Indian Health Service

Governance, Risk, and Compliance (GRC)
Navigating the IT Governance Landscape

JASON WELLS AND GODFRED KWAO

IT AUDIT ANALYSTS

AUGUST 2024

Discussion

- Who We Are
- Who are Our Partners?
- Working Together
- What is Meant by IT Governance?
- GRC Framework (Governance, Risk Management, and Compliance Processes)
- Resources

Who We Are

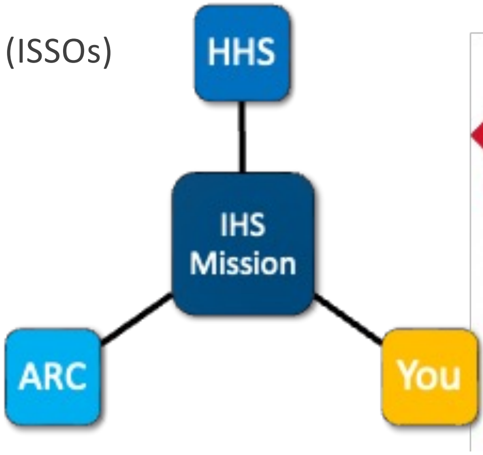
The Audit Response and Coordination (ARC) Team supports IHS OIT’s efforts to remain compliant with cybersecurity mandates and risk management:

- 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 the entire IHS and aims to accomplish one goal: Achieving the IHS mission. This includes:

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



HHS

IHS Mission

ARC

You

IT Governance and Achieving the IHS Mission

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 healthcare systems through strong partnerships and culturally responsive practices.

Our Strategic Goals are:

- 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.

Understanding the Essence of IT Governance

IT governance represents the framework and processes by which organizations ensure that their IT endeavors align with business objectives, mitigate risks, and comply with regulatory requirements.

It is a strategic approach that governs IT investments, operations, and decision-making, thereby ensuring the effective utilization of technology to achieve business goals.

Types of IT Governance

Structural Governance

- Focuses on the organizational structure, delineation of roles, and responsibilities concerning IT decision-making and oversight
- Ensures clarity in authority, accountability, and reporting structures related to IT functions

Process Governance

- Emphasizes the establishment, monitoring, and optimization of IT-related processes
- Includes project management, service delivery, change management, and quality assurance frameworks.

Types of IT Governance

Strategic Governance

- Aligns IT initiatives with the overarching business strategy
- Involves creating IT strategies, defining objectives, and ensuring that IT investments contribute to the organization's long-term goals

Resource Governance

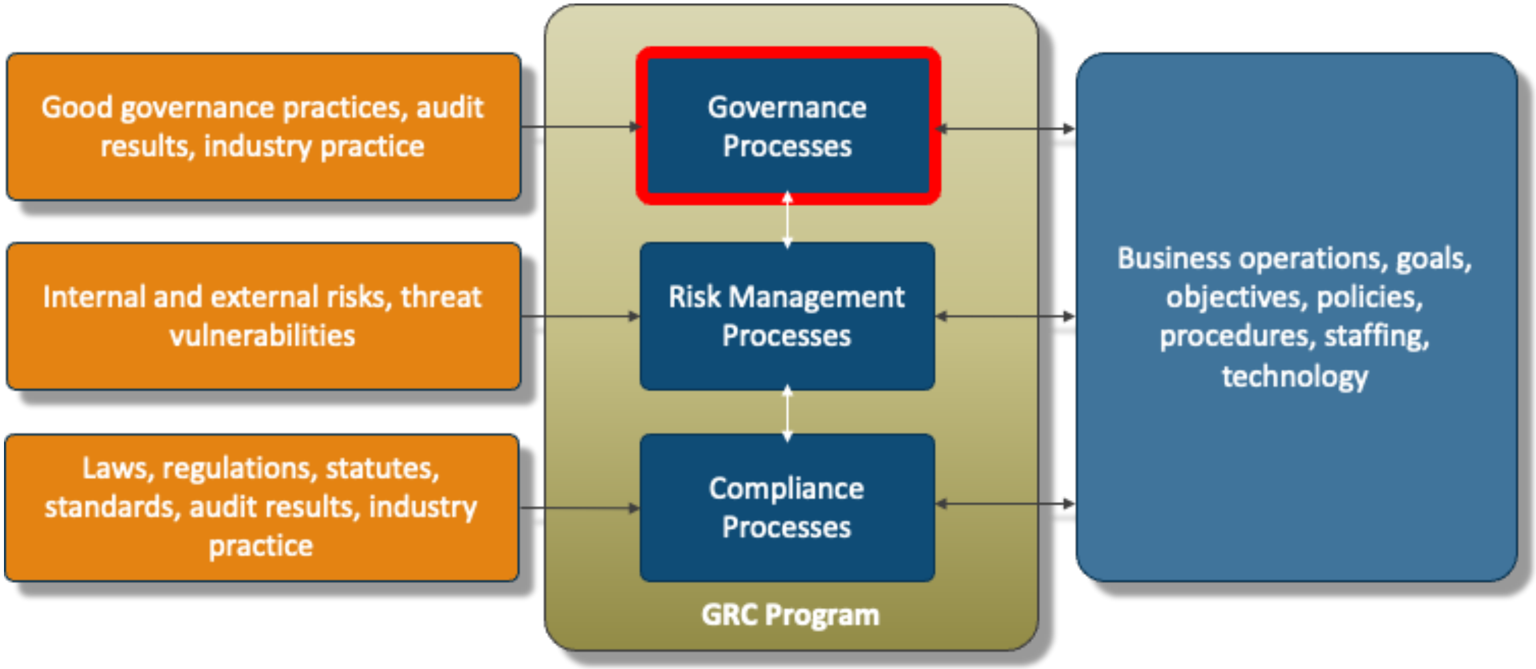
- Involves managing IT resources effectively
- Covers aspects such as budget allocation, resource allocation, and optimization of technological assets to maximize their value

IT Governance Frameworks

NIST Cybersecurity Framework: Developed by the National Institute of Standards and Technology (NIST), this framework offers guidelines for improving cybersecurity posture. It assists organizations in managing and reducing cybersecurity risks.

ITIL (Information Technology Infrastructure Library): ITIL is a set of practices that focuses on IT service management (ITSM). It offers a framework for delivering IT services efficiently and aligning them with business needs, emphasizing continual improvement.

GRC Framework: GRC Program Basics



Good governance practices, audit results, industry practice

Internal and external risks, threat vulnerabilities

Laws, regulations, statutes, standards, audit results, industry practice

Governance Processes

Risk Management Processes

Compliance Processes

GRC Program

Business operations, goals, objectives, policies, procedures, staffing, technology

Implementing Effective IT Governance

Implementing robust IT governance involves several key steps:

- **Assessment**: Conducting an assessment of current IT practices, risks, and governance structures
- **Strategy Alignment**: Aligning IT strategies with business objectives to ensure congruence
- **Framework Adoption**: Selecting and implementing an appropriate governance framework tailored to the organization's needs
- **Clear Roles and Responsibilities**: Defining clear roles, responsibilities, and reporting lines for IT governance
- **Continuous Improvement**: Establishing mechanisms for continual evaluation, learning, and adaptation to evolving needs and technologies

Key Roles in IT Governance

Key participants involved in the IHS risk management and governance process include:

- **Mitch Thornburgh** is the Chief Information Officer (CIO) and Authorizing Official (AO) with the authority to formally assume responsibility and accountability for operating a system; providing common controls inherited by organizational systems; or using a system, service, or application from an external provider

- **Andrea Scott** is the Deputy CIO responsible for developing and maintaining security policies, procedures, and control techniques to address security requirements; overseeing personnel with significant responsibilities for security and ensuring that the personnel is adequately trained; assisting senior organizational officials concerning their security responsibilities; and reporting to the head of the agency on the effectiveness of the organization's security program, including the progress of remedial actions.

Key Roles in IT Governance

Key participants involved in the IHS risk management and governance process include:

- **Benjamin Koshy** is the Chief Information Security Officer (CISO) responsible for carrying out the CIO security responsibilities under the Federal Information Security Modernization Act (FISMA) and serving as the primary liaison for the chief information officer to the system owners, common control providers, and system security officers. Is empowered to coordinate and conduct the day-to-day activities associated with managing risk to information systems and organizations.
- **Carl Mitchell** is the Senior Agency Official for Privacy with agency-wide responsibility and accountability for ensuring compliance with applicable privacy requirements and managing privacy risk.

Challenges in IT Governance

Organizations encounter various challenges in establishing and maintaining effective IT governance:

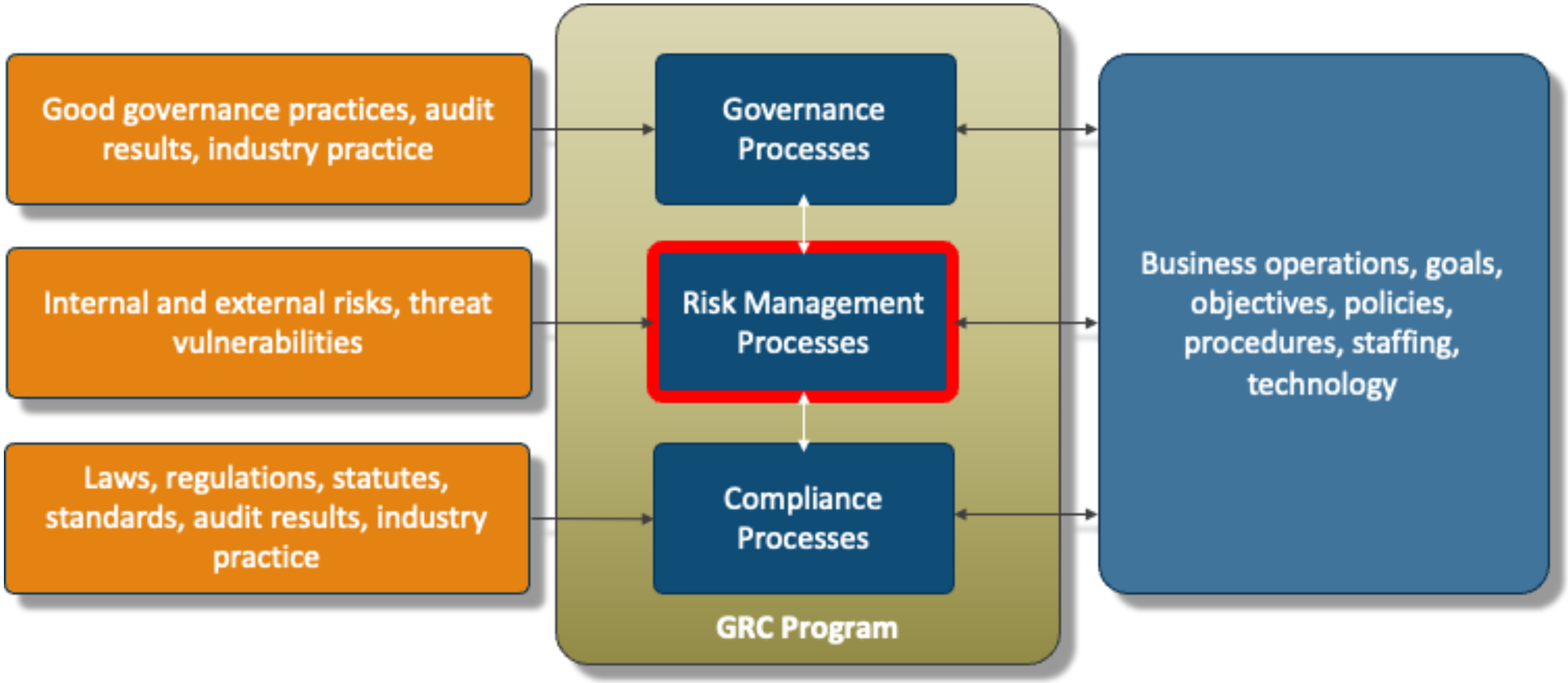
- **Complexity:** Managing diverse IT landscapes, technologies, and stakeholders can be complex and challenging
- **Resistance to Change:** Encountering resistance when implementing new governance structures or processes across the organization
- **Resource Constraints:** Allocating adequate resources for technology, expertise, and time for governance initiatives
- **Dynamic Technology Landscape:** Keeping pace with rapid technological advancements and adapting governance frameworks accordingly
- **Cybersecurity Concerns:** Addressing cybersecurity threats and ensuring robust measures for data protection

Future Trends in IT Governance

The future of IT governance is evolving with emerging trends:

- **AI and Automation Integration:** Utilization of AI and automation for enhancing governance processes and decision-making
- **Data-Centric Governance:** Shifting focus towards data governance, given the increasing volume and importance of data assets
- **Cloud-Centric Governance:** Adapting governance frameworks for cloud-based environments to ensure security and compliance
- **Privacy-Centric Approaches:** Strengthening governance practices to align with evolving privacy regulations and ethical considerations

GRC Framework: GRC Program Basics



Good governance practices, audit results, industry practice

Internal and external risks, threat vulnerabilities

Laws, regulations, statutes, standards, audit results, industry practice

Governance Processes

Risk Management Processes

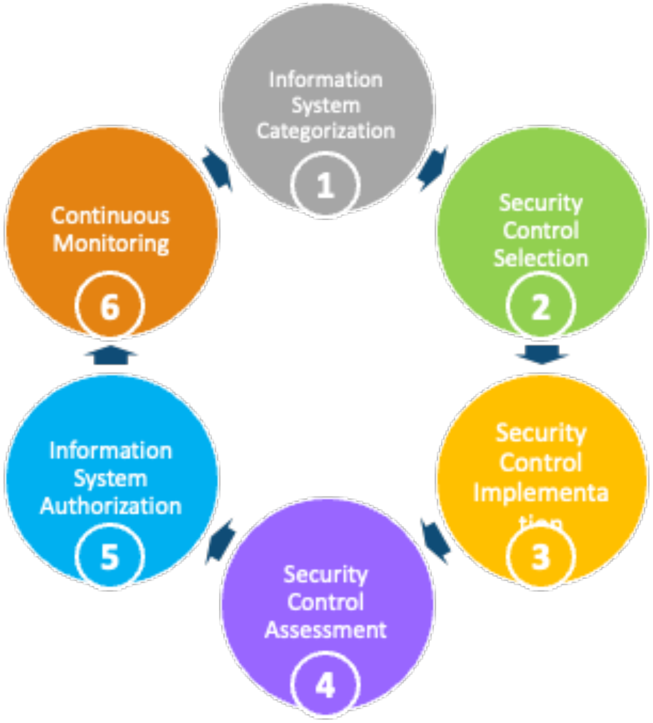
Compliance Processes

GRC Program

Business operations, goals, objectives, policies, procedures, staffing, technology

Risk Management

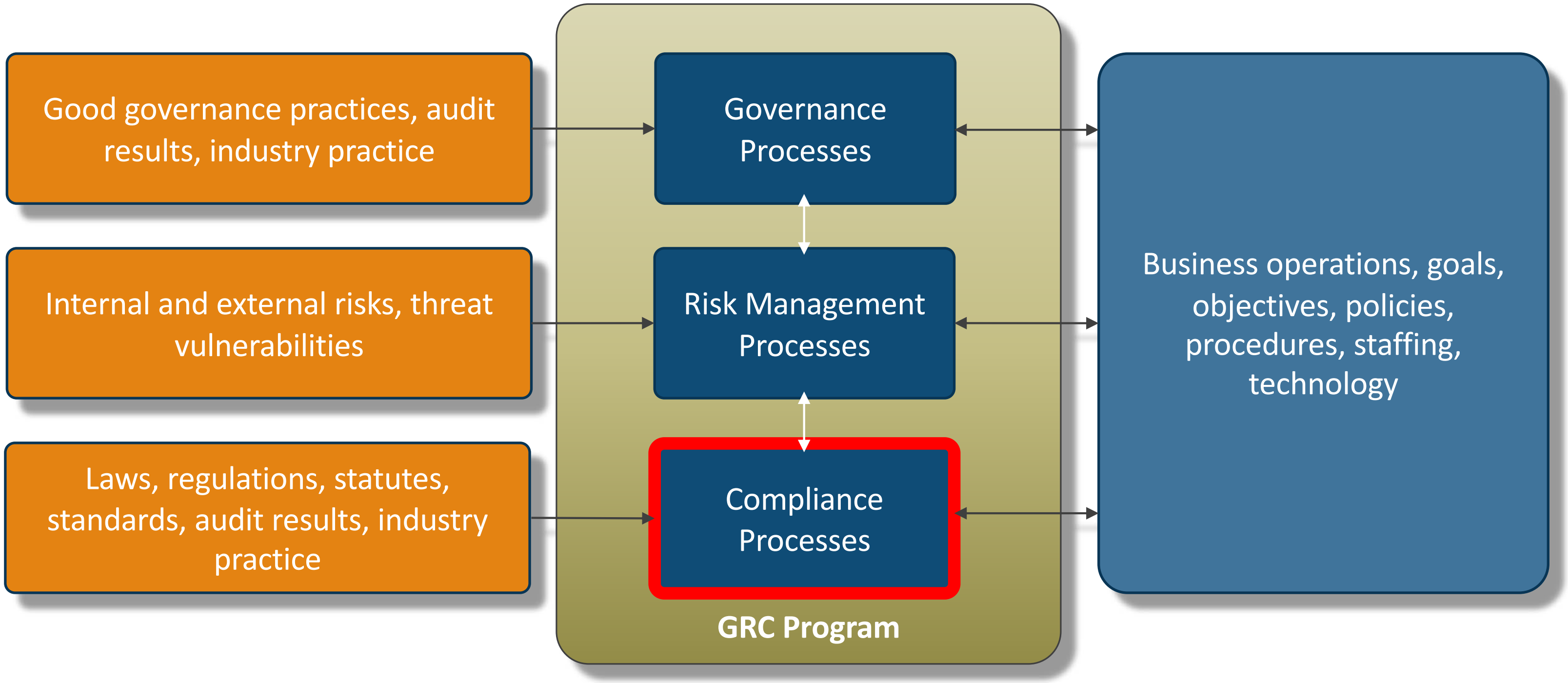
- Audit Process Lifecycle
- Plan of Action and Milestones (POA&M) Development
- Binding Operational Directives
- Data Calls
- POA&M Management
- Vulnerability Scanning


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

Risk Management: Plan of Action and Milestones

- POA&Ms 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.

GRC Framework: GRC Program Basics



Good governance practices, audit results, industry practice

Internal and external risks, threat vulnerabilities

Laws, regulations, statutes, standards, audit results, industry practice

Governance Processes

Risk Management Processes

Compliance Processes

GRC Program

Business operations, goals, objectives, policies, procedures, staffing, technology

Compliance

Definition: Adhering to standards and regulatory requirements set forth by agency, law, or authority group.

Organizations must achieve compliance by establishing risk-based controls that protect the confidentiality, integrity, and availability (CIA) of information.

- 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

Types of Data Subject to Cybersecurity Compliance

Personally Identifiable Information

- Date of birth
- First/last names
- Address
- Social Security number
- Mother's maiden name

Protected Health Information

- Medical history
- Insurance records
- Appointment history
- Prescription records
- Hospital admission records

Types of Data Subject to Cybersecurity Compliance

Financial Information

- Credit card numbers, expiration dates, and CVV values
- Bank account information
- Debit or credit card personal identification numbers
- Credit history or credit ratings

Other

- Race
- Religion
- Marital status
- IP addresses
- Email addresses, usernames, and passwords
- Biometric data (fingerprints, facial recognition, and voice prints)

The Benefits of a Sound IT GRC Program

Effective IT governance yields numerous benefits:

- **Aligned IT Investments:** Ensure that IT investments and initiatives are in sync with business objectives, maximizing their value
- **Risk Mitigation:** Identifies and mitigates IT-related risks, safeguarding the organization against potential threats
- **Operational Efficiency:** Streamlines IT processes, enhances productivity, and reduces redundancies and wastage
- **Compliance Adherence:** Ensures adherence to regulatory requirements and industry standards, avoiding legal and financial implications
- **Strategic Alignment:** Aligns IT strategies with business goals, fostering innovation and competitiveness

Conclusion

Navigating the IT governance landscape is a pivotal endeavor for any organization. Through the adoption of suitable governance types, frameworks, and best practices, organizations can harness the full potential of their technological resources. By continually evolving to meet emerging challenges and embracing future trends, good IT governance becomes indispensable for driving innovation and mitigating risks to our systems.

This helps ensure our ability to succeed in our vision of promoting healthy communities and quality healthcare systems through strong partnerships and culturally responsive practices while maintaining our strategic goals.

Resources

- **NIST Cybersecurity Framework:** https://www.nist.gov/cyberframework

- **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

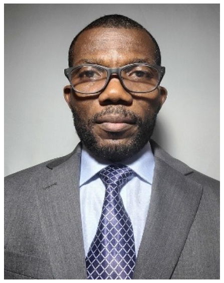
Amalis Hernandez

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.Bivin
@ihs.gov

ARC Mailbox: IHSSecurityAudit@ihs.gov

INDIAN HEALTH SERVICE · PHS · 1955