



2023 IHS – OIT & ORAP Conference



Indian Health Service (IHS) Authority To Operate (ATO) Risk and Compliance (R&C) Security Assessment and Authorization (SA&A) Process

Presented by	Sam Tharakan Mathew
Title	R&C Federal Team Lead
Phone	(301) 526-8489
Email	Sam.Mathew@ihs.gov
Team Email	IHSDISRiskAndCompliance@ihs.gov
Target Date	24 August 2023
Target Start Time	10 :00 AM EST



DYK? – Atlanta, Georgia!

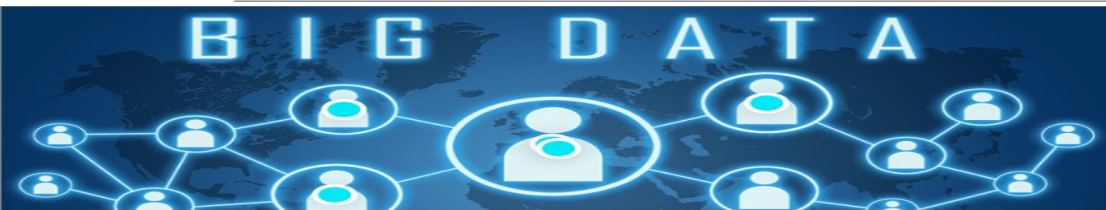


What is Atlanta, Georgia famous for, besides being home to the Coca-Cola headquarters and the busiest airport in America (and the world!)?

- **Before 1836, the Creek and Cherokee Native American people were the original inhabitants of the Atlanta area.**
- Atlanta is the 38th largest city in the United States, with some common nicknames for Atlanta are City in a Forest, Dogwood City, and Empire City of the South.
- The Atlanta flag features the state's coat of arms in gold on a blue background. The emblem has a phoenix rising from flames and the dates the city was incorporated (1847) and the end end of the Civil War (1865). Atlanta was the only city in North America destroyed as an act of war, and its symbol is a phoenix.
- The Georgia Aquarium in Atlanta was the largest in the world when it was first built in 2005 and remains the country's largest (and word's third largest) today.
- Atlanta has 5 major professional sports teams: Atlanta Falcons (NFL), Atlanta Hawks (NBA), Atlanta Braves (MLB), Atlanta Dream (WNBA) and Atlanta United (MLS).
- **Atlanta has the second-most shopping centers in the U.S.**
- There are over 55 streets with the name Peachtree in Atlanta.
- ...etc



World's Most Valuable Commodity



• **D.A.T.A.** is now becoming the most valuable commodity on earth, surpassing fossil fuels like oil.

• The BIG TECH giants that deal in data, such as Google, Amazon, Facebook, Apple, Microsoft and Tesla, are becoming increasingly powerful.

- **DYK?** *An individual's Facebook data may be worth over \$100, and one individual recently sold his data for \$2,733 on Kickstarter.*

Regulating the internet giants

The world's most valuable resource is no longer oil, but data

The data economy demands a new approach to antitrust rules





OIT-DIS Risk & Compliance Team



The Risk and Compliance (R&C) Team D2D Roles & Responsibilities:

- ✓ Aligns to the IHS-DIS objectives while managing the cyber risks, in order to achieve the regulatory needs (FISMA/HIPAA/GAO/A-123/OIG/BOD/HHS = 7+).
- ✓ Improves the security of IHS data by identifying gaps, categorizing and documenting security risks that have the potential to impact IHS's ability to satisfy its mission, vision, goals and priorities.
- ✓ Establishes governance, formality, ownership, and accountability by developing, conducting and updating security assessments for IHS-HQ and other related national systems.

Who's your PoC at the Risk & Compliance Team?

Sam Tharakan Mathew | MS, PMP, CISM, CISA, CASP+, CEH

Sam comes with a broad and diverse background in IT-OT engineering. He has attained his masters degree with multiple industry certifications in both IT-OT and project management. Over 15 years, Sam has significantly contributed as a key senior management consultant to the IT-OT cybersecurity programs at various private sectors and Federal Nuclear Energy facilities. Sam was also a member of the LexisNexis management team, where he established the LN-RT organization's first global GRC & Audit Department, which was responsible for overseeing and assisting the Federal USPTO's ATO mission, amongst other commercially globalized healthcare, intellectual property and financial compliance frameworks.



R&C Links

- [R&C SharePoint Site](#)
- [R&C Security Publications](#)
- [NIST 800-37 RMF](#)
- [NIST 800-53 InfoSec](#)
- [Archer GRC](#)
- [IHS Front Lines](#)

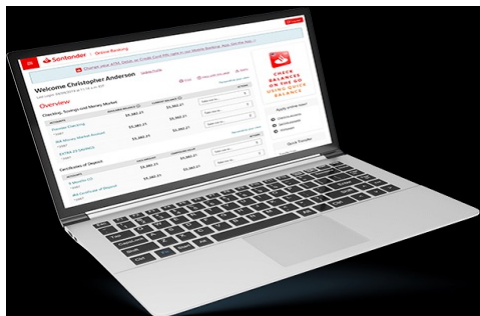




The C.I.A = ?

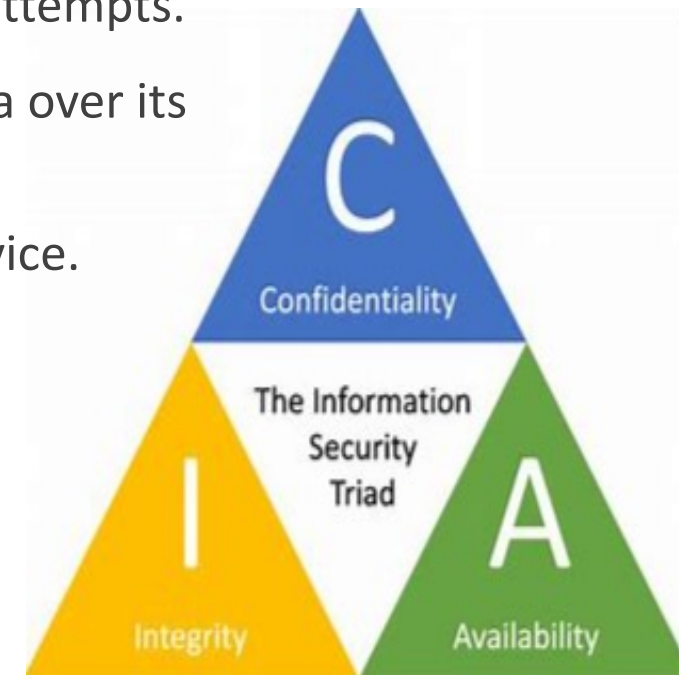
Confidentiality/ Integrity/ Availability (CIA) is a benchmark model that governs how the IHS protects its information systems and data.

- **Confidentiality** prevents privacy information from unauthorized access attempts.
- **Integrity** maintains the consistency, accuracy and trustworthiness of data over its entire lifecycle of service delivery
- **Availability** refers to the readiness of data that is required to deliver service.



NOTE: Consider an online banking account as an example.

*It is critical that the user's information is secret (**confidentiality**), accurate (**integrity**) and accessible (**availability**) at all times.*





IHS' Mission/ Vision/ Goals?

Indian Health Service
The Federal Health Program for American Indians and Alaska Natives

[A to Z Index](#)
[Employee Resources](#)
[Feedback](#)

The Indian Health Service is working closely with our tribal partners to coordinate a comprehensive public health response to both [COVID-19](#) and [mpox](#).

[About IHS](#)
[Locations](#)
[for Patients](#)
[for Providers](#)
[Community Health](#)
[Careers@IHS](#)
[Newsroom](#)

[About IHS](#) / Agency Overview

About IHS

Agency Overview

Annual Budget

Eligibility

Key Leaders

IHS Calendar

Indian Health Manual

Organizational Structure

Our Employees

Agency Overview

The Indian Health Service, an agency within the Department of Health and Human Services, is responsible for providing federal health services to American Indians and Alaska Natives. The provision of health services to members of federally-recognized tribes grew out of the special government-to-government relationship between the federal government and Indian tribes. This relationship, established in 1787, is based on Article I, Section 8 of the Constitution, and has been given form and substance by numerous treaties, laws, Supreme Court decisions, and Executive Orders. The IHS is the principal federal health care provider and health advocate for Indian people, and its goal is to raise their health status to the highest possible level. The IHS provides a comprehensive health service delivery system for American Indians and Alaska Natives.

Our Mission: to raise the physical, mental, social, and spiritual health of American Indians and Alaska Natives to the highest level

Our Vision: healthy communities and quality health care systems through strong partnerships and culturally responsive practices

Strategic goals:

- to ensure that comprehensive, culturally appropriate personal and public health services are available and accessible to American Indian and Alaska Native people;
- to promote excellence and quality through innovation of the Indian health system into an optimally performing organization; and
- to strengthen IHS program management and operations

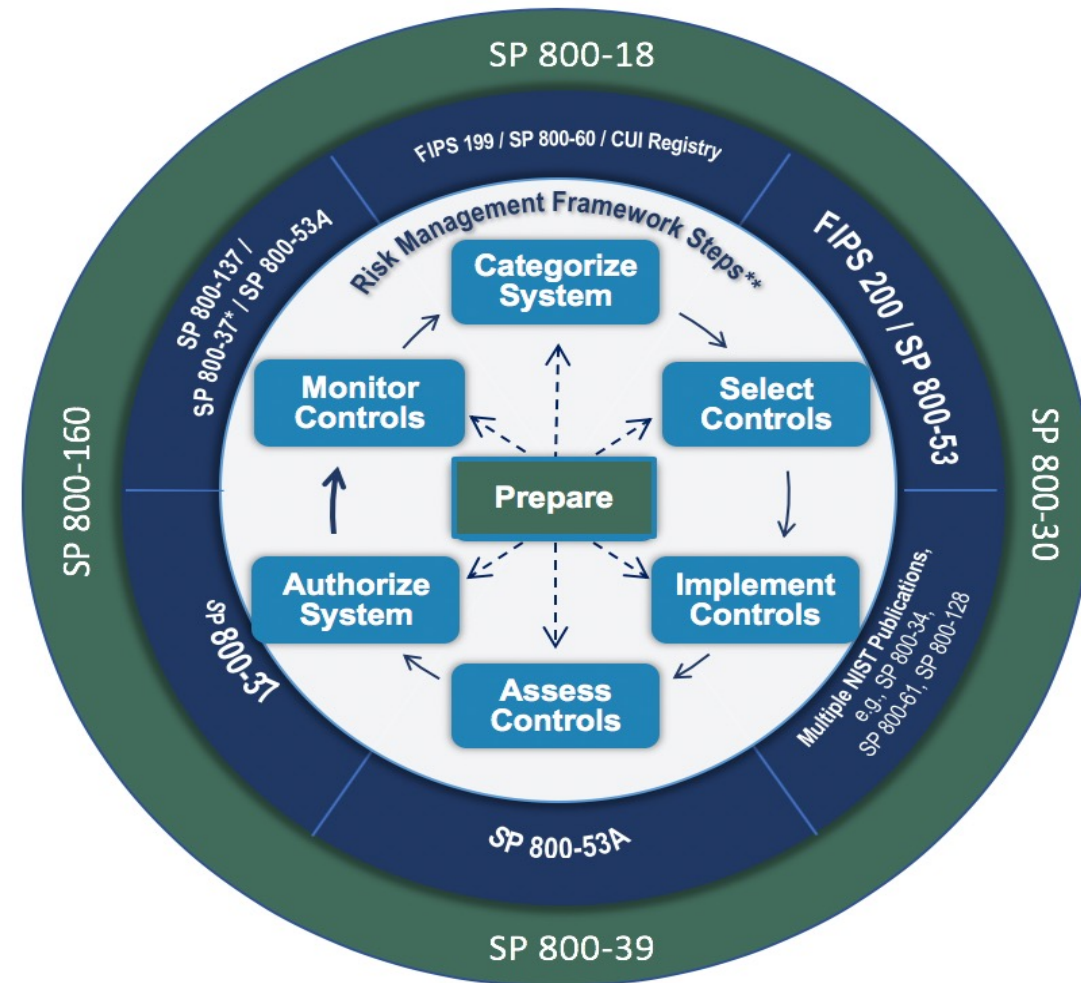
Related Information ⓘ

- [Fact Sheets](#)

Risk Management Framework (RMF)

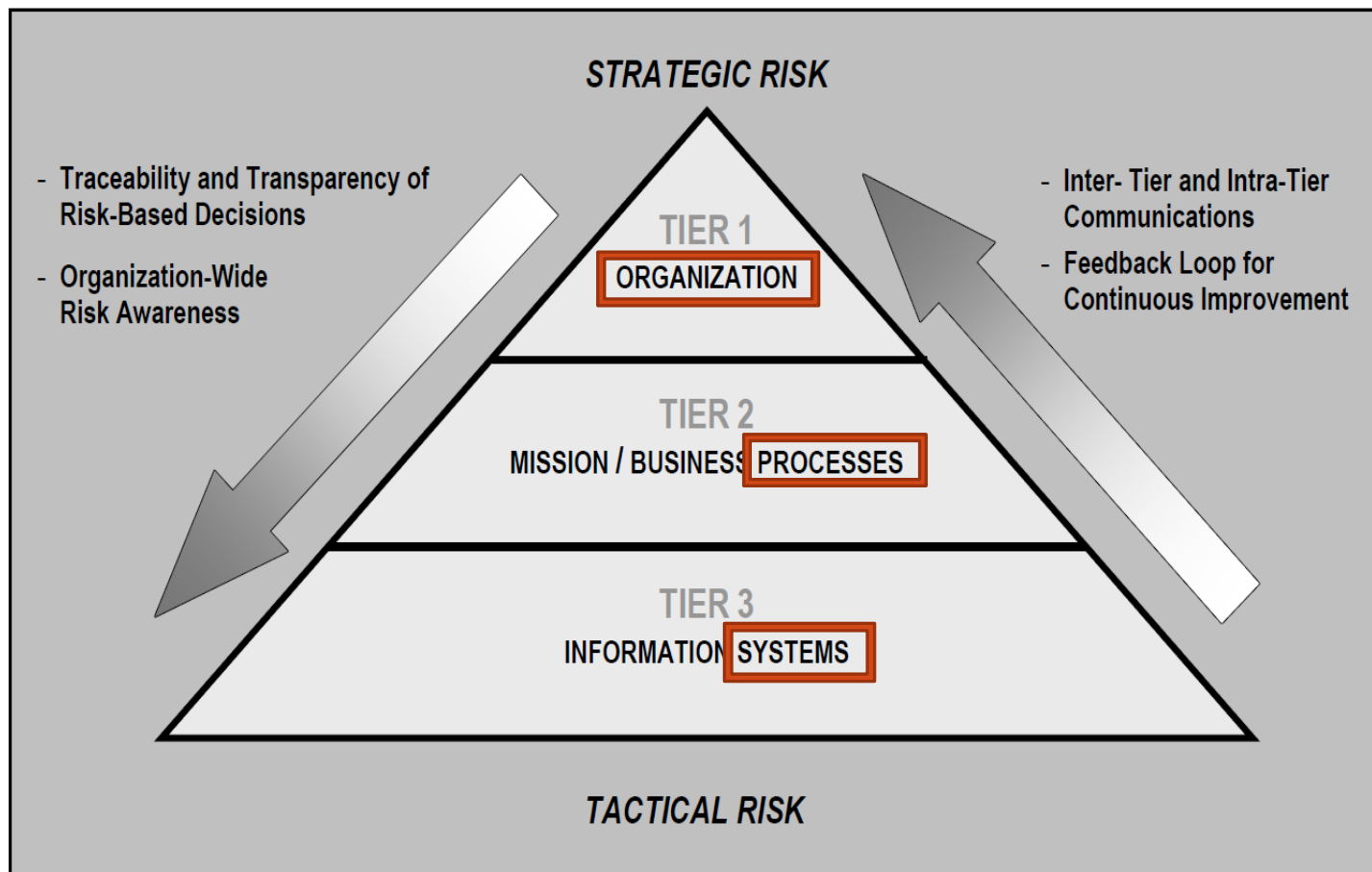
NIST SP 800-37, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy

The National Institute of Standards and Technology (NIST) Risk Management Framework (RMF) 800-37, provides guidelines that help ~~businesses and~~ government agencies comply with Federal Information Processing Standards (**FIPS**) requirements for information systems and data and NIST Special Publication **800-39** requirements.



3-TIER RISK MANAGEMENT

NIST SP 800-39, Chapter 2, Section 2.2, Managing Information Security Risk: Organization, Mission, and Information System View



- **Tier-1** provides a prioritization of missions/business functions which in turn drives investment and funding by strategic and tactical *decisions*.
- Thus, Tier-1, affects the development of enterprise/ InfoSec *architecture* at **Tier-2**
- Allocations and deployment of *management, operational,* and *technical* security controls at **Tier-3**

FIGURE 2: MULTITIERED ORGANIZATION-WIDE RISK MANAGEMENT

IHS' 3-TIER SYSTEM

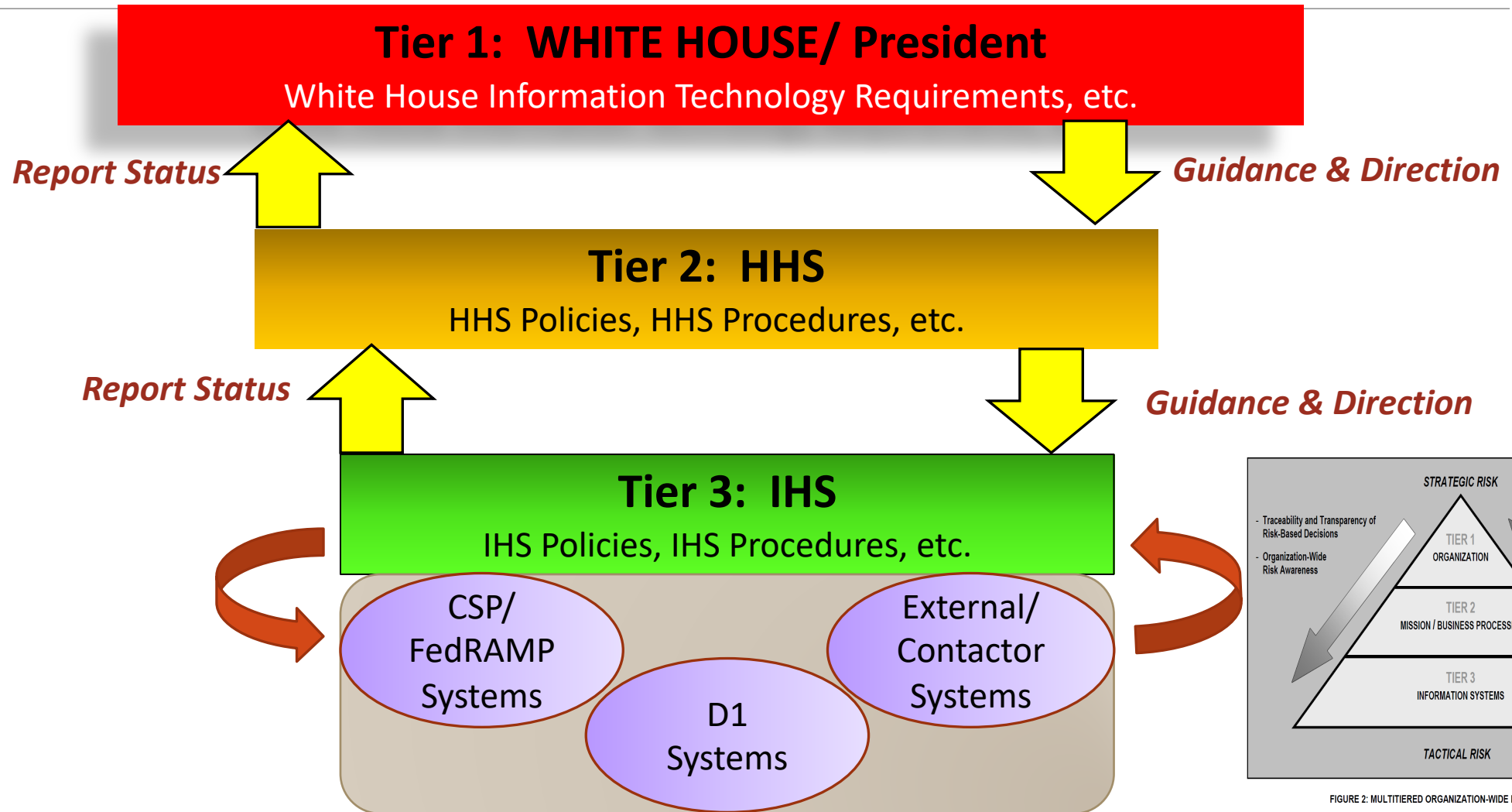


FIGURE 2: MULTITIERED ORGANIZATION-WIDE RISK MANAGEMENT

System Acronym	System Name
4DH	Four Directions Hub
AaaS	Authentication as a Service-OKTA
AD	Enterprise Network Management Services
AGRC	Archer Governance Risk and Compliance
ARMD	AA Ring MD
CEP MDS	IHS Credentialing Enterprise Program and MD-Staff
CHEF	Catastrophic Health Emergency Fund Online Tool
CRW	Crowdstrike
DFI	Digital Forensic Investigator
EDR	Electronic Dental Record
ENI	Enterprise Network Infrastructure
EPMT	Enterprise Portfolio Management Tool
EVVCM	Enterprise Voice and Video Collaboration Meetings
HBP	Hyperion Budget and Planning System
HQDC	Private Cloud and Data Center Infrastructure (Headquarters Data Center)
IAM	Identity Access Management
I-STAR	Safety Tracking and Response
ISTS	Information Security Ticketing System
ITSSS	IT System Security Scanner
MAS	Malware Analysis Sandbox
MCAS LC	Microsoft Cloud Application Security Log Collectors
MDM	IHS MaaS360 MDM System
MediTrax	MediTrax
MPI/HIE	Master Patient Index/ Health Information Exchange
MS365	MicroSoft 365
NPIRS	National Patient Information and Reporting System
OEHE	Office of Environmental Health and Engineering Web Applications
PHR/RPMS DIRECT	Personal Health Record/Resource and Patient Management System DIRECT Messaging
RPMS	Resource Patient Management System
SDTS	Secure Data Transfer Service
SEAT	Splunk Enterprise Adoption Tool
SN	ServiceNow
WEB	Web Services
Webex	IHS Secure Video and Web Conferencing System
XFS	XMEDIUM XM Fax System



46+

IHS SYSTEMS

(as of 19 Aug 2023)

- 35 @ Active ATOs
 - 8 @ FedRAMP/ CSPs
- 11 @ Pending TBDs

TBD System(s)	System Name
<ul style="list-style-type: none"> • 11 POSSIBLE NEW SYSTEMS IN PIPELINE NEEDING ATOs 	1) Armis
	2) Docusign
	3) HealthStream
	4) JVN Teleophthalmology
	5) LibreView
	6) Nuance Dragon
	7) Policy Stat
	8) Qgenda
	9) VistA
	10) XMEDIUM XM Fax System
	11) Zoom.gov



Why Do You Need Your System to be Authorized?



A properly authorized system provides IHS the following benefits:

- Adheres to federal security compliance guidelines: System states – Risk Awareness/ Avoidance/ Acceptance/ Transfer, (Vendor, Cloud, FedRAMP)
- Helps IHS define and maintain its asset inventory.
- Aligns with the IHS's mission, vision and strategic goals.
- Facilitates the appropriate level of system protection.





Obtaining System Authorization



To obtain an IHS system authorization, perform the following tasks:

- Work with the Division of Information Security's ISSOs!
- Ensure that the System Owner/Division Director has:
 - Officially registered the system in the RSA Archer Governance, Risk, And Compliance (GRC) system
 - Provided an HHS-IHS Universal Unique Identifier.
- Integrate information security in the system design and development.
- Complete and assemble required system documentation: start **8 months** prior to assessment start date.
- Conduct an initial full-scope assessment 3 months prior to deploying the system in a production environment.
- Continue to work with the Division of Information Security's ISSOs, R&C team to complete a System Assessment Report (SAR) and submit it to the AO/CIO to request an ATO.

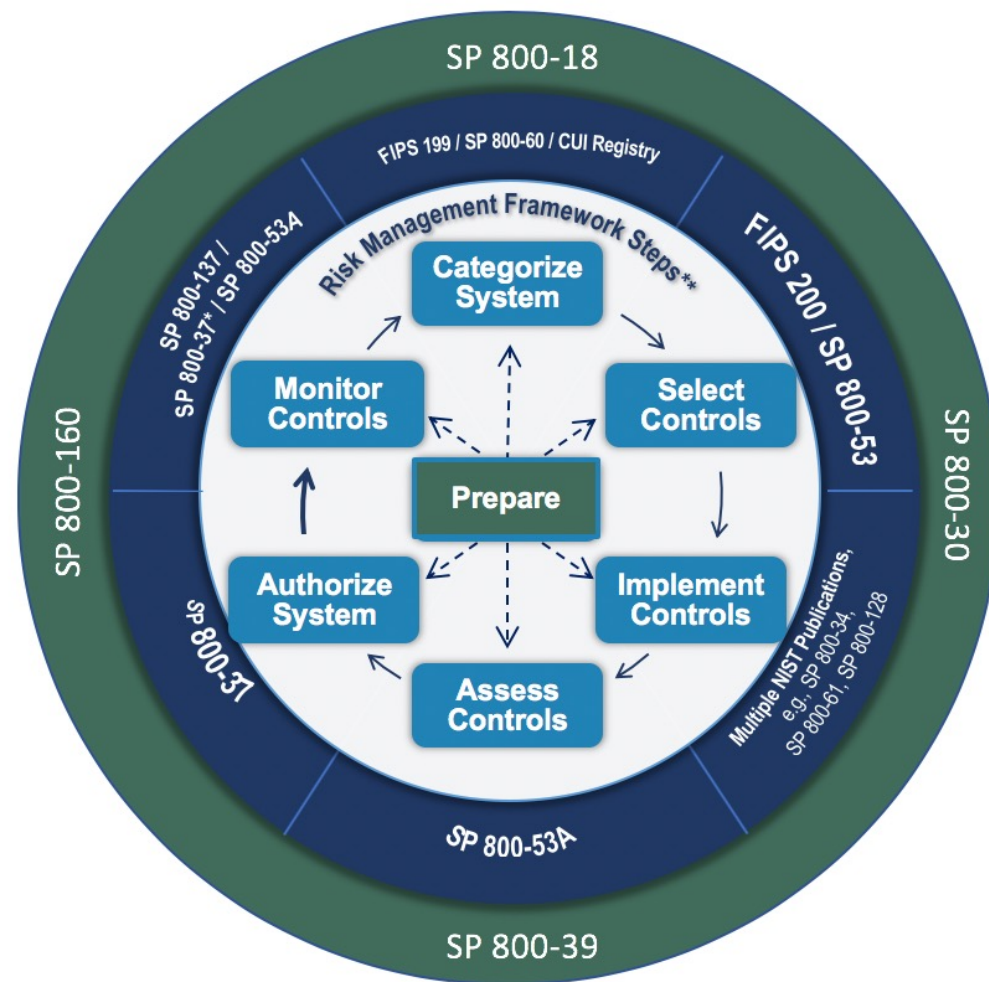


NIST-800-37/ Risk Management Framework

The National Institute of Standards and Technology (NIST) Risk Management Framework (RMF) 800-37, provides guidelines that help businesses and government agencies comply with Federal Information Processing Standards (FIPS) requirements for information systems and data and NIST Special Publication 800-39 requirements.

The NIST RMF consists of the following 6-Prep Steps:

- Step 1: Categorize Information Systems
- Step 2: Select Security Controls
- Step 3: Implement Security Controls
- **STEP 4: ASSESS SECURITY CONTROLS**
- Step 5: Authorize Information System
- Step 6: Monitor Security Controls





R&C Team' Playbo

- It is the System' - Security Assessment Plan (SAP)
- The CSA/ R&C Assessment Team is on hand to ca evaluation that complies with NIST-RMF, by utiliz methods described in NIST publications.
- In order to execute the SA&A process efficiently core references are utilized by R&C.
 - [NIST-SP-800-53A](#), *Assessing Security and Privacy Controls in Federal Information Systems*
 - [NIST-SP-800-115](#), *Technical Guide to Information Security Testing and Assessment*
 - [NIST-SP-800-137A](#), *Assessing InfoSec Continuous Monitoring (ISCM) Programs*
- The primary source of “my” verification and valid following:
 - Big-4-Plans: System' SSP [PL-2] + IRP [IR-8], CMP [CM-9], ISCP
 - System boundary Inventory [CM-8], against the scan results [F
 - IHS-DIS IS2P Baseline (OpDiv) Rev5 Handbook/ SOP
 - 3-Tier Common Controls, Policies and Procedures



Indian Health Service
Division of Information Security

Standard Operating Procedure for
Security Assessment and Authorization

DIS-SOP-22-04
Version 1.0
February 2023

CONTROLLED UNCLASSIFIED INFORMATION
Controlled with Standard Dissemination
This information is subject to safeguarding measures that reduce the risks of unauthorized or inadvertent disclosure. Dissemination is permitted to the extent that it would further the execution of a lawful or official purpose.



NIST 800-12

An Introduction to Information Security

- In accordance with **Section 5** of the National Institute of Standards and Technology (NIST) Special Publication (SP) **800-12**, Revision 1, **structuring policies and procedures should be as follows:**
- **Program Policy** – is used to create an organization’s information security program. Program policies set the strategic direction for security and assign resources for its implementation within the organization.
 - **These policies will be approved and issued by the CISO** to establish or restructure the Information Security Program.
 - Examples of these policies would be high level like **access control, risk management and media sanitizing.**
 - All IHS systems would follow these same policies and use them in their respective certification packages.
- **Issue Specific Policy** – There are many areas for which issue-specific policy may be appropriate.
 - New technologies and the discovery of new threats often require the creation of an issue-specific policy.
 - Examples of issue specific policies are **email privacy, social media, Bring Your Own Device (BYOD),** etc.
 - **These policies will also be approved and issued by the CISO as they affect IHS as a whole.**
- **System Policy** – While program and issue-specific policies are broad, high-level policies written to encompass ALL, system-specific policies provide information and direction on what actions are permitted on a particular system.
 - System policies dictate exactly how a system or component of the system will be securely configured.
 - Note, that one system specific policy could cover multiple systems, for example, **a DISA-STIGs** could be mandated for all systems, and specific STIGs or benchmark could be issued for specific system components (Windows, Linux, etc.).
 - **System policies should be crafted by the more technical personnel and may not be formally approved by CISO.**
- **DIS-PSA Team Function** – Before any policy goes to the CISO, the PSA Team will vet the policy against industry standard and best security practices and recommend change if any shortcoming is found to streamline the approval process.

5	Information Security Policy	26
	5.1 Standards, Guidelines, and Procedures.....	26
	5.2 Program Policy	27
	5.2.1 Basic Components of Program Policy.....	27
	5.3 Issue-Specific Policy	28
	5.3.1 Example Topics for Issue-Specific Policy.....	28
	5.3.2 Basic Components of Issue-Specific Policy.....	29
	5.4 System-Specific Policy	30
	5.4.1 Security Objectives.....	31
	5.4.2 Operational Security Rules.....	31
	5.4.3 System-Specific Policy Implementation.....	32
	5.5 Interdependencies.....	32
	5.6 Cost Considerations.....	33



NIST 800-53, Rev 5 Controls

- IHS conducts assessments on a 3-year cycle.
- Each year, IHS assesses one third of the controls along with any additional volatile controls.
- **NIST SP 800-53, Revision 5 provides a catalog of security controls grouped in control families. It also defines hundreds of control enhancements.**
 - *High baseline = 170 controls;*
 - *Moderate baseline = 159 controls;*
 - *Low baseline = 115 controls*

ID	Control Family	ID	Control Family
AC	Access Control	PE	Physical and Environmental Protection
AT	Awareness and Training	PL	Planning
AU	Audit and Accountability	PM	Program Management
CA	Security Assessment and Authorization	PS	Personnel Security
CM	Configuration Management	*PT(R5)	Personally Identifiable Information Protection 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(R5)	Supply Chain Risk Management



ATO Pre-Assessment Required Documents

The following documents need to be provided before a System' Security Assessment is conducted, in order for the R&C' Security Control Assessor (SCA) to perform the ATO assessment.

Pre-Assessment Documents	
Document Name/Type	Stakeholders
Cloud/FedRAMP (if applicable) – Rev 5	System Owner (SO), Information System Security Officer (ISSO), Chief Information Security Officer (CISO)
Privacy Impact Analysis (PIA)	SO, PO
Interconnection Security Agreement (ISA)	SO, ISSO, Interconnected System SO
System Security Plan (SSP) – Rev 5	SO, ISSO
Information System Contingency Plan (ISCP)	SO, ISSO, Disaster Recovery & Contingency Planning (DRCP)
Configuration Management Plan (CMP)	SO, ISSO, DRCP
Incident Response Plan (IRP)	SO, ISSO, DRCP

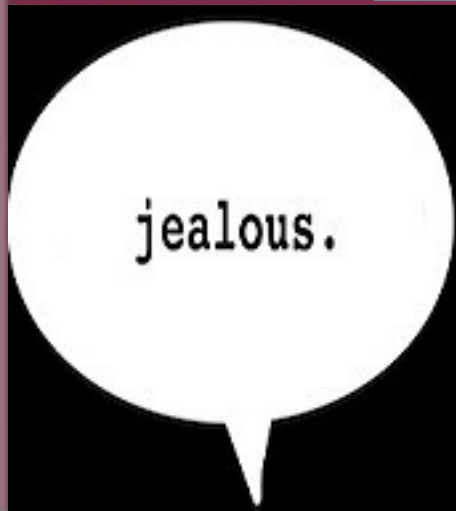
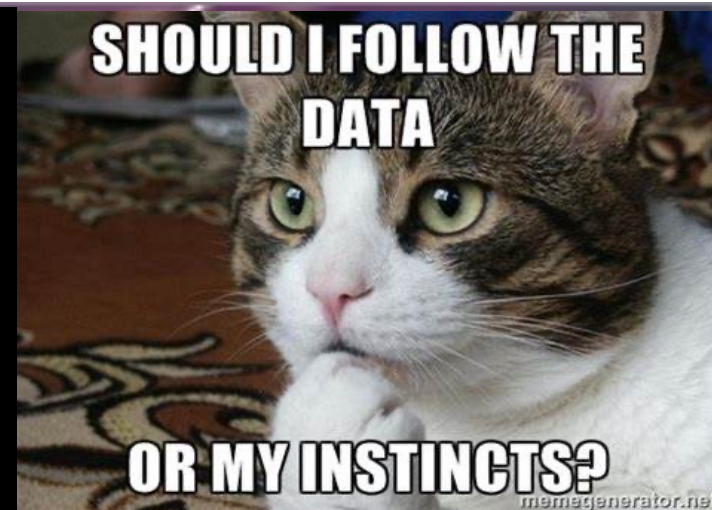




Follow The "What/Who"?



"Trust but Verify."
- Ronald Wilson Reagan



FOLLOW THE
DATA





ATO Post-Assessment Required Documents



The following documents are collected after a System Security Assessment. These documents comprise the ATO package.

Post-Assessment Documents	
Document Name/Type	Stakeholders
Security Assessment Plan (SAP)	SO, ISSO, SCA
Security Testing and Evaluation (ST&E)	SO, ISSO, SCA
Security Assessment Report (SAR)	SO, ISSO, CISO, SCA
Plan of Action and Milestones (POA&M)	SO, ISSO, CISO, Audit Response & Coordination (ARC)
Authorization to Operate (ATO) Memo	AO, CISO, SO, ISSO, SCA



Assessment Workflow Diagram (RMF Step 4)

DIS-SOP-22-04

Security Assessment and Authorization

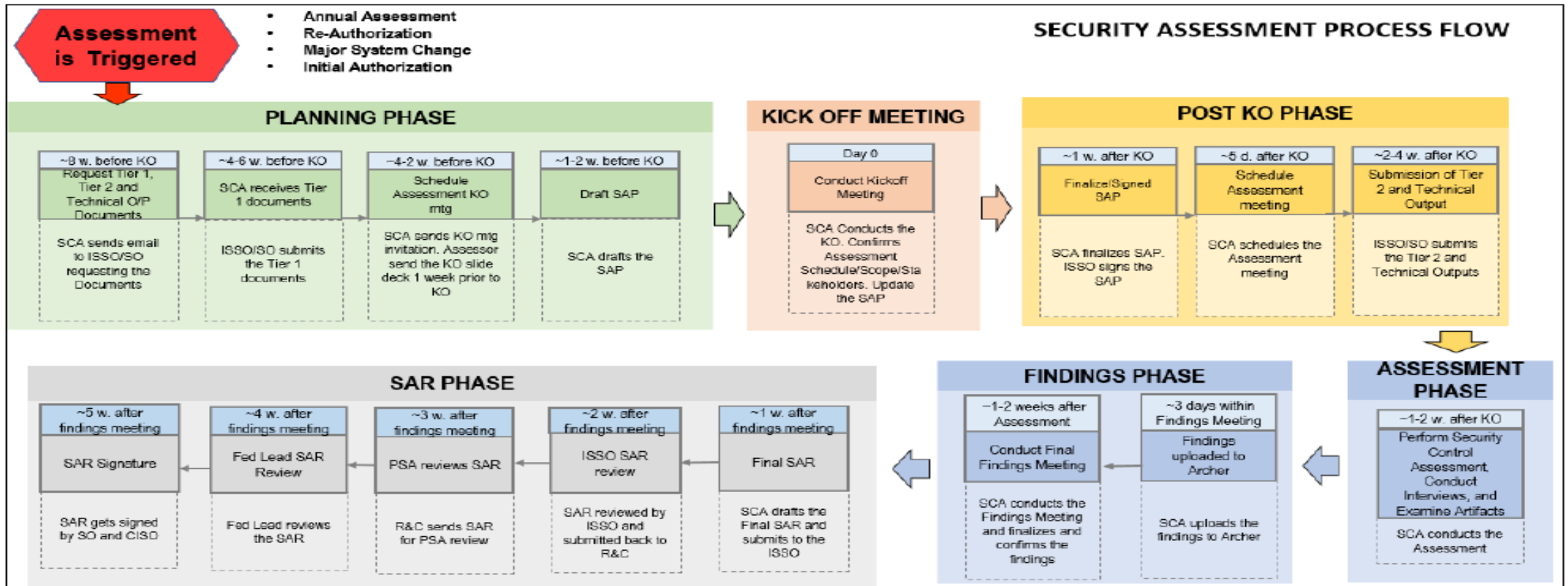


Figure 1: SA&A Process Flow

“Future” Assessment Workflow

NIST SP 800-53A Rev. 5

ASSESSING SECURITY AND PRIVACY CONTROLS IN INFORMATION SYSTEMS AND ORGANIZATIONS

Figure 8 summarizes the security and privacy control assessment process, including the activities carried out before, during, and after the assessment.

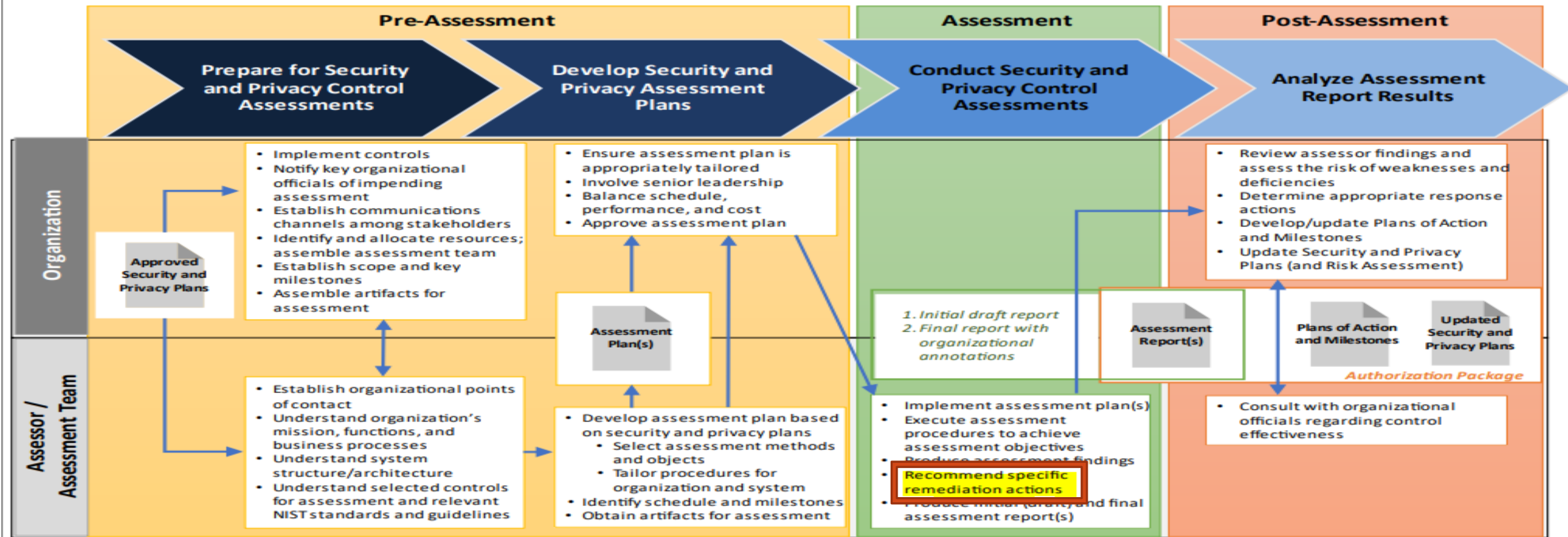


FIGURE 8: SECURITY AND PRIVACY CONTROL ASSESSMENT PROCESS OVERVIEW

NIST SP 800-55
Performance Measurement
Guide for Information
Security

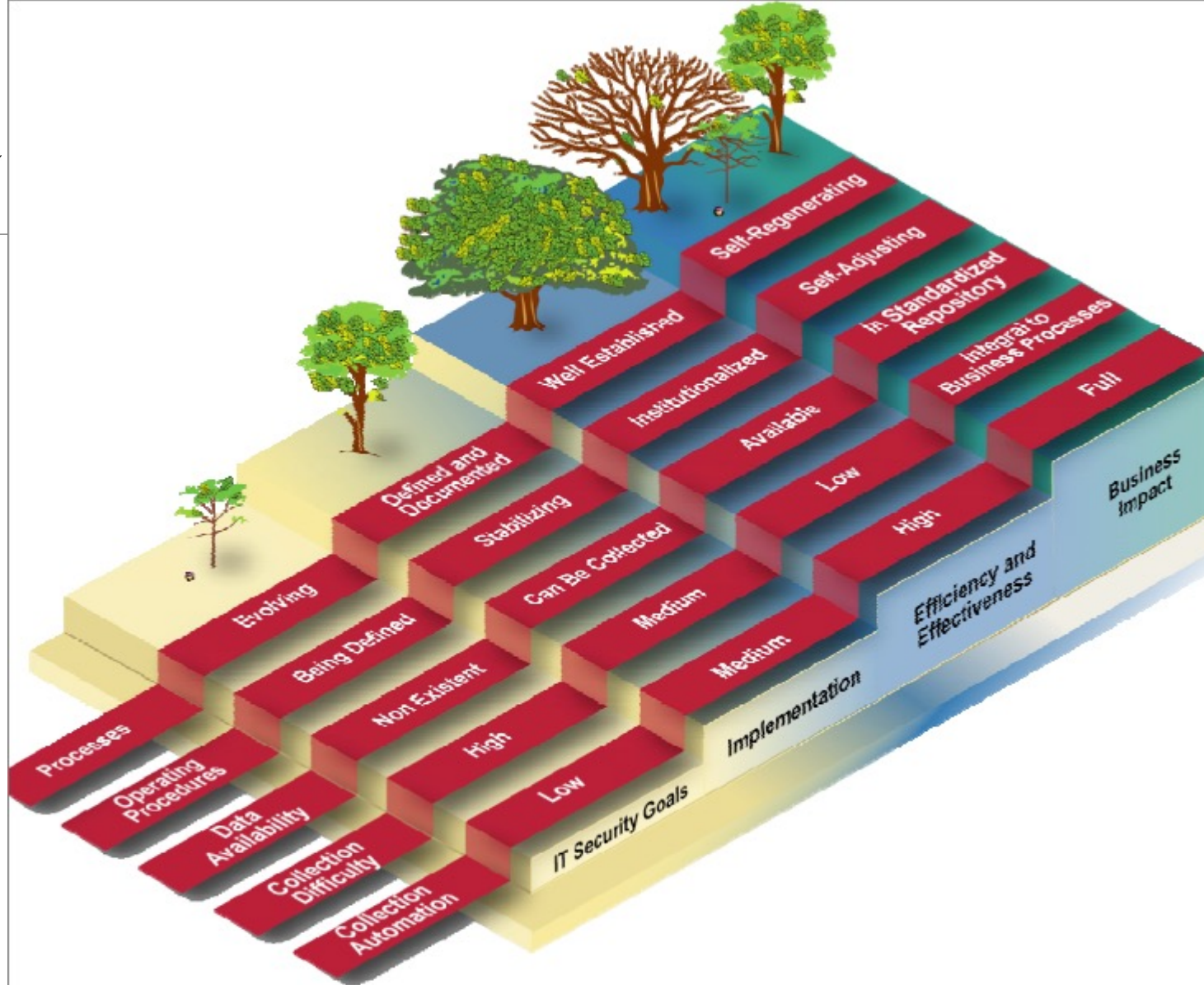
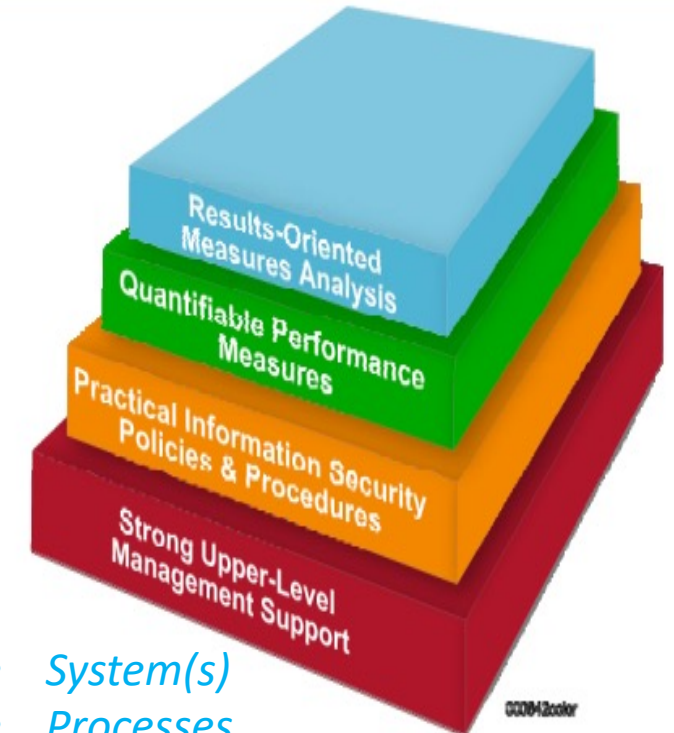


Figure 3-1. Information Security Program Maturity and Types of Measurement



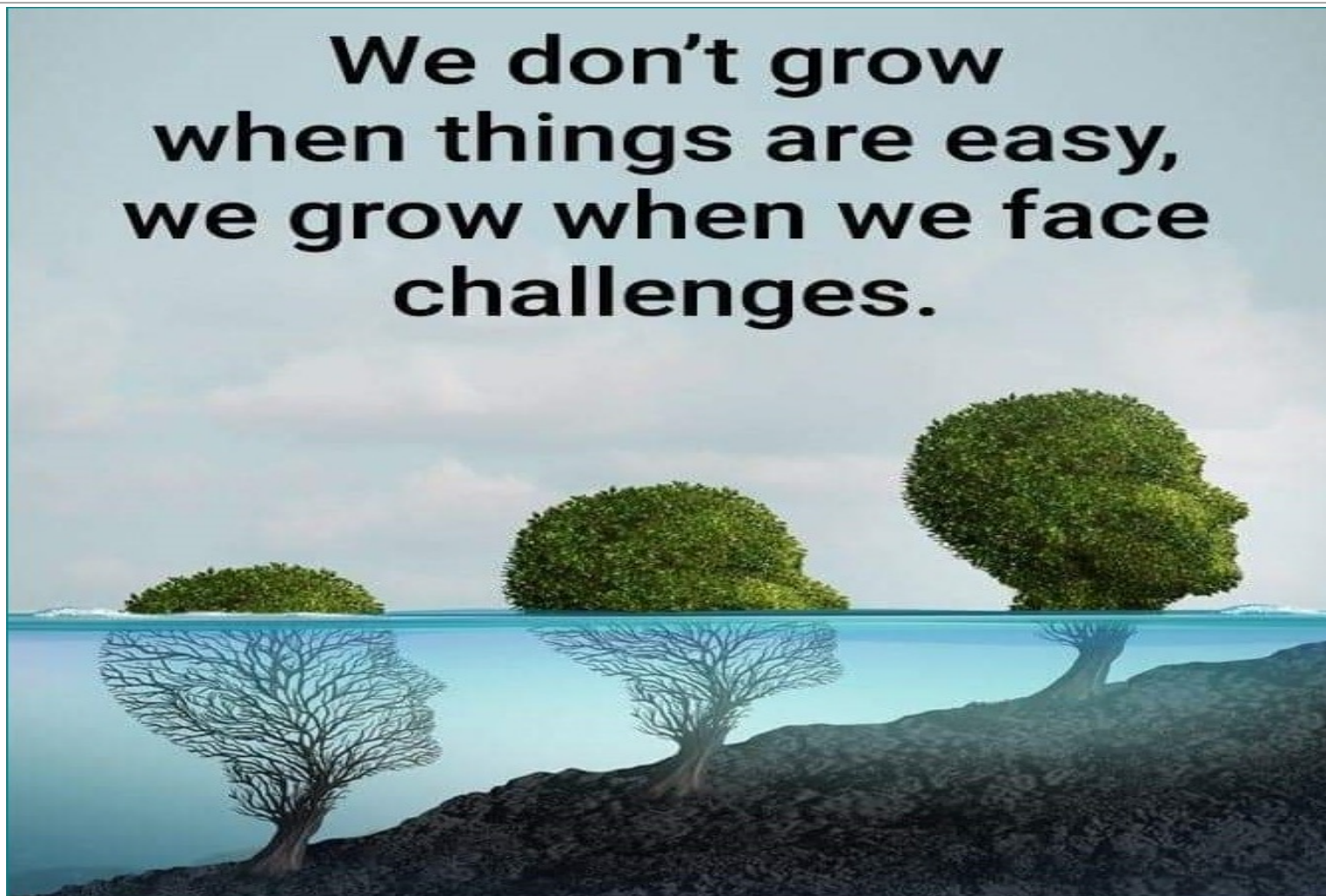
- System(s)
- Processes
- SOPs

Figure 1-1. Information Security Measurement Program Structure



When do we grow?

**We don't grow
when things are easy,
we grow when we face
challenges.**





Parkinson's Law?

The 4-W's:

Why - doing this objective/ project?

- Framework Requirements?

What - will be done & what resources are needed?

- Implementation impacts and the equipment required to perform

Who - is responsible for implementation?

- Identify the personnel's duty in day to day operations

When - is the estimated date of completion?

- SOPs documented, is the objective actually implemented, if not, by when?

Parkinson's Law

If you allow the task to take any amount of your time, then the work will expand proportionally!

Parkinson's law says: "Work expands so as to fill the time available for its completion". So! **The more time you allow for your task, the longer it will take to complete it.**



What does RACI stand for?

RACI is an acronym for responsible, accountable, consulted, and informed. Each represents the roles and levels of involvement of a stakeholder against the corresponding task/milestone. Let's dive into the definition of each term.

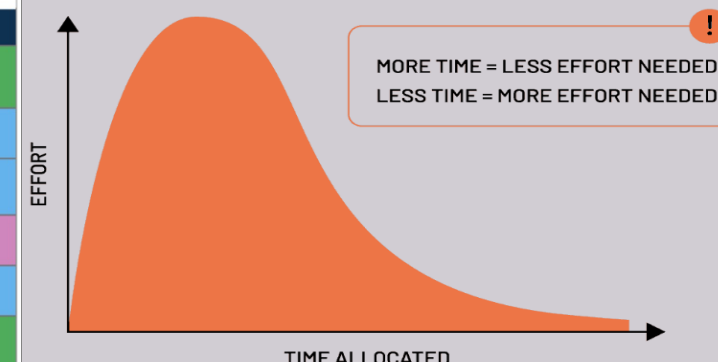
Responsible	Who is <i>responsible</i> for doing the actual work for the project task.
Accountable	Who is <i>accountable</i> for the success of the task and is the decision-maker. Typically the project manager.*
Consulted	Who needs to be <i>consulted</i> for details and additional info on requirements. Typically the person (or team) to be consulted will be the subject matter expert.
Informed	Who needs to be kept <i>informed</i> of major updates. Typically senior leadership.

RACI matrix example

R	Responsible
A	Accountable
C	Consulted
I	Informed

Project Activity / Deliverable	Project Manager	Consultant	Architect	Contractor	Client
Define functional and aesthetic needs	I	I	C	I	R
Assess risk	A	R	I	C	I
Define performance requirements	A	R	I	I	I
Create design	A	C	R	I	C
Execute construction	A	C	C	R	I
Approve construction work	I	I	C	C	R

Parkinson's Law

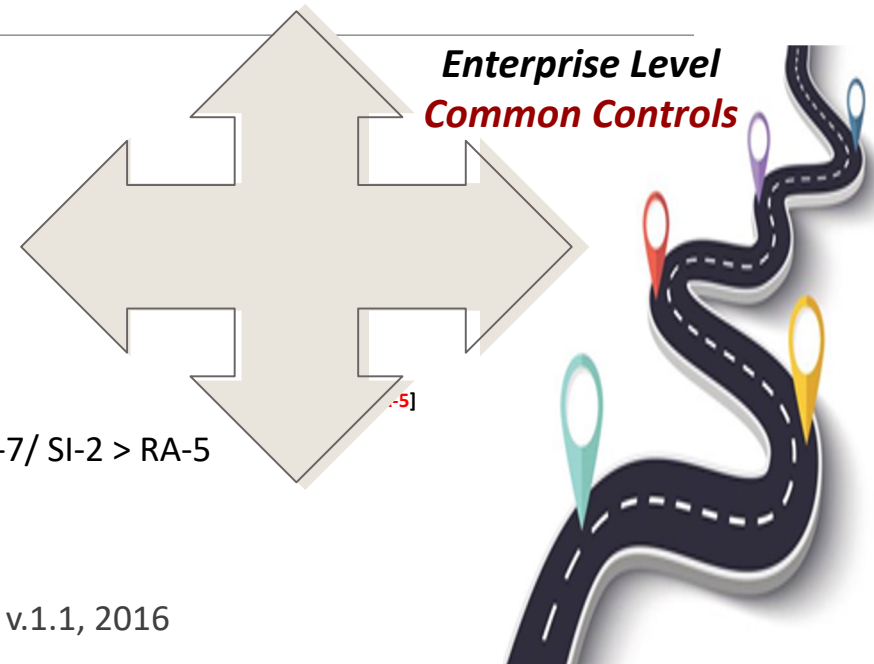




DIS: Risk & Compliance Team Road Map



- **DIS Continuous Monitoring Strategy/ NIST-800-37 + 137A**
- FY-ATO Annual Assessment (SAP) Fixed Schedule/ Project Plans
- SAP & SAR Template vs HHS/ Archer
- ~~IHS Volatile/ Critical Controls – NIST 800-53, Rev 5~~
- Redefine grouped and SCAN based POAMs [PEs, PL-1s, RA-5]
 - **Critical & High risk vulnerabilities** (CVEs with CVSS scores) > NIST = RA-5 > CM-6/CM-7/ SI-2 > RA-5
- Policies & SMEs SOPs that govern day-to-day (D2D) activities
 - **Vulnerability Management**
 - **NIST 800-40** and CRR Supplement Resource Guide, Vol 4, Vulnerability Management, v.1.1, 2016
- Redefined R&C process, alignment and uniformity for ATO assessments per each NIST-800-53 Family Controls and/or enhanced sub controls.
 - GRC Tool – RSA Archer Repository and/or Automation!
 - NIST/RMF Training zoom sessions! (open to all)
- **Future Aspirations... Fast Track ATO!** 😊





IHS Volatile/ Critical/ Core Controls	Annually Assessed (20 controls)
Account Management	AC-2
Wireless Access	AC-18
Content Of Audit Records	AU-3
Audit Review, Analysis, And Reporting	AU-6
Security Impact Analysis	CM-4
Configuration Settings	CM-6
Least Functionality	CM-7
Information System Component Inventory	CM-8
Configuration Management Plan	CM-9
Contingency Plan	CP-2
Contingency Plan Testing	CP-4
Incident Response Plan	IR-8
Security Planning Policy And Procedures	PL-1
System Security Plan	PL-2
Risk Assessment	RA-3
Vulnerability Scanning	RA-5
System Development Life Cycle	SA-3
Security Engineering Principles	SA-8
Flaw Remediation	SI-2
Malicious Code Protection	SI-3



- **DIS-CISO Approved as of 24 May 2023**





SAR Template Progress IHS vs HHS...



Aaa5 Security Assess

Table of Cont

Approval.....

Executive Summary

1. System Overv

1.1 System Id

1.2 System Po

1.3 System Ty

1.4 Operatio

1.5 Minor Ap

1.6 Informati

1.7 Overall Se

2. Assessment A

2.1 Assessme

2.2 Risk Dete

2.3 Security C

3. Risk Assessme

3.1 Assessme

3.1.1 New

3.1.2 Existi

3.2 Accepted

Appendix A. Security

Appendix B. Applica

Appendix C. Acronyms..... 31

nan Services

A) SAR)

System Acronym Security Assessment Plan								Month Year
ID	Control Description	Sensitivity Level for non-CSP and CSP systems						Assess ment Year
		Low	Low - CSP	Mod	Mod - CSP	High	High - CSP	
Contingency Planning (CP)								
CP-1	Contingency Planning Policy & Procedures	CP-1	CP-1	CP-1	CP-1	CP-1	CP-1	3
CP-2	Contingency Plan	CP-2	CP-2 (1) (2) (3)	CP-2 (1) (3) (8)	CP-2 (1) (2) (3) (8)	CP-2 (1) (2) (3) (4) (5) (8)	CP-2 (1) (2) (3) (8)	1, 2, 3
CP-3	Contingency Training	CP-3	CP-3	CP-3	CP-3	CP-3 (1)	CP-3 (1)	2
CP-4	Contingency Plan Testing	CP-4	CP-4	CP-4 (1)	CP-4 (1)	CP-4 (1) (2)	CP-4 (1) (2)	1, 2, 3
CP-6	Alternate	Not	Not in	CP-6	CP-6	CP-6	CP-6	2

5 Security Assessment Report Results 8



SAR Template Progress...



NIST SP 800-53A Rev. 5

ASSESSING SECURITY AND PRIVACY CONTROLS IN INFORMATION SYSTEMS AND ORGANIZATIONS

Figure 8 summarizes the security and privacy control assessment process, including the activities carried out before, during, and after the assessment.

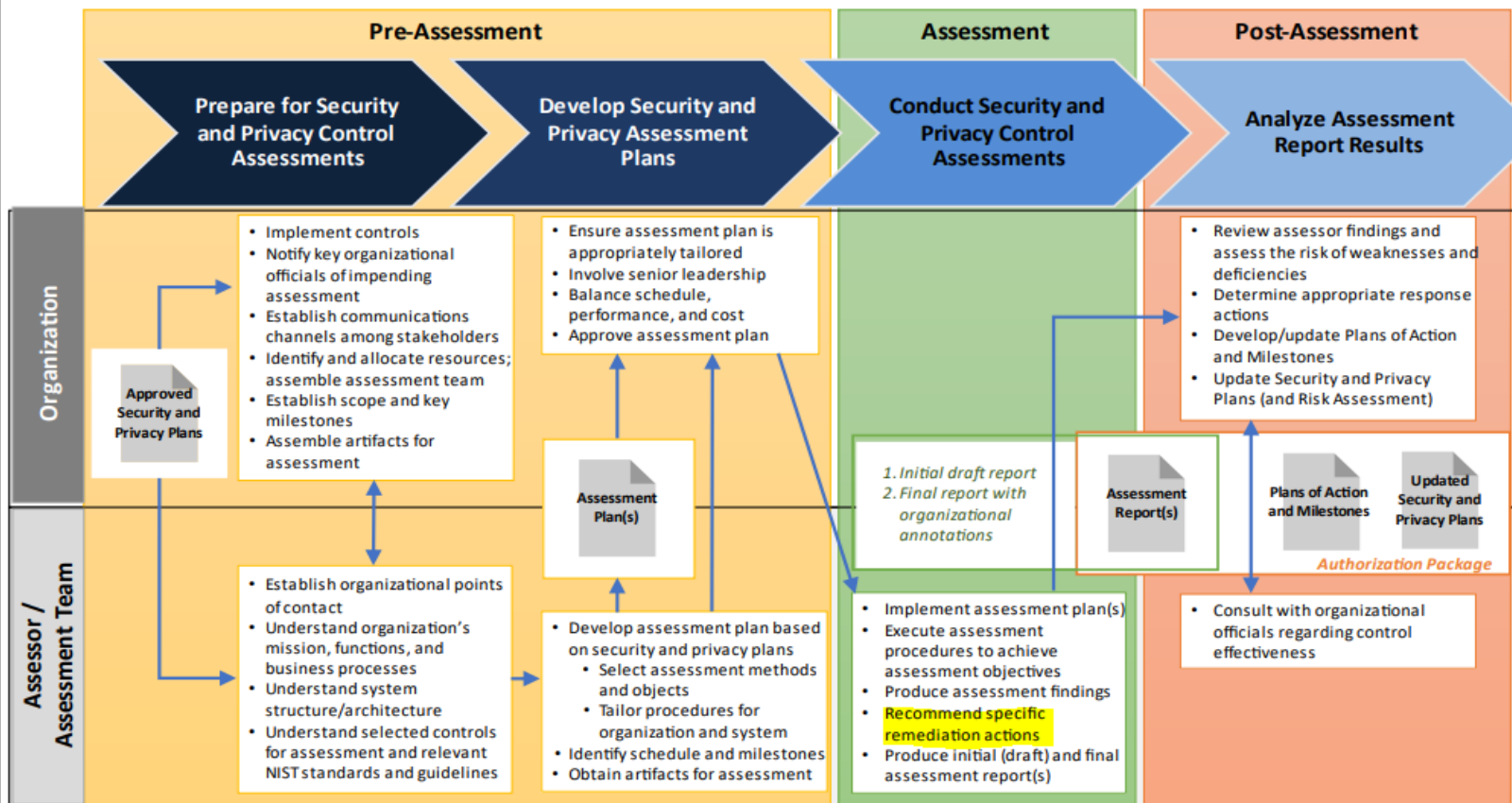


FIGURE 8: SECURITY AND PRIVACY CONTROL ASSESSMENT PROCESS OVERVIEW

Table 23: Identified Vulnerabilities

Weakness Identifier: IHS_HQ_2023_Q1_01a

Weakness Identifier	Affected Control(s)	Likelihood Rating (Low, Medium, High)	Impact Rating (Low, Medium, High)	POA&M Due Date
	SI-2	High	High	5/22/2023

This vulnerability was first identified on 11/5/2020. Findings (APRIL 8, 2023).

In April 2023 {file name = Vuln Scan 04.08.2023.xlsx}, there are "Critical" scan based on findings.

scan findings shown in file Vuln Scan 04.08.2023.xlsx.

To ensure all identified "Critical" vulnerabilities are remediated.

Plans that demonstrate all identified "Critical" vulnerabilities have been remediated.

	Milestone Status	Milestone Due Date
	In Progress	5/9/2023
	Not Started	5/19/2023
Reference to ARC	Not Started	5/22/2023

Small Steps?

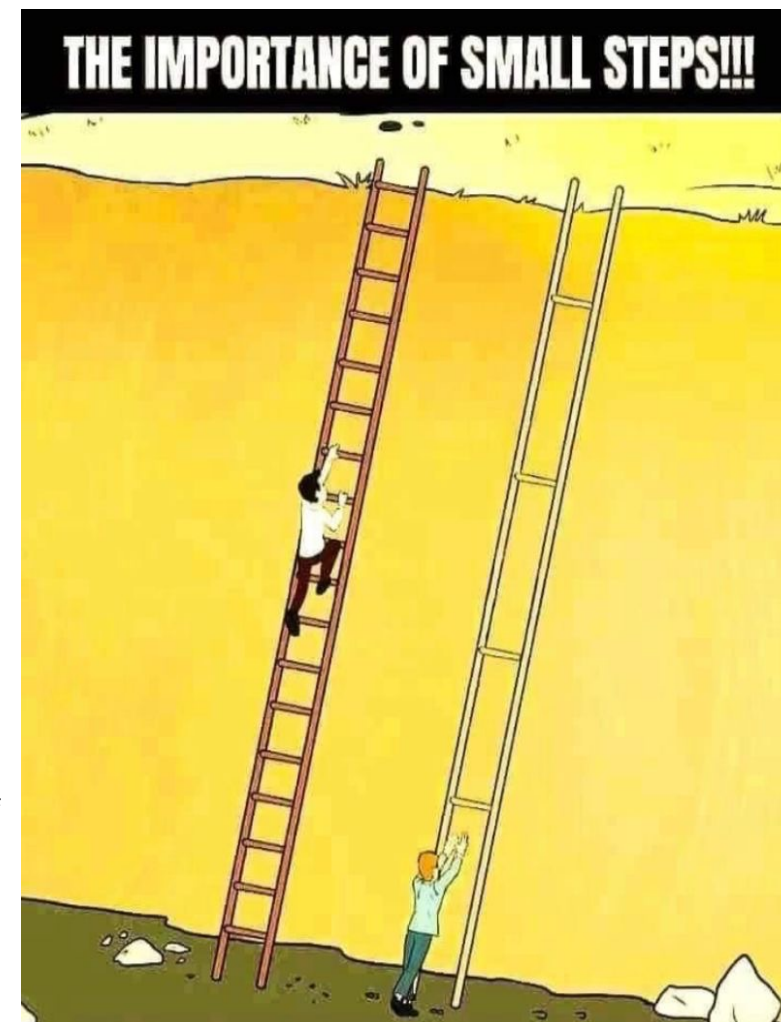
Security is often a combination of multiple small steps and ongoing efforts to protect systems, data, and people.

By breaking down security measures into manageable tasks, we can build a robust security posture and reduce the risk of large-scale breaches or compromises.

Rather than attempting to implement security solutions all at once, it's usually more effective to take small, incremental steps to improve security. This approach allows for careful testing, evaluation, and adjustment along the way, reducing the risk of overlooking critical vulnerabilities or causing significant disruptions.

Here are few examples to illustrate this concept :

- **Regular Updates and Patching:** Keeping software, applications, and systems up to date with the **latest security patches** is crucial. By consistently applying small updates, you can address known vulnerabilities and protect against emerging threats. Neglecting these small steps can expose systems to significant security risks.
- **Employee Training:** Security awareness and **training programs** should focus on small, actionable steps that employees can take to enhance security. This includes practices such as using strong passwords, recognizing phishing attempts, being cautious with email attachments, and reporting suspicious activities. Breaking down security practices into manageable steps increases the likelihood of adoption and compliance.
- **Monitoring and Response:** Effective security often involves constant monitoring and prompt response to security events. By breaking down the detection and response process into smaller steps, security teams can identify and address potential threats in a **timely manner**, preventing or minimizing damage.
- **Network Segmentation:** Dividing a **network into smaller, isolated segments** can enhance security by limiting the impact of a potential breach. If an attacker gains access to one segment, their lateral movement within the network can be restricted, reducing the potential damage they can cause.
- **Secure Development Practices:** In the realm of software development, following secure coding practices and conducting **regular code reviews** can help identify and remedy potential security vulnerabilities early on. By focusing on small, manageable portions of code, developers can identify and fix security issues more effectively.





NIST 800-53, Rev 5 - Control SA-2?

SA-2: Allocation of Resources

Control Family: [System and Services Acquisition](#)

CSF v1.1 References: [ID.GV-4](#)

PF v1.0 References: [GV.PO-P2](#)

Baselines:

Low	SA-2
Moderate	SA-2
High	SA-2
Privacy	SA-2

Previous Version: NIST Special Publication 800-53 Revision 4:
[SA-2: Allocation Of Resources](#)

Control Statement

- Determine the high-level information security and privacy requirements for the system or system service in mission and business process planning;
- Determine, document, and **allocate the resources** required to protect the system or system service as part of the organizational capital planning and investment control process; and
- Establish a discrete line item for information security** and privacy in organizational programming and budgeting documentation.

Supplemental Guidance

Resource allocation for information security and privacy includes funding for system and services acquisition, sustainment, and supply chain-related risks throughout the system development life cycle.

Related Controls

NIST Special Publication 800-53 Revision 5

- [PL-7: Concept of Operations](#)
- [PM-3: Information Security and Privacy Resources](#)
- [PM-11: Mission and Business Process Definition](#)
- [SA-9: External System Services](#)
- [SR-3: Supply Chain Controls and Processes](#)
- [SR-5: Acquisition Strategies, Tools, and Methods](#)

SA-2: Allocation of Resources

Control Statement:

- Determine the high-level information security and privacy requirements for the system or system service in mission and business process **planning**;
- Determine, document, and **allocate the resources required to protect** the system or system service as part of the organizational capital planning and investment control process; and
- Establish a discrete line item** for information security and privacy in organizational programming and **budgeting** documentation.

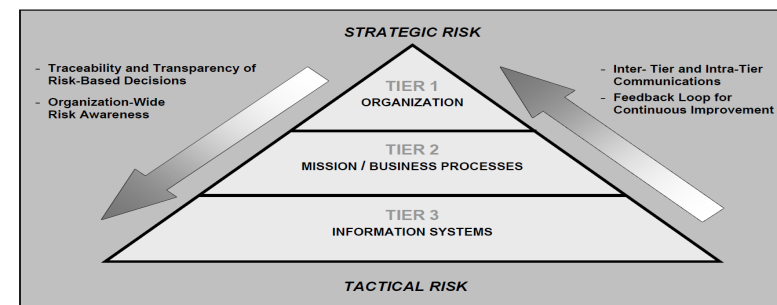
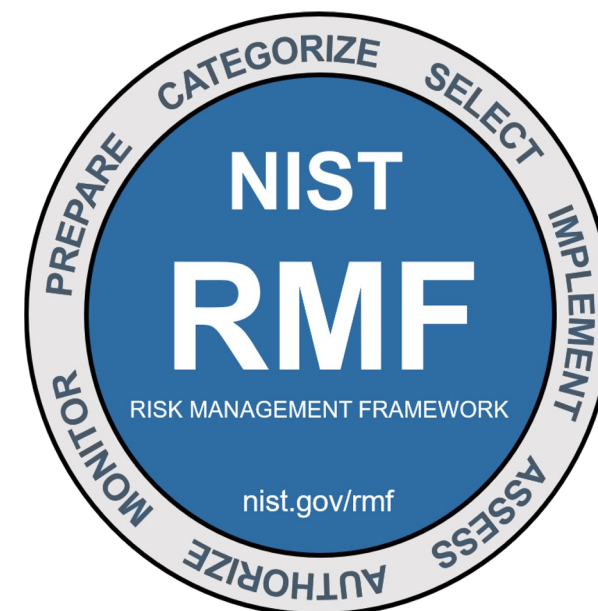
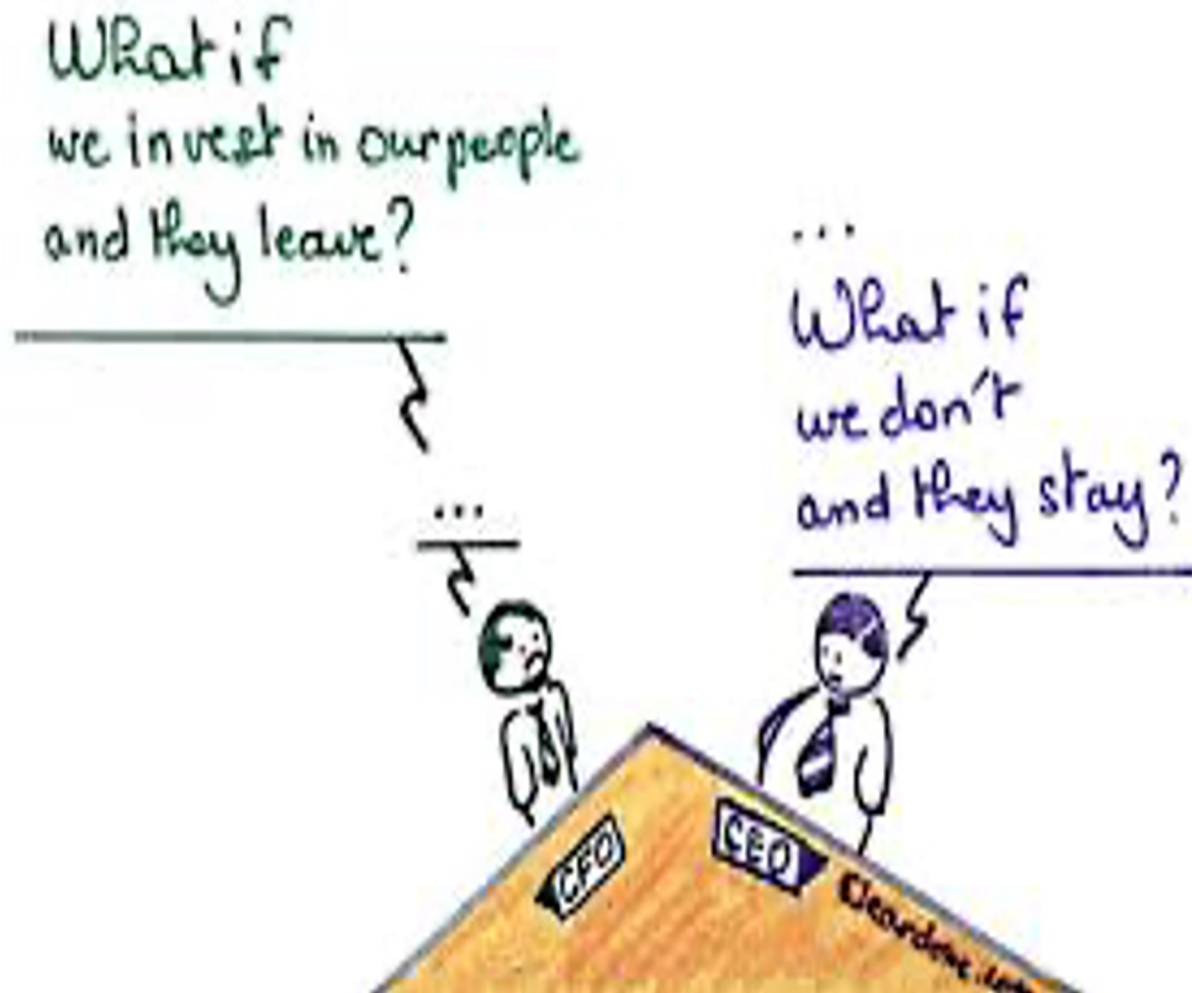


FIGURE 2: MULTITIERED ORGANIZATION-WIDE RISK MANAGEMENT

Training Aids/ NIST Reference(s)





IHS' Mission/ Vision/ Goals!

- **Our Mission:** to raise the physical, mental, social, and spiritual health of American Indians and Alaska Natives to the **highest level**
- **Our Vision:** healthy communities and quality health care **systems** through strong partnerships and culturally responsive practices
- **Strategic goals:**
 - to ensure that comprehensive, culturally appropriate personal and public health **services** are **available** and **accessible** to American Indian and Alaska Native people;
 - to promote excellence and quality through innovation of the Indian health **system** into an **optimally performing** organization; and
 - to strengthen IHS **program management** and **operations**.





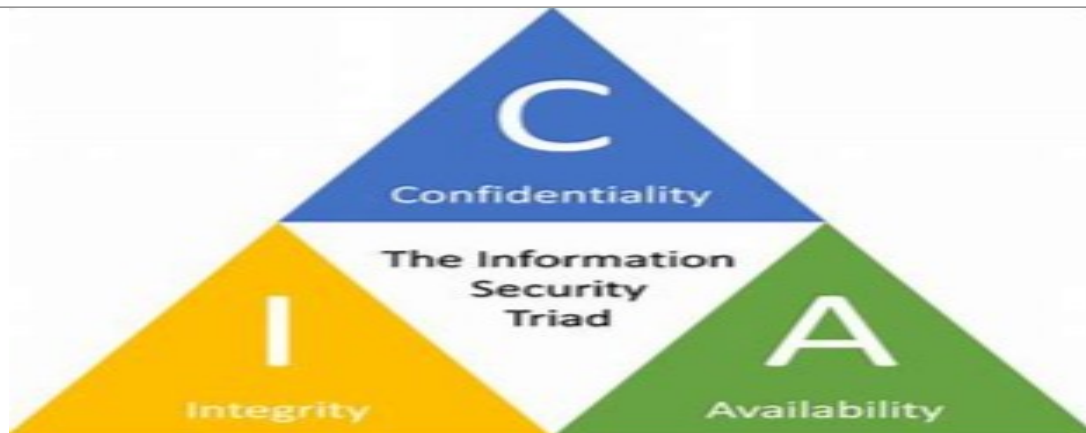
IHS/ NIST Acronyms & Abbreviations

Glossary | <https://csrc.nist.gov/glossary>

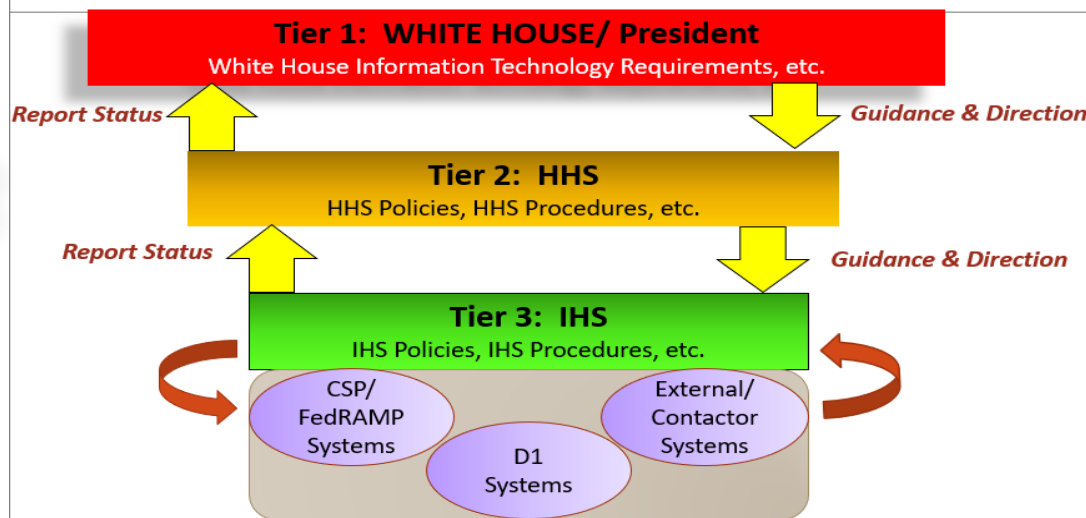


Acronym	Definition
AO	Authorizing Official
ATO	Authorization to Operate
CIA	Confidentiality, Integrity, Availability
CISO	Chief Information Security Officer
CMP	Change Management Plan
CSP	Cloud Service Provider
DRCP	Disaster Recovery and Contingency Planning
FedRAMP	Federal Risk and Authorization Management Program
FIPS	Federal Information Processing Standards
IRP	Incident Response Plan
ISA	Interconnection Security Agreement
ISCP	Information System Contingency Plan
ISSO	Information System Security Officer

Acronym	Definition
NIST	National Institute of Standards and Technology
PIA	Privacy Impact Assessment
POA&M	Plan of Action and Milestones
RMF	Risk Management Framework
SAP	Security Assessment Plan
SAR	Security Assessment Report
SCA	Security Control Assessor
SO	System Owner
SP	Special Publication
SSP	System Security Plan
ST&E	Security Testing and Evaluation



IHS' 3-TIER SYSTEM



The End