Indian Health Service

Audits…Do I have to?

The Importance of Auditing for Compliance and Risk Management

AMALIS HERNANDEZ – AUDIT TEAM LEAD

JASON WELLS – IT AUDIT ANALYST

AUGUST 22, 2023

Discussion

- Who We Are
- Who are Our Partners?
- Why are IT Audits Crucial?
- Audits and Continuous Monitoring
- Risk Management: Plans of Action and Milestones
- Data Calls
- Working Together
- ARC Accomplishments
- Resources

Who We Are

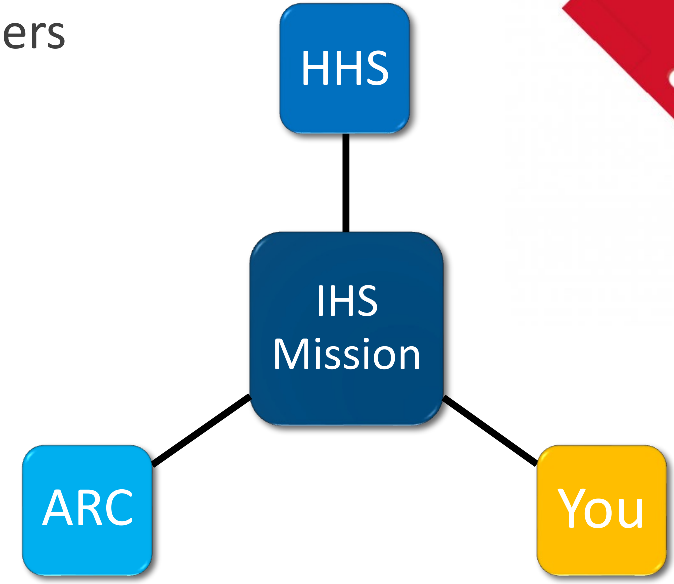
The Audit Response and Coordination (ARC) Team supports IHS' OIT's efforts to remain compliant with cybersecurity mandates and risk management:

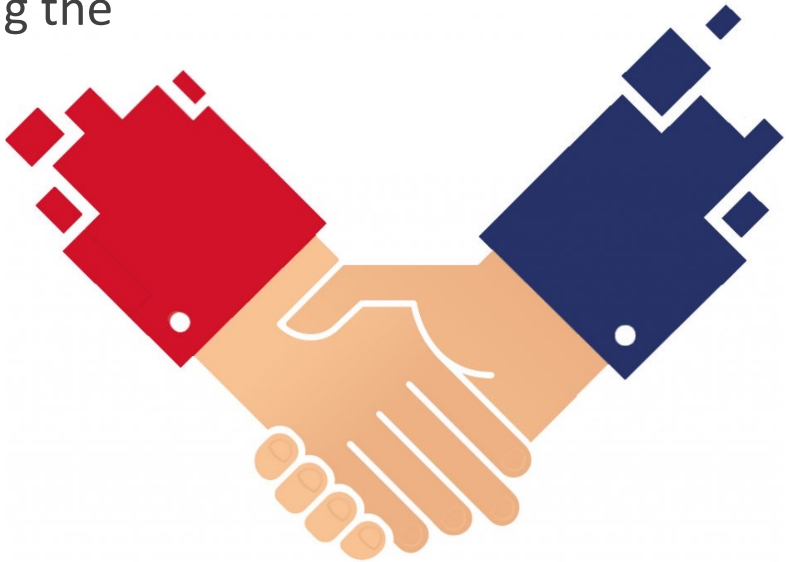
- We serve as a liaison during IT audits.
- We facilitate communication between the auditors and key stakeholders.
- We coordinate data calls and consolidate information received for timely submissions.
- We evaluate responses and supporting documents for accuracy, completeness, and consistency.
- We manage the Plan of Action and Milestones (POA&M) process and compliance reporting.

Who are Our Partners?

ARC partners with all of IHS to accomplish one goal; achieving the IHS mission. Including, but not limited to:

- System Owners
- Information System Security Officers
- System Administrators
- Enterprise Administrators
- Disaster Recovery Teams
- Incident Response Teams





Why are IT Audits Crucial?

- Achieving IHS mission
- To review compliance with laws, regulations and mandates.
- Cyber Resilience
- Cyber Health and Maturity
- Risk Identification, Tracking and Reduction

Why are IT Audits Crucial?

Achieving the IHS 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

Why are IT Audits Crucial?

Cybersecurity Laws, Regulations, and Mandates Compliance

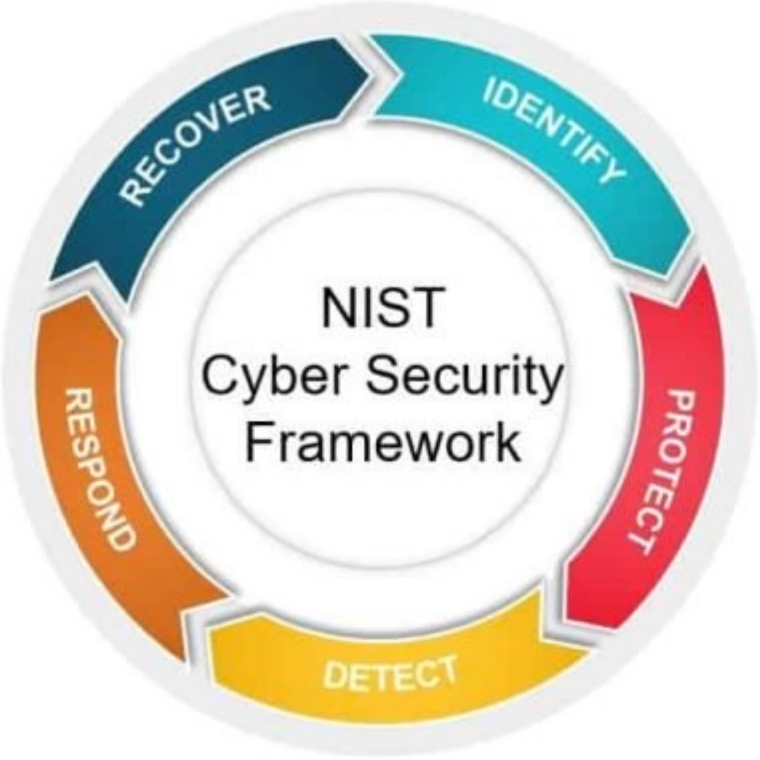
- Executive Order (EO) 14028 - "Improving the Nation's Cybersecurity" (issued May 12, 2021) requires agencies to enhance cybersecurity and software supply chain integrity.
- HIPAA: Health Insurance Portability and Accountability Act 45 CFR Part 160, 45 CFR Part 164 - HIPAA has security, privacy, and breach notification rules. The law applies to health care providers, health plans, health care clearinghouses, and, in some instances, business associates of these businesses called covered entities. HIPAA has particular rules to determine compliance.
- FISMA: United States legislation that defines a framework of guidelines and security standards to protect government information and operations. This risk management framework was signed into law as part of the Electronic Government Act of 2002, and later updated and amended. IT requires federal agencies, and others it applies to, to develop, document and implement agency-wide information security programs.

Why are IT Audits Crucial?

Cyber Resilience

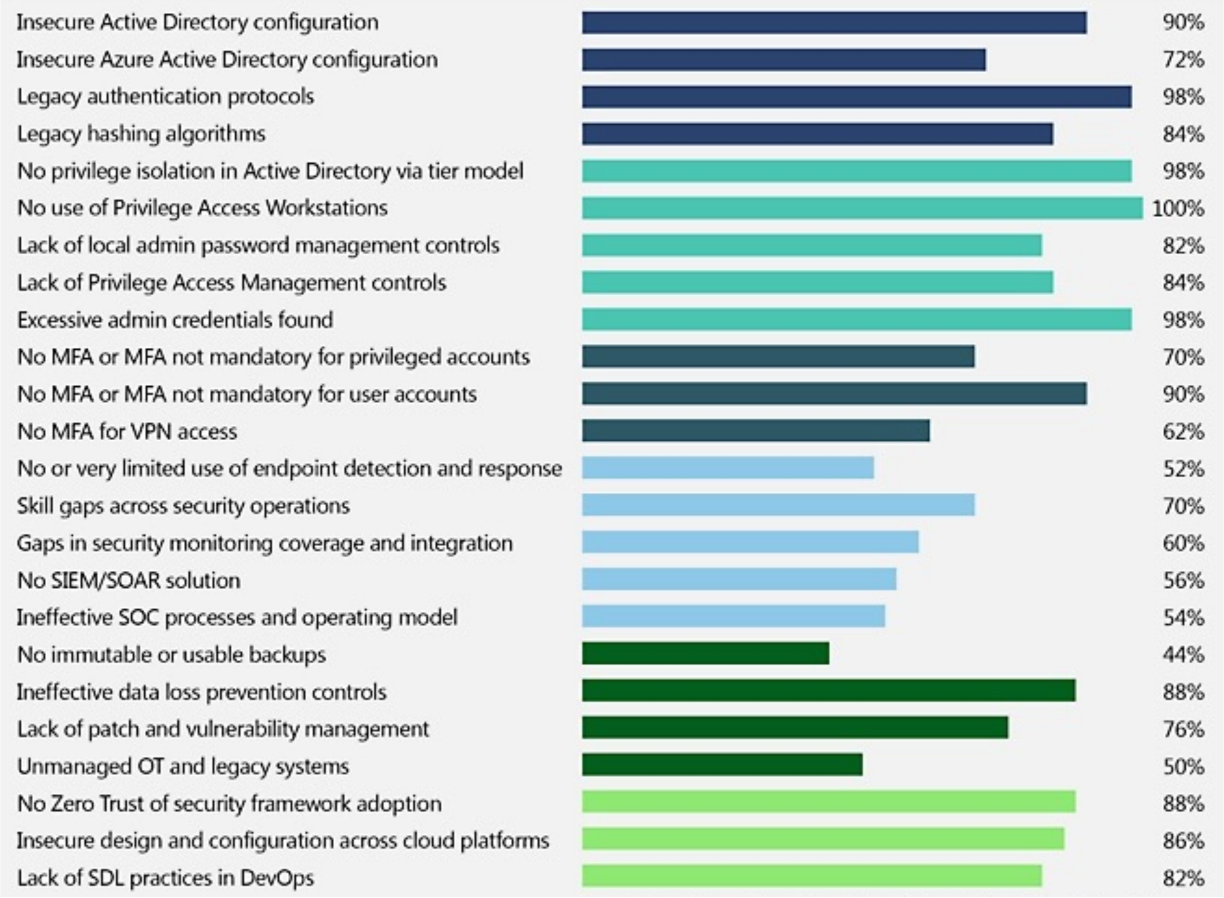
Cyber Resilience

- The ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources.
- Cyber resiliency is intended to enable mission or business objectives that depend on cyber resources to be achieved in a contested cyber environment.
- Sources: NIST SP 800-172, NIST SP 800-160 Vol. 2 Rev. 1



Why are IT Audits Crucial?

Cyber Resilience



Insecure Configuration of Identity Provider

Insufficient Privilege Access and Lateral Movement Controls

No Multifactor Authentication

Low Maturity Security Operations

Lack of Information Protection Control

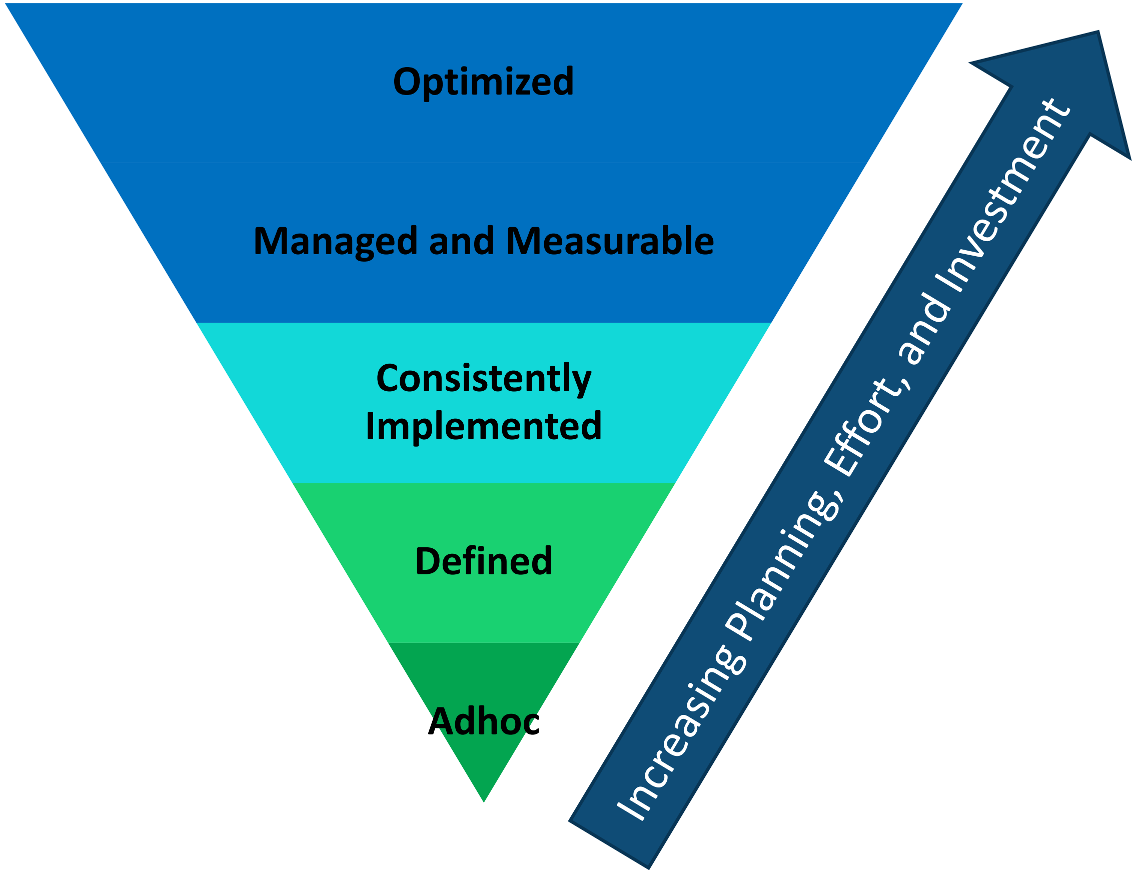
Limited Adoption of Modern Security Frameworks

Source: Microsoft Digital Defense Report 2022

Why are IT Audits Crucial?

Cyber Health and Maturity

- Provides a structure for organizations to baseline current capabilities in cybersecurity workforce planning, establishing a foundation for consistent evaluation
- Management tool for leadership in identifying opportunities for growth and evolution

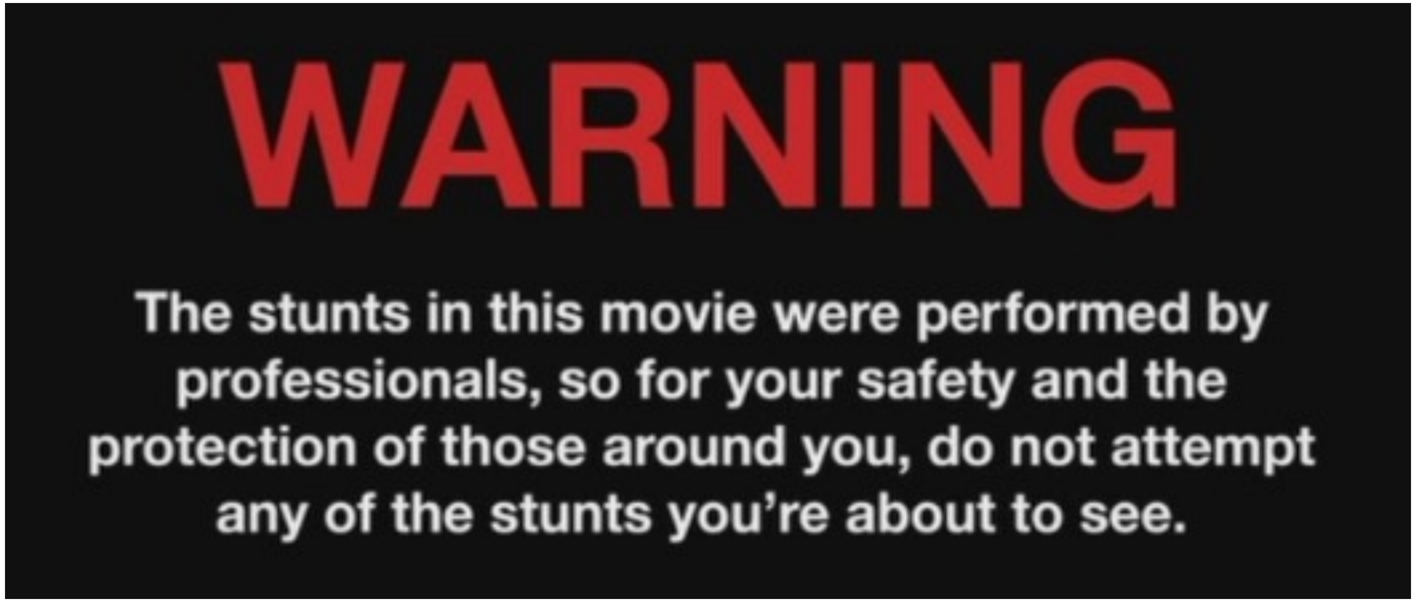


Why are IT Audits Crucial?

Risk Tracking and Reduction

- OMB requires all known weaknesses to be identified and tracked in a POA&M for risk tracking and reduction efforts.
- Guidance directs CIOs and agency program officials to develop, implement, and manage POA&Ms for all programs and systems they operate and control
- OMB Memorandum M-04-25 states that a POA&M is a tool that identifies tasks that need to be accomplished and provides information for the E-Government Scorecard under the President's Management Agenda.

Do I Have To?



WARNING

The stunts in this movie were performed by professionals, so for your safety and the protection of those around you, do not attempt any of the stunts you're about to see.

Please enjoy the video

Do I Have To?

Please enjoy the video

Audits and Continuous Monitoring

- Government Accountability Office (GAO)
- A-123 Assessment
- Office of Inspector General (OIG)
- Federal Information Security Modernization Act (FISMA)
- Binding Operational Directives
- Various HHS Data Calls

Audits and Continuous Monitoring

GAO Audits

- The Government Accountability Office (GAO) aka "congressional watchdog”.
- Independent agency in the legislative branch that helps Congress fulfill its legislative and oversight responsibilities.
- At the request of Congress, or by requirements in legislation, GAO audits federal agencies and programs to assess how well they are working, and their fiscal performance.

Audits and Continuous Monitoring

A-123 Assessments

- The Office of Management and Budget (OMB) Government Circular A-123 defines management's responsibility to implement an Enterprise Risk Management (ERM) framework and internal controls in federal agencies.

- The Federal Managers Financial Integrity Act (FMFIA) of 1982 requires agencies to conduct an annual assessment of IT general controls over financial reporting.

- Agencies are required to submit to the Congress an annual assurance statement.

- Material weaknesses and a summary of corrective actions must be reported to OMB and Congress.

Audits and Continuous Monitoring

OIG Audits

- The Office of Inspector General (OIG) conducts independent audits to examine the performance of the Department of Health & Human Services (HHS) programs to help reduce waste, fraud, abuse, and mismanagement.

- OIG conducts periodic follow-ups of IG recommendations and oversees HHS' annual financial statement and FISMA audits.

- In 2021, IHS experienced a virtual audit to determine if cybersecurity controls have been implemented to protect its telehealth technologies.

Audits and Continuous Monitoring

FISMA Audits

- Federal Information Security Modernization Act (FISMA) is a law amended in 2014 to reduce overall reporting, strengthen the use of continuous monitoring, and increase focus on compliance.
- Increases the security of sensitive information, provides continuous monitoring, and eliminates vulnerabilities in a timely and cost-effective manner.
- Requires Inspectors General to perform an annual independent evaluation of agency's information security programs and practices.
- Failure to comply with FISMA may result in potential penalties.
- Agencies are required to submit quarterly and annual progress updates to fulfill congressional reporting requirements.

Audits and Continuous Monitoring

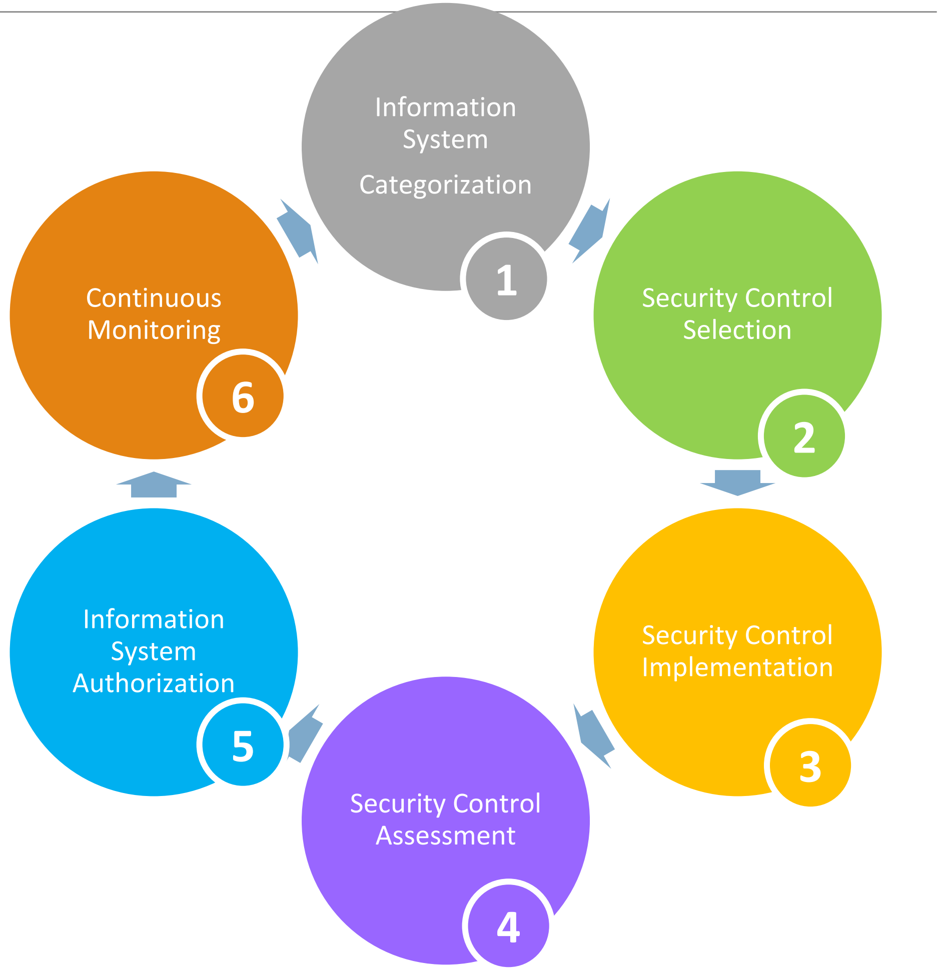
Binding Operational Directives

- A binding operational directive is a compulsory direction to federal, executive branch, departments and agencies for purposes of safeguarding federal information and information systems.
- The Department of Homeland Security (DHS) develops and oversees the implementation of binding operational directives pursuant to the Federal Information Security Modernization Act of 2014.
- Federal agencies are required to comply with DHS-developed directives.

Risk Management

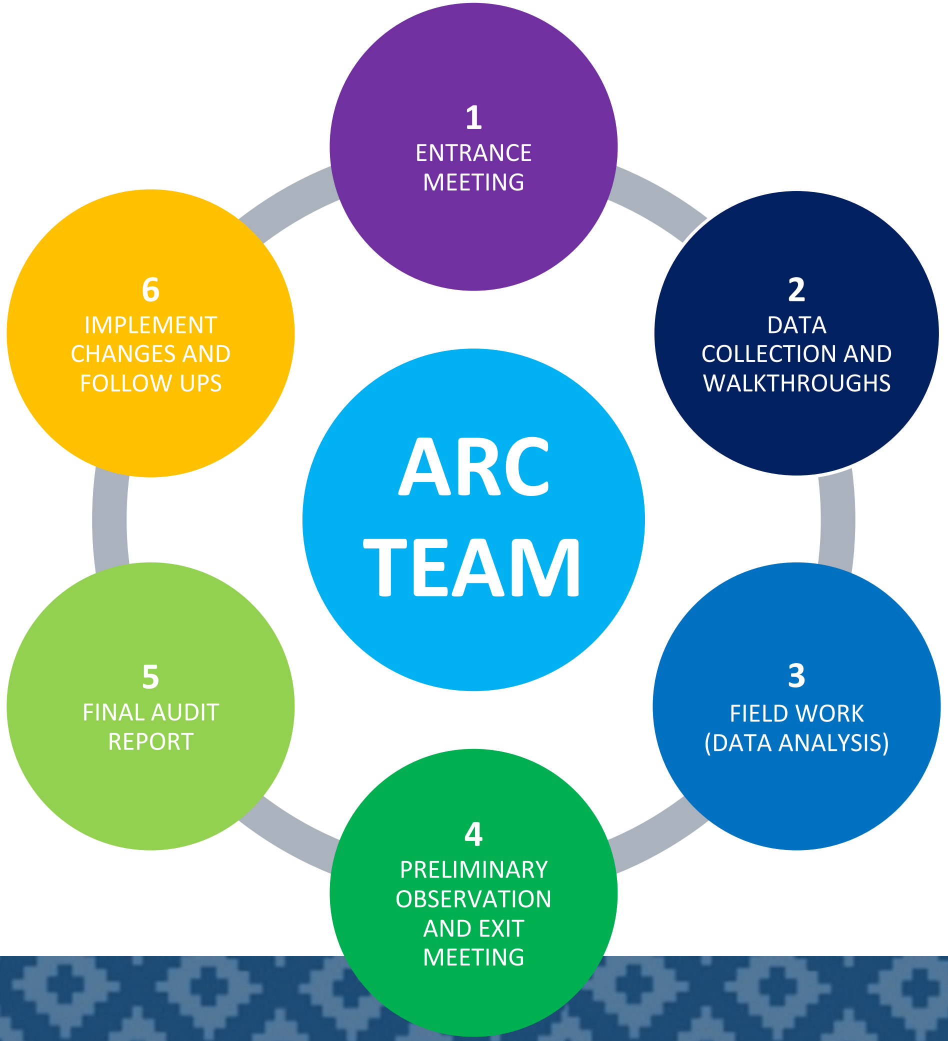
How We Work Together

- Audit Process Lifecycle
- Plan of Action and Milestones
- Binding Operational Directives, Data Calls


Information System Categorization
1
Security Control Selection
2
Security Control Implementation
3
Security Control Assessment
4
Information System Authorization
5
Continuous Monitoring
6

Risk Management

Audit Process Lifecycle


ARC TEAM
1
ENTRANCE MEETING
2
DATA COLLECTION AND WALKTHROUGHS
3
FIELD WORK (DATA ANALYSIS)
4
PRELIMINARY OBSERVATION AND EXIT MEETING
5
FINAL AUDIT REPORT
6
IMPLEMENT CHANGES AND FOLLOW UPS

Risk Management

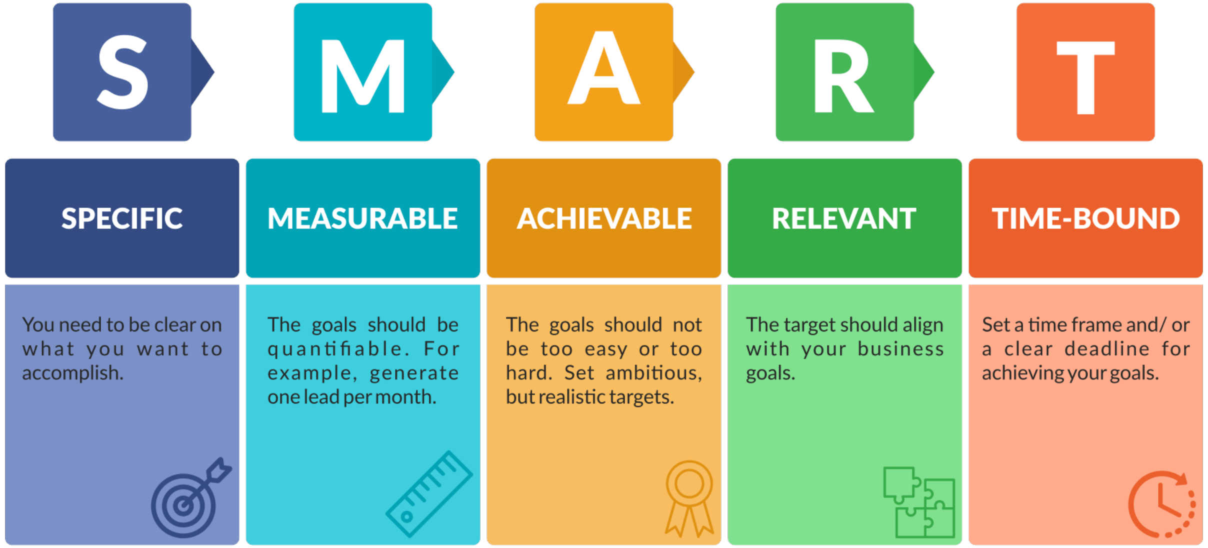
Plan of Action and Milestones

- Plan of Action and Milestones (POA&M) are required by FISMA to effectively manage security risks and mitigate weaknesses.
- There are two types of weaknesses:
  - **Program -** weakness may impact multiple IT systems as a result of a deficiency in an IT program.
  - **System -** weakness is specific to one IT system.
- Every IT system should have a POA&M to identify, manage, and mitigate weaknesses.
- All weaknesses must be recorded and managed in a POA&M. The ARC Team submits a monthly POA&M weakness report to HHS and works with the ISSOs to perform quarterly reviews.

Risk Management

Plan of Action and Milestones Criteria

- Set **SMART** milestones
- Identify necessary resources
- Monitor progress



S
SPECIFIC
You need to be clear on what you want to accomplish.

M
MEASURABLE
The goals should be quantifiable. For example, generate one lead per month.

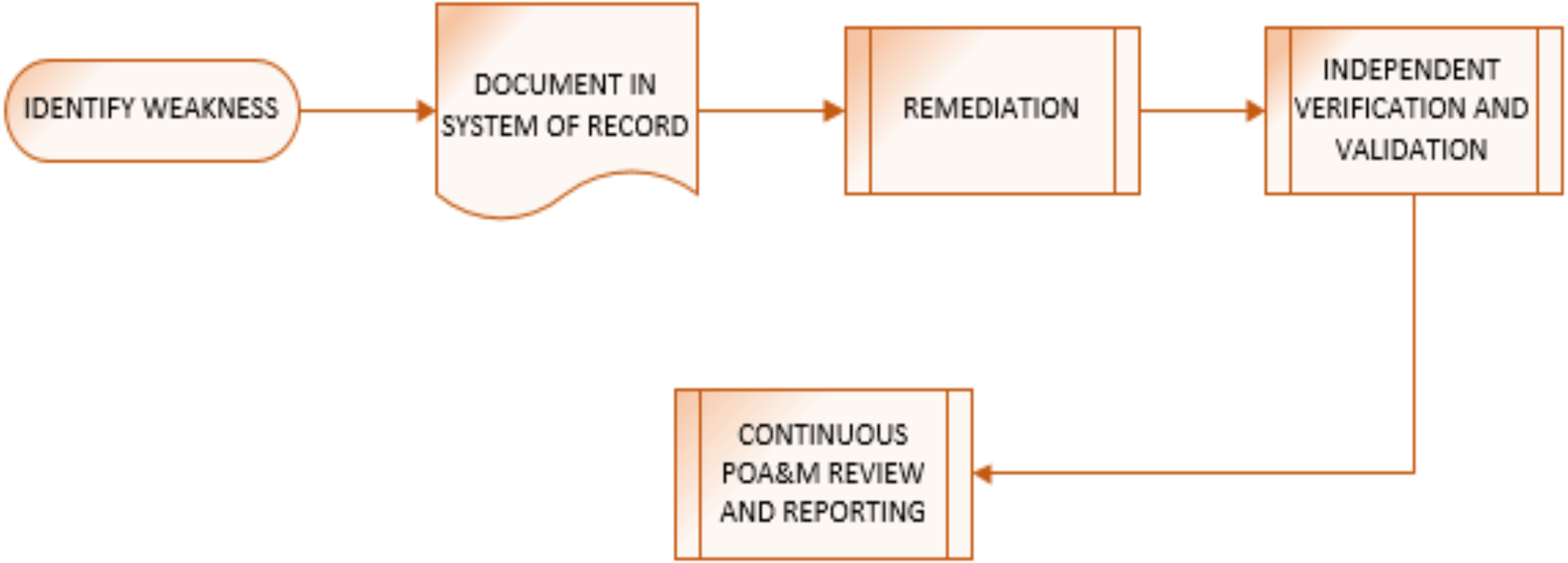
A
ACHIEVABLE
The goals should not be too easy or too hard. Set ambitious, but realistic targets.

R
RELEVANT
The target should align with your business goals.

T
TIME-BOUND
Set a time frame and/ or a clear deadline for achieving your goals.

Risk Management

Plan of Action and Milestones Process


IDENTIFY WEAKNESS
DOCUMENT IN SYSTEM OF RECORD
REMEDIATION
INDEPENDENT VERIFICATION AND VALIDATION
CONTINUOUS POA&M REVIEW AND REPORTING

Risk Management

Plan of Action and Milestones Closure

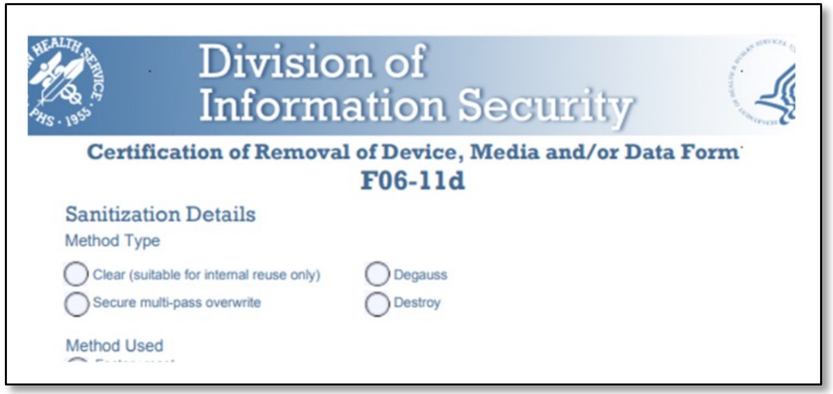
The ARC Team…

- Performs an Independent Verification and Validation (IV&V) of evidence provided.
- Facilitates the closure of the POA&M by the auditor of the requesting agency.

Risk Management

Plan of Action and Milestones Closure

1. Memo
2. Emails
3. Scan results (i.e. vulnerability scans …)
4. Screenshots (date/timestamp)
5. Demo
6. Approved and/or signed Relevant document(s) CMP, ISCP, SSP, Network and Data Flow Diagrams etc.
7. Form F06-11d (Certification of Removal of Device, Media and/or Data Form)



Division of Information Security

Certification of Removal of Device, Media and/or Data Form

F06-11d

Sanitization Details

Method Type

○ Clear (suitable for internal reuse only) ○ Degauss

○ Secure multi-pass overwrite ○ Destroy

Method Used

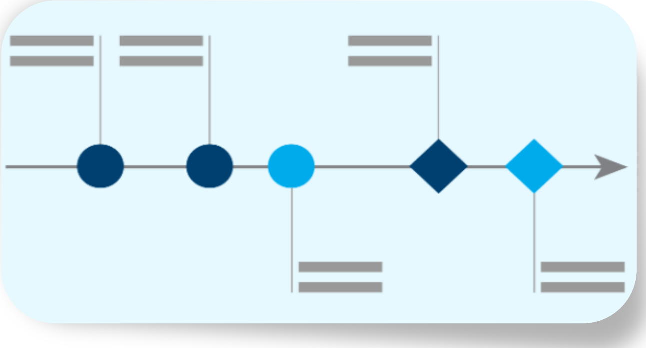
✓Relevant ✓Reliable ✓Sufficient

Risk Management

Plan of Action and Milestones Remediation Timeline

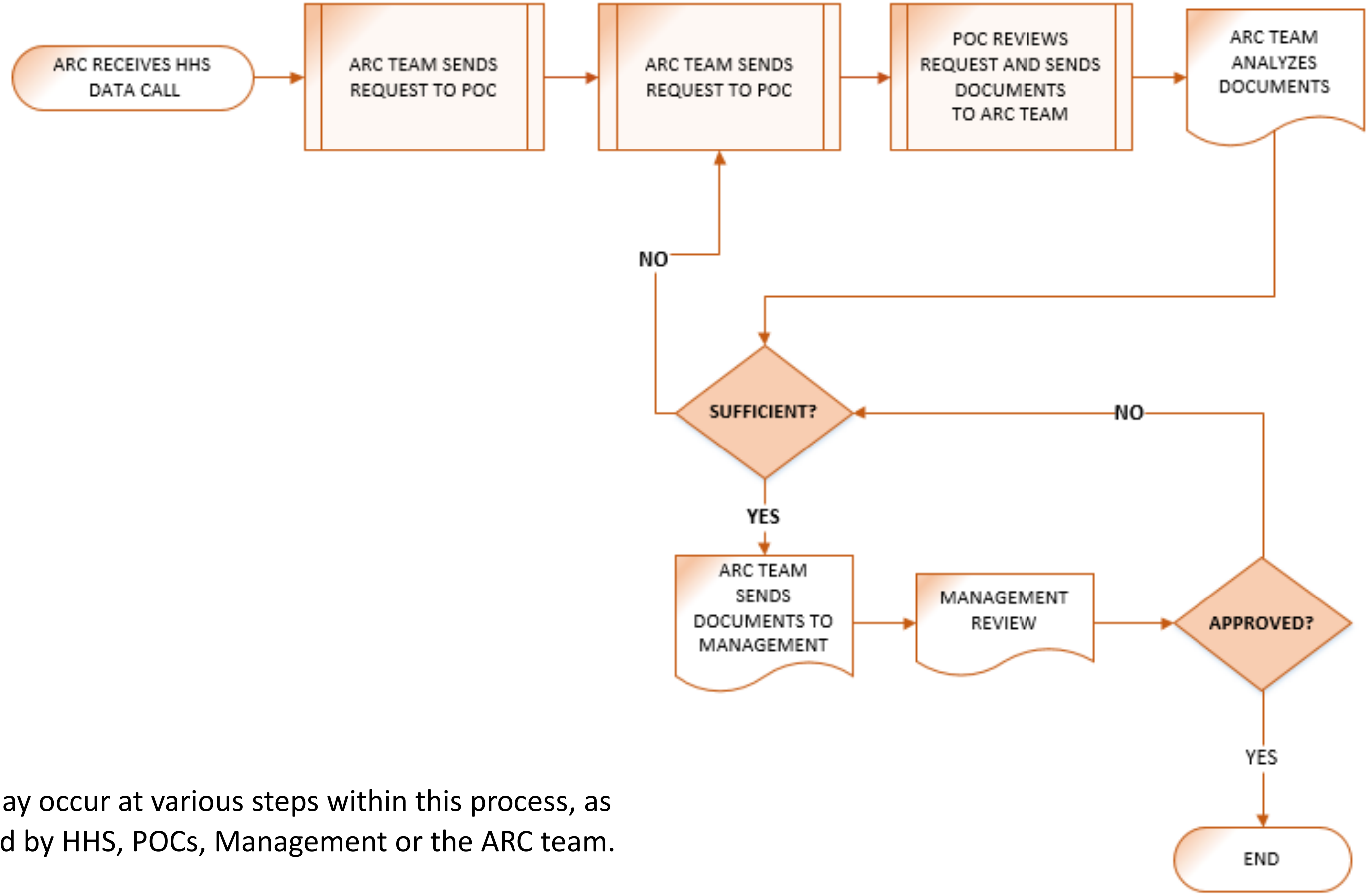
Per HHS’ POA&M Standard, all weaknesses from vulnerability scanning, security assessments and audits must be remediated within the following timelines:

- Critical within 15 days (in accordance with DHS BOD 19-02)
- High within 30 days (in accordance with DHS BOD 19-02)
- Moderate within 90 days (in accordance with FedRAMP Guidance)
- Low within 365 days



Data Calls

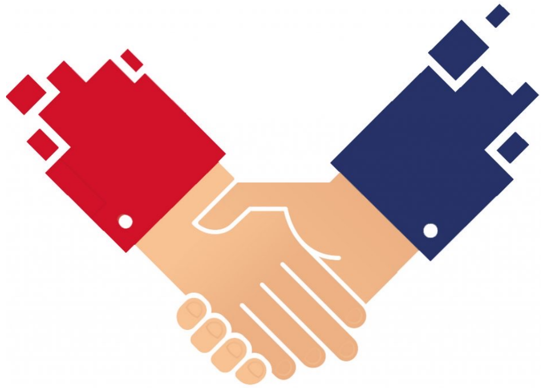
Data Call Process


ARC RECEIVES HHS DATA CALL
ARC TEAM SENDS REQUEST TO POC
ARC TEAM SENDS REQUEST TO POC
POC REVIEWS REQUEST AND SENDS DOCUMENTS TO ARC TEAM
ARC TEAM ANALYZES DOCUMENTS
NO
SUFFICIENT?
NO
YES
ARC TEAM SENDS DOCUMENTS TO MANAGEMENT
MANAGEMENT REVIEW
APPROVED?
YES
END

Note: Follow-up meetings may occur at various steps within this process, as necessary, either precipitated by HHS, POCs, Management or the ARC team.

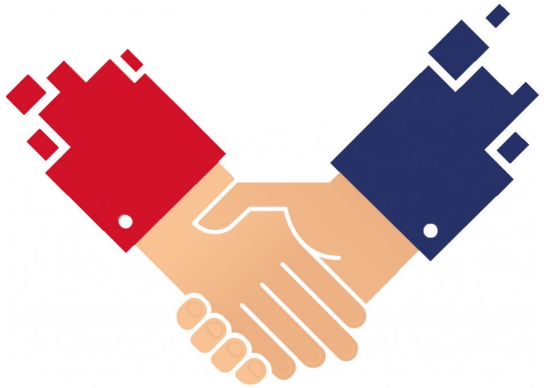
Working Together

- Document your process and keep documents up to date.
- Ask for clarification or defer the request to appropriate personnel to avoid delays.
- Inform the ARC team if additional time is needed to address a request.
- Label documents with the request number or POA&M weakness ID listed in the front of the file name when responding to data calls.



Working Together

- Don’t create documents to satisfy a request.
- Never include sensitive data in emails going outside IHS, such as IP addresses unless required by HHS. When required, provide ARC sensitive information using Secure Data Transfer Service (SDTS).
- Don’t provide any unnecessary and unsolicited information.
- Consistently adhere to defined processes.



ARC Accomplishments

- YTD closed 25% of open POA&Ms this fiscal year. Expected to surpass closure rate from previous years.

- Improved collaboration across IHS for building a well-rounded Risk Management program.

- Reduced the SME level of effort (time and resources) required to respond to Weakness/POAs&M data calls.

- Eliminated duplicate requests which resulted in fewer data calls being sent to SMEs.

Resources

- **HHS POA&M SOP:** Standards for Plans of Action and Milestones (POA&M) Management and Reporting: https://intranet.hhs.gov/document/standard-plans-action-and-milestones-poam-management-and-reporting

- **IHS POA&M SOP:** https://home.ihs.gov/sites/oittfs/themes/ihs-intranet-theme/display_objects/documents/sops/DIS_06-07_POAM_SOP_082017.pdf

- **POA&M Templates:** https://home.ihs.gov/oittfs/templates/

- **Binding Operational Directive 19-02:** https://cyber.dhs.gov/bod/19-02/

- **FedRAMP POA&M Template Completion Guide:** https://www.fedramp.gov/assets/resources/documents/CSP_POAM_Template_Completion_Guide.pdf

Resources

- **NIST Cybersecurity Framework and NIST 800-53 Rev. 5 Controls:**
  - Framework: https://www.nist.gov/cyberframework
  - Controls: https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/SP_800_53_5_1_0/home
- **GAO:** https://www.gao.gov
- **OIG:** https://oig.hhs.gov
- **HHS Information Systems Security and Privacy Policy (ISP2):** Available Upon Request
- **FISMA:** https://www.cisa.gov/federal-information-security-modernization-act
- **A-123 Federal Information System Controls Audit Manual (FISCAM):**
  - https://www.gao.gov/fiscam
  - https://www.congress.gov/113/plaws/publ283/PLAW-113publ283.pdf

Contact Us

IT Audit Team Lead

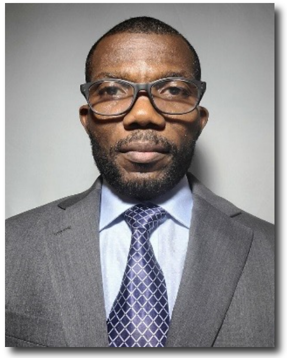
Amalis Hernandez

Amalis.Hernandez@ihs.gov

IT Audit Analyst

Stacie Henderson

Stacie.Henderson@ihs.gov



IT Audit Analyst

Godfred Kwao

Godfred.Kwao@ihs.gov

IT Audit Analyst

Dolly Aguilar

Dolly.Aguilar@ihs.gov

IT Audit Analyst

Jason Wells

Jason.Wells@ihs.gov

IT Audit Analyst

Amaryliss Bivins

Amaryliss.Bivins@ihs.gov

ARC Mailbox: IHSSecurityAudit@ihs.gov

INDIAN HEALTH SERVICE · PHS · 1955

CEU Information

- CEU Code: 85854JYA
- CEUs: 1.50
- Specialty: Core A