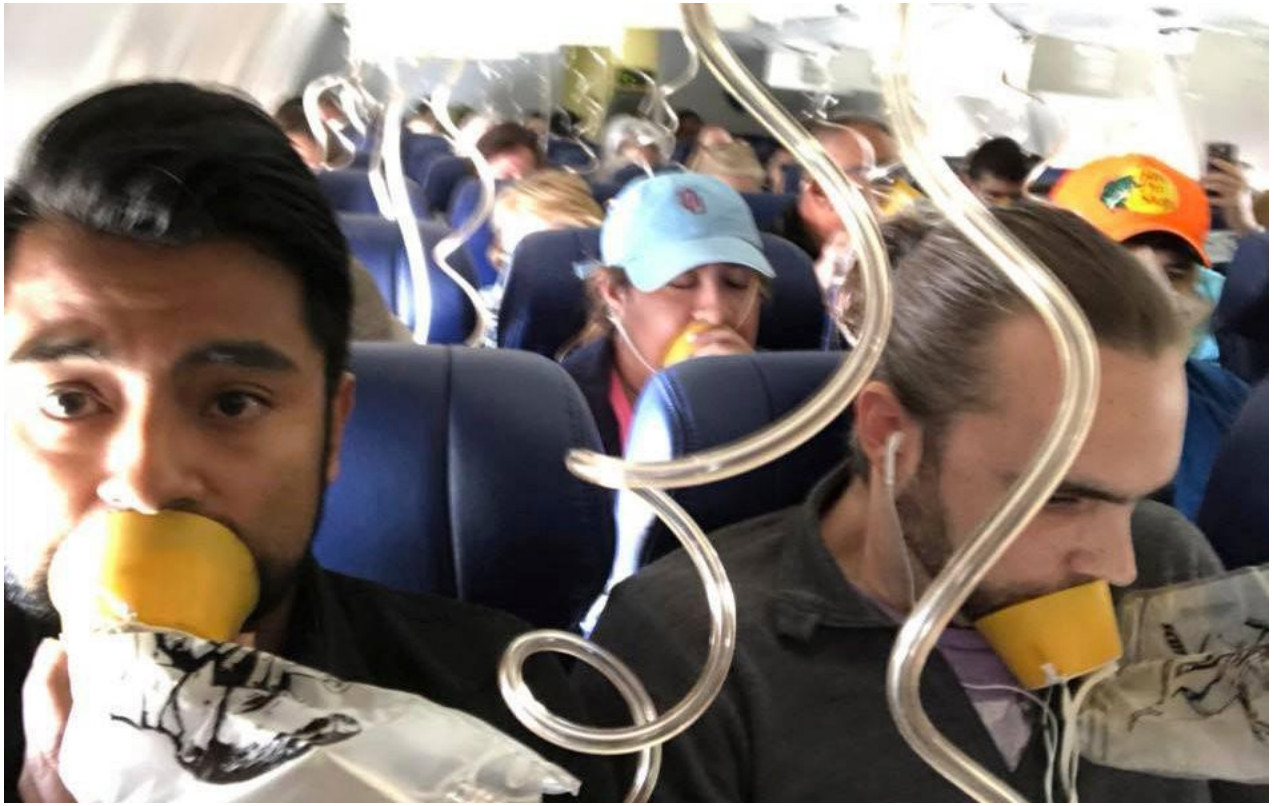
Airline Safety Videos

US Airways Flight 1549 crash landed in the Hudson

Only 4 of 150 passengers properly put on their life vest

Source: WSJ

Airline Safety Videos



What's wrong with this picture?

Source: CNN

Airline Safety Videos

New Zealand Air

Source: https://www.nytimes.com/2017/07/19/travel/british-airways-flight-safety-videos.html

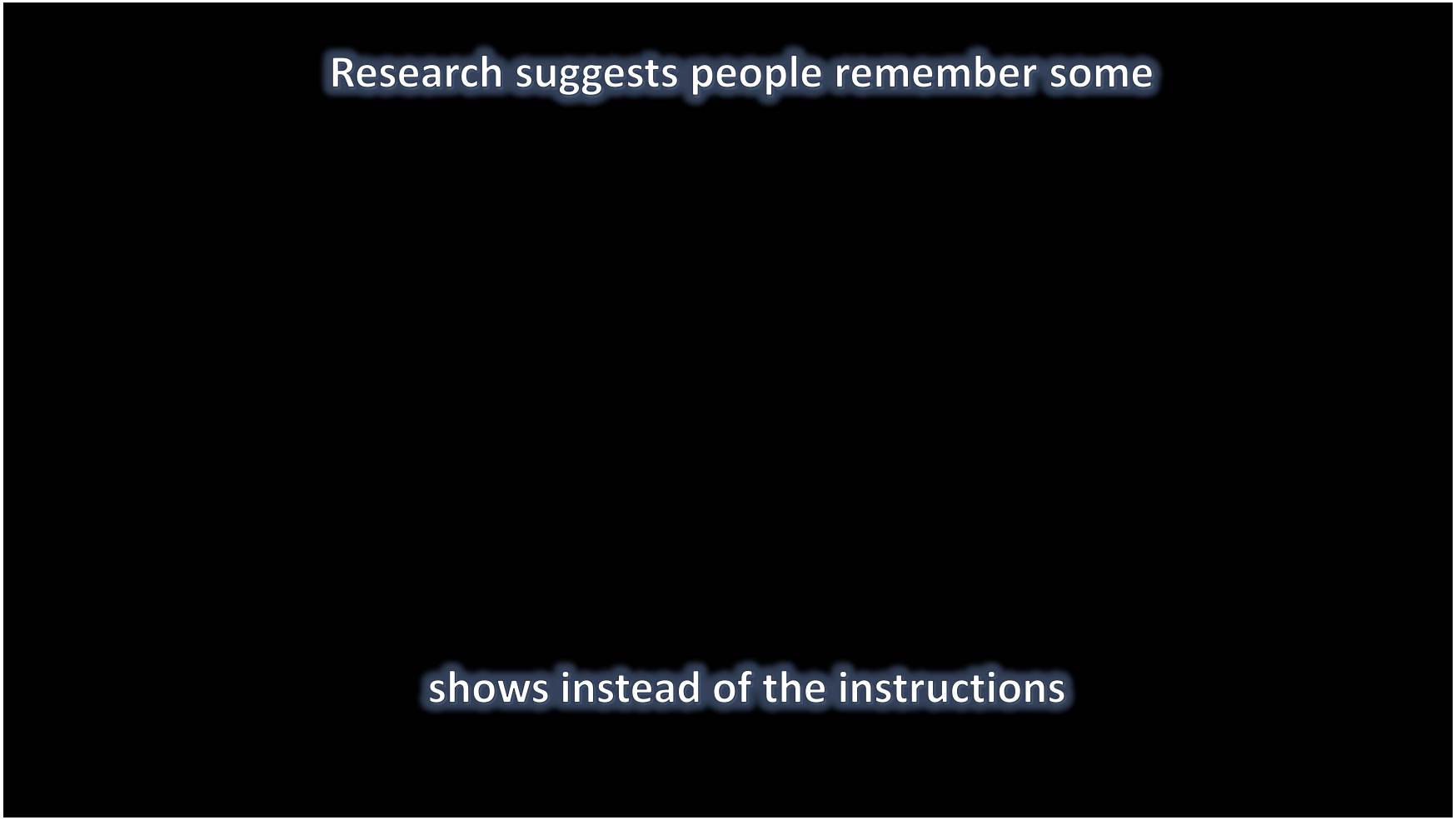
Airline Safety Videos

Source: https://www.nytimes.com/2017/07/19/travel/british-airways-flight-safety-videos.html

Airline Safety Videos

Virgin Airlines

Defense Health Agency



Source: https://www.wsj.com/articles/passengers-to-airlines-enough-with-the-wacky-safety-videos-1477320357

Controls + Train + Nudge + Process = Compliance? +Culture

Defense Health Agency

- **FLUENT**: leaders and their staffs need to be "cyber fluent" so they can fully understand the cybersecurity implications of their decisions. *2018 DoD Cyber Strategy*
- **FIT**: ongoing promotional campaign directed at 9.5M beneficiaries. *Defense Health Agency, 2016-Present*
- **HYGIENE**: cybersecurity hygiene = personal hygiene in that it is the individual's responsibility; it includes all online behaviors. *2017 Health Care Industry Cybersecurity Task Force Recommendation*

Questions?

Feel free to contact me:

- servio.f.medina.civ@mail.mil

Plus ça change
Plus ç'est la même chose
~Rush, Circumstances

Possibly (NOT) okay

- 15-Minute screen timeout. Got to Yes: memo signed by AO/CIO granting exception for OR and other restricted areas: up to 4 hours after coordination with PMO.
- Transmitting PII/PHI *to/from*.mil, .gov, .com *–from/to* non GFE. Got to Yes: DoD SAFE.
- Transfer files to government equipment from flash. Getting to Yes: depends on device, requires AO approval.
- CTR transcription services with non-GFE computer at home. Got to Yes: enforced a business associate agreement that already stipulated GFE for use.
- Using free/public web services for healthcare scheduling. Getting to Yes: bring IT (enterprise) capability needs through Governance
- Defibrillator pulled from use in MTF bc built-in wi-fi. Got to Yes: coordinated with MEDLOG
- Access DoD data/EMR with personal device. Got to Yes: Citrix/AVHE
- Use Amazon Echo or Google Home…on desk…at work (NOT kidding). Getting to No? OPSEC/Privacy policy prohibits recording/sending official business on non-GFE. BUT, this capability is in Every. Smart. Phone, so…
- Text and email PHI with personal equipment/account. Getting to Yes: understand the requirement and what is not working *–from the healthcare providers' perspective*
- Cybersecurity training answers *and even questions* do not make sense to some providers. Getting to Yes: provide contextually meaningful training supplemental to vice relying on the 1 hour of mandatory training.

Virginia Information Technologies Agency

Quantitative Cyber Risk Analysis

Risk Management Team
Commonwealth Security and Risk Management

3/4/2020

Objective

- To develop an accurate and defendable methodology to estimate costs associated with the detection, response, and recovery activities associated with cyber security incidents within the Commonwealth Executive Branch, independent agencies and institutions of higher education.

Purpose

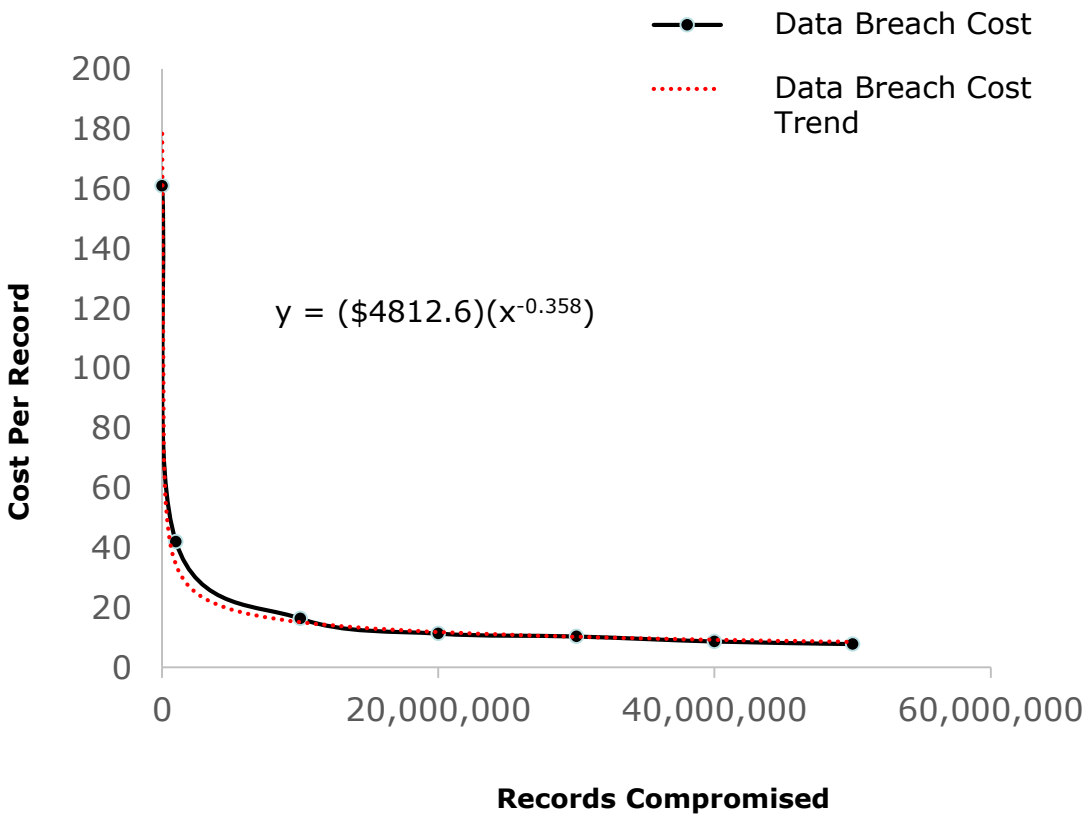
- Provide Executive leadership an enhanced ability to make informed risk based decisions:
  - IT Investments
  - Security enhancements
  - Security exceptions
  - Cyber liability insurance
  - Protect AAA Bond Rating
  - Understand the reputational risks

Model Component Definitions

- Baseline risk
  - Risk incurred for agencies with basic cyber hygiene program
  - Each application measured for likelihood of breach and impact of breach
- Residual risk
  - Risk incurred by the Commonwealth after identifying missing security controls
  - Missing controls increase the likelihood of a breach
- Loss Event cost estimate
  - Based on industry trends and Commonwealth costs
  - Formula based on line of best fit for data collected

Data Breach Cost Calculation

- As the number of compromised records increases, the cost exponentially decays
- Commonwealth analysis produced a cost factor of $4,812.60 for 2019
- Industry estimates include direct and indirect response cost



Data Breach Cost Range

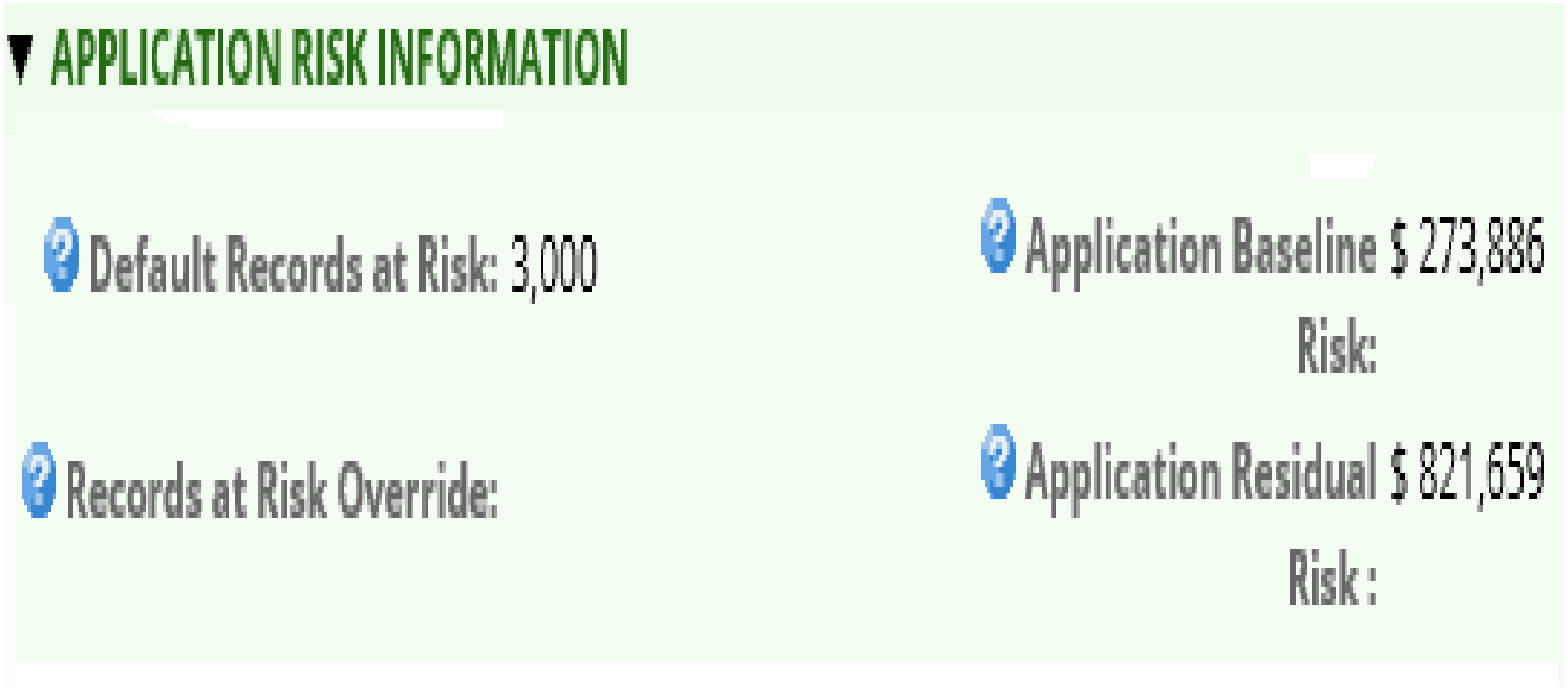
- Industry standard is the high end of the range
- Data breaches result in both direct and indirect costs
  - Direct cost is direct expense outlay to resolve the breach
  - Indirect cost is time, effort and other organizational resources allocated to data breach resolution
- Commonwealth analysis removes some of the indirect costs associated with a data breach

Reputational Risk

- Represented by the number of citizens impacted by an incident

- May not directly correlate with the number of records impacted
  - Public safety
  - Transportation infrastructure
  - Critical infrastructure

Archer Fields



Application inherent risk

- This field utilizes either the default records at risk or the override as stated earlier, and uses the formula previously covered in order to determine the financial risk associated with the application.

Records at Risk Override

- If this field is filled out by the AITR, it will be used instead of the default.

Application Residual Risk

- This field takes the Inherent Risk Field and modifies it based upon the open findings, and their association to the CIS top 20 controls.

Application Residual Risk Calculation

- For each CIS control that the applcation doesn't meet, it will increase the risk, by 8% for Basic controls(1-6), 4% for foundational controls(7-16), and 3% for organizational controls(17-20), the maximum being 200% However, if there is no audit or risk assessment completed, there is instead a 3x multiplier placed on it.

Help Text

- Can be found on the above fields, and should help somewhat in clarifying them.

Questions

Upcoming Events

COV Information Security Conference

2020 vision: A future of innovation

April 16 & 17

Richmond, VA

Virginia Information Technologies Agency

COV Information Security Conference

2020 Security Conference Registration and Call for Papers

Registration for the 2020 Commonwealth of Virginia (COV) Information Security Conference is now open. The conference will be held on April 16 & 17 at the Altria Theater in Richmond. Deadline for Call for Papers is March 6.

Conference Cost: $175

Conference and registration information can be found on the link below.

https://www.vita.virginia.gov/commonwealth-security/cov-is-council/cov-information-security-conference/

For all other conference questions: covsecurityconference@vita.virginia.gov

Keynote Speaker – Day One

Susie Adams, Chief Technology Officer
Microsoft Federal

Keynote Speaker – Day One

Larry Weaver

Professional Comedian and Business Leader

IS Orientation 2020

The next IS Orientation will be held on

March 31, 2020

1p-3p in room 1211 (CESC)

Presenter: Marlon Cole (CSRM)

Registration Link:
http://vita2.virginia.gov/registration/Session.cfm?MeetingID=10

April ISOAG

Arlyn Burgess

Data Science opportunities and barriers: The power of partnership”

UVA School of Data Science

Alan Gernhardt

Public Records

Virginia Freedom of Information Advisory Council

Eric Culbertson

MSS Web Content Reporting Tool

ATOS

ADJOURN

THANK YOU FOR ATTENDING

Picture courtesy of www.v3.co.uk