

CIS Controls: Practical Application, Compliance and Maturity Models Comparison CMMI/NIST CSF



Milton Kabia
ISSO/IT Security Director ANTHC
mkabia@anthc.org

Common Cybersecurity Model and Frameworks

**CMMI = Capability
Management Model
Integration**

**NIST CSF = NIST
Cybersecurity Framework**

**COBIT5 = Control
Objectives for
Information Technology**

**CMMC = Cybersecurity
Maturity Model**



CIS Security Controls to Mitigate Cyberattacks Risk

By Implementing these security controls, an organization can mitigate the risk of cyberattacks by over 80%

- › **01: Inventory and Control of Enterprise Assets:** enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/Internet of Things (IoT) devices; and servers) connected to the infrastructure physically, virtually, remotely, and those within cloud environments.
- › **02: Inventory and Control of Software Assets:** Actively manage (inventory, track, and correct) all software (operating systems and applications) on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution
- › **03: Data Protection:** Develop processes and technical controls to identify, classify, securely handle, retain, and dispose of data.



CIS Security Controls to Mitigate Cyberattacks Risk

By Implementing these security controls, an organization can mitigate the risk of cyberattacks by over 80%

- › **04: Secure Configuration of Enterprise Assets and Software:** Establish and maintain the secure configuration of enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/IoT devices; and servers) and software (operating systems and applications).
- › **05: Account Management:** Use processes and tools to assign and manage authorization to credentials for user accounts, including administrator accounts, as well as service accounts, to enterprise assets and software.
- › **06: Access Control Management:** Use processes and tools to create, assign, manage, and revoke access credentials and privileges for user, administrator, and service accounts for enterprise assets and software.



CIS Security Controls to Mitigate Cyberattacks Risk

By Implementing these security controls, an organization can mitigate the risk of cyberattacks by over 80%

- › **07: Continuous Vulnerability Management:** Develop a plan to continuously assess and track vulnerabilities on all enterprise assets within the enterprise's infrastructure, in order to remediate, and minimize, the window of opportunity for attackers.
- › **08: Audit Log Management:** Collect, alert, review, and retain audit logs of events that could help detect, understand, or recover from an attack.
- › **09: Email and Web Browser Protection:** Improve protections and detections of threats from email and web vectors, as these are opportunities for attackers to manipulate human behavior through direct engagement.



CIS Security Controls to Mitigate Cyberattacks Risk

By Implementing these security controls, an organization can mitigate the risk of cyberattacks by over 80%

- › **10: Malware Defense:** Prevent or control the installation, spread, and execution of malicious applications, code, or scripts on enterprise assets.
- › **11: Data Recovery:** Establish and maintain data recovery practices sufficient to restore in-scope enterprise assets to a pre-incident and trusted state.
- › **12: Network Infrastructure Management:** Establish, implement, and actively manage (track, report, correct) network devices, in order to prevent attackers from exploiting vulnerable network services and access points.



CIS Security Controls to Mitigate Cyberattacks Risk

By Implementing these security controls, an organization can mitigate the risk of cyberattacks by over 80%

- › **13: Network Monitoring and Defense:** Operate processes and tooling to establish and maintain comprehensive network monitoring and defense against security threats across the enterprise's network infrastructure and user base.
- › **14: Security Awareness and Skills Training:** Establish and maintain a security awareness program to influence behavior among the workforce to be security conscious and properly skilled to reduce cybersecurity risks to the enterprise.
- › **15: Service Provider Management:** Develop a process to evaluate service providers who hold sensitive data, or are responsible for an enterprise's critical IT platforms or processes, to ensure these providers are protecting those platforms and data appropriately.



CIS Security Controls to Mitigate Cyberattacks Risk

By Implementing these security controls, an organization can mitigate the risk of cyberattacks by over 80%

- › **16: Application Software Security:** Manage the security life cycle of in-house developed, hosted, or acquired software to prevent, detect, and remediate security weaknesses before they can impact the enterprise.
- › **17 Incident Response Management:** Establish a program to develop and maintain an incident response capability (e.g., policies, plans, procedures, defined roles, training, and communications) to prepare, detect, and quickly respond to an attack.
- › **18: Penetration Testing:** Test the effectiveness and resiliency of enterprise assets through identifying and exploiting weaknesses in controls (people, processes, and technology), and simulating the objectives and actions of an attacker

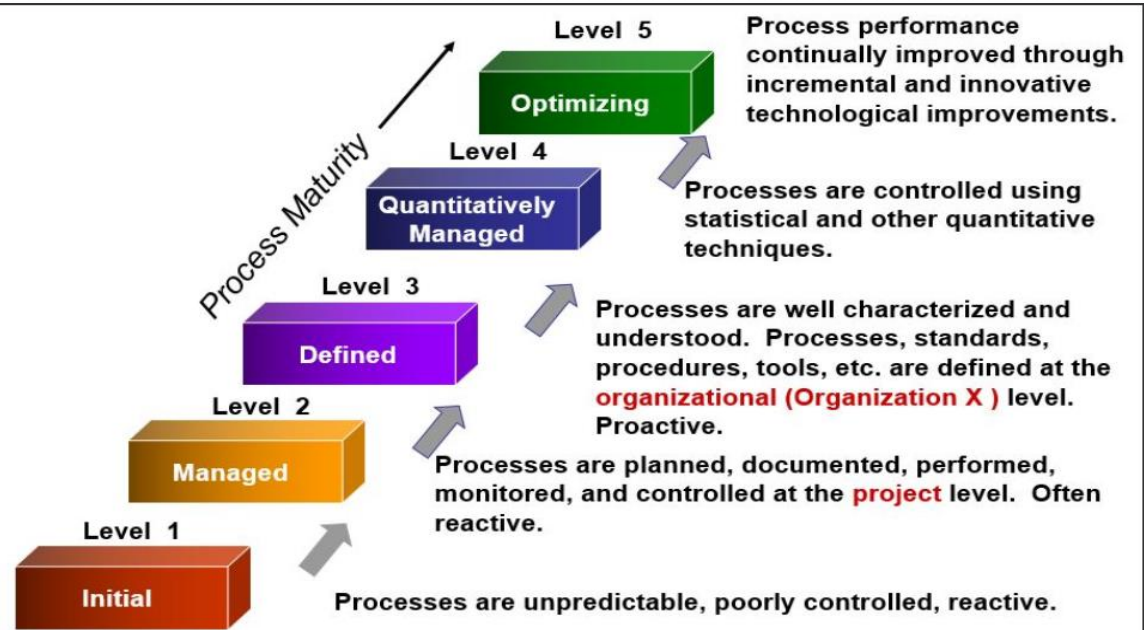


CMMI Cybersecurity Models

CMMI

What is CMMI?

Capability Maturity Model Integration (CMMI) is a process level improvement training and appraisal program.



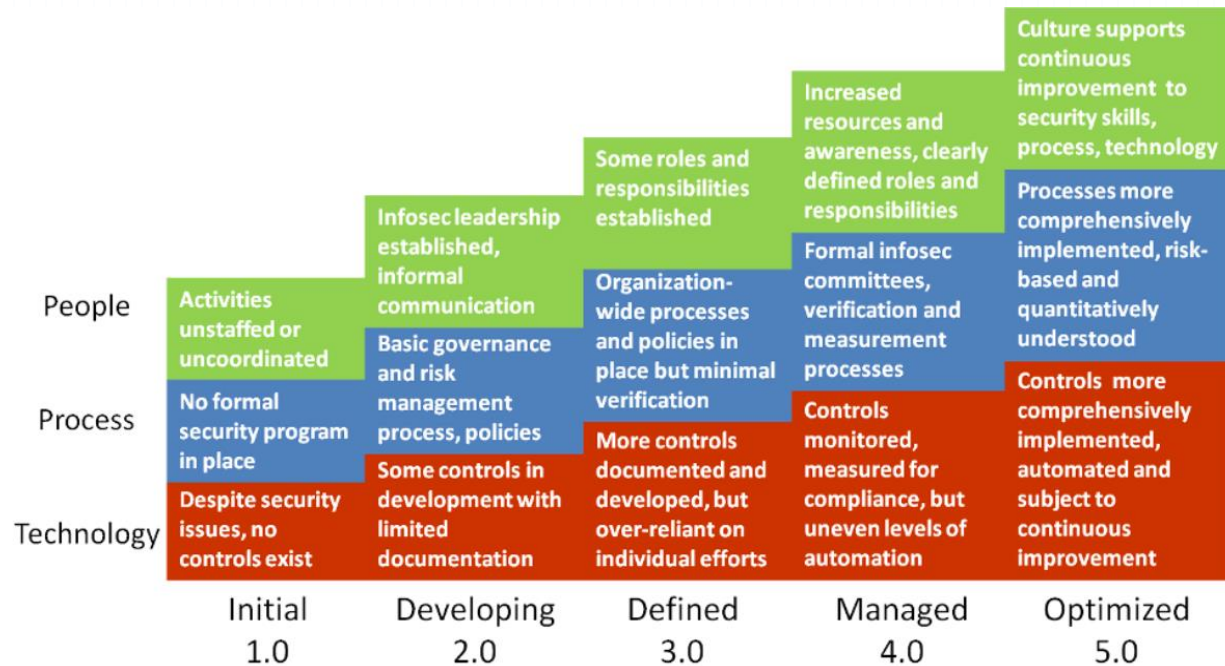
CMMI Maturity Levels

NIST CSF Cybersecurity Framework

NIST CSF

What is NIST CSF?

The NIST cybersecurity framework is used to organize and improve a cybersecurity program.



NIST CSF Maturity Levels

COBIT5 Cybersecurity Framework

COBIT5

What is COBIT5?

COBIT 5 is a framework from the Information Systems Audit and Control Association (ISACA) for the management and governance of information technology (IT).

Level	Status	Description
0	Non-existent	Process is not applied at all.
1	Initial/ <i>ad hoc</i>	Process is ad hoc and disorganized.
2	Repeatable but intuitive	Process follows regular patterns.
3	Defined process	Process is documented and communicated.
4	Managed and measurable	Process is monitored and measured.
5	Optimized	Process follows best practices and automated

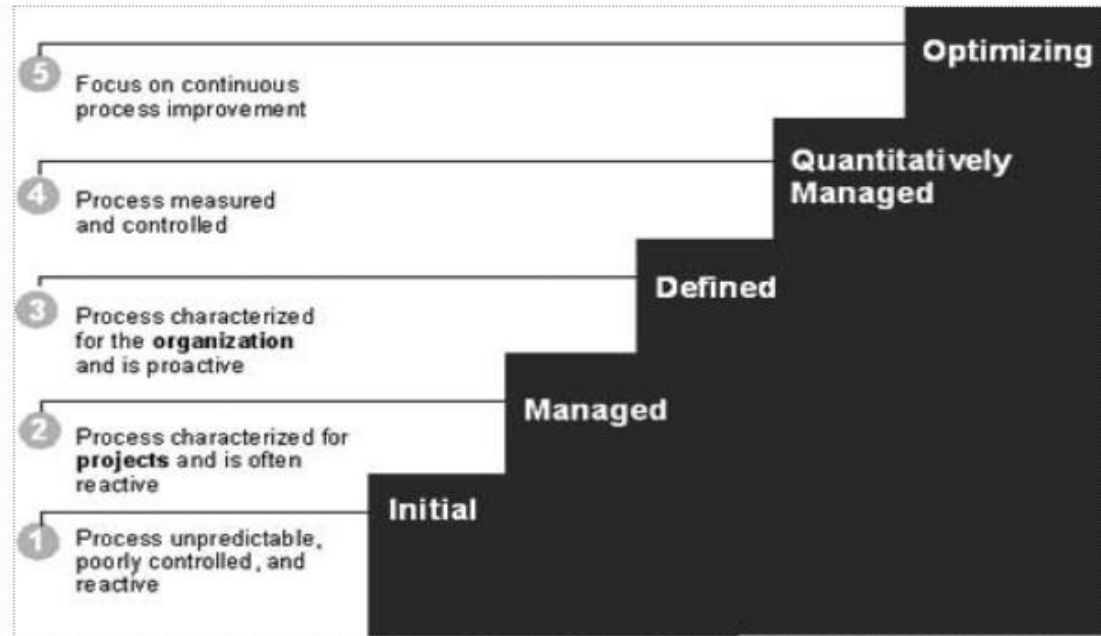
COBIT5 Maturity Levels

CMMC Cybersecurity Model Certification

CMMC

What is CMMC?

The Department of Defense's (DoD) Cybersecurity Maturity Model Certification (CMMC) is an assessment standard designed to ensure that defense contractors are in compliance with current security requirements for protecting sensitive defense information.



CMMC Maturity Levels

Cybersecurity Models and Framework Levels

LEVEL	CMMI	NIST CSF	COBIT5	CMMC
0			Non-Existent	
1	Initial	Initial	Initial	Initial
2	Managed	Developing	Repeated but Intuitive	Managed
3	Defined	Defined	Defined Process	Defined
4	Quantitatively Managed	Managed	Managed and Measurable	Quantitatively Managed
5	Optimizing	Optimized	Optimized	Optimizing

InfoSec Program using the Security Controls

- › Definition of an InfoSec Program
- › Program Charter
- › Domains



InfoSec Program Charter

Program Charter

Introduction

The vision of ANTHC is Alaska Native people are the healthiest in the world. ANTHC recognizes that Alaska Natives have a choice to use ANTHC for their medical needs and want to be the provider of choice for Alaska Natives. We understand that our job is a role of service and want to provide the best possible care for Alaska Natives.

Program Charter

This Charter and the information security policies adopted by ANTHC are the basis of our information security program.

These documents provide a high-level view of how information assets that have been entrusted to ANTHC will be protected and document the responsibilities of ANTHC staff in providing this protection.

The goal of any security program is a continual improvement; however, we understand that constant reevaluation and adjustment are required.

InfoSec Program Domains

- › This HIT information security program comprises of 18 control domains from a common security framework derived from the Critical Security Controls and complying with the NIST 800-53 Framework.

- › The controls have been mapped to the
 - ISO 27001/27002
 - HIPAA
 - HITECH
 - Omnibus Final
 - PCI/DSS



Developing an InfoSec Program using the Security Controls

- › **01: Inventory and Control of Enterprise Assets:** Enterprise assets (end-user devices, including portable and mobile
 - network devices;
 - Internet of Things (IoT)
 - servers
 - VMs
 - Remote Devices
 - cloud environments.

Assessment Criteria



Security Risk Management Assessment Checklist



Information Security Policy

1. Information Security Policy Document

- o Does an information security policy exist, which is approved by the management, published and communicated as appropriate to all employees?
- o Does it state the management commitment and set out the organizational approach to managing information security?

2. Review and Evaluation

Does the Security policy have an owner, who is responsible for its maintenance and review according to a defined process?



Security of Third Party Access

1. Identification of risks from third party

- o Are risks from third party access identified and appropriate security controls implemented?
- o Are the types of accesses identified, classified and reasons for access justified?
- o Are secure risks with third party contractors working onsite identified and appropriate controls implemented?



Responding to security/threat incidents

1. Reporting security/ threat incidents

- a) Does a formal reporting procedure exist, to report security/threat incidents through appropriate management channels as quickly as possible?

2. Reporting security weaknesses

- a) Does a formal reporting procedure or guideline exist for users, to report security weakness in, or threats to, systems or services?



Media handling and security

1. Management of removable computer media

- a) Does a procedure exist for management of removable computer media such as tapes, disks, cassettes, memory cards and reports?



Business Requirements for Access control

1. Access Control Policy

- a) Have the business requirements for access control been defined and documented.
- b) Does the Access control policy address the rules and rights for each user or group of users?
- c) Are the users and service providers given a clear statement of the business requirement to be met by access controls?



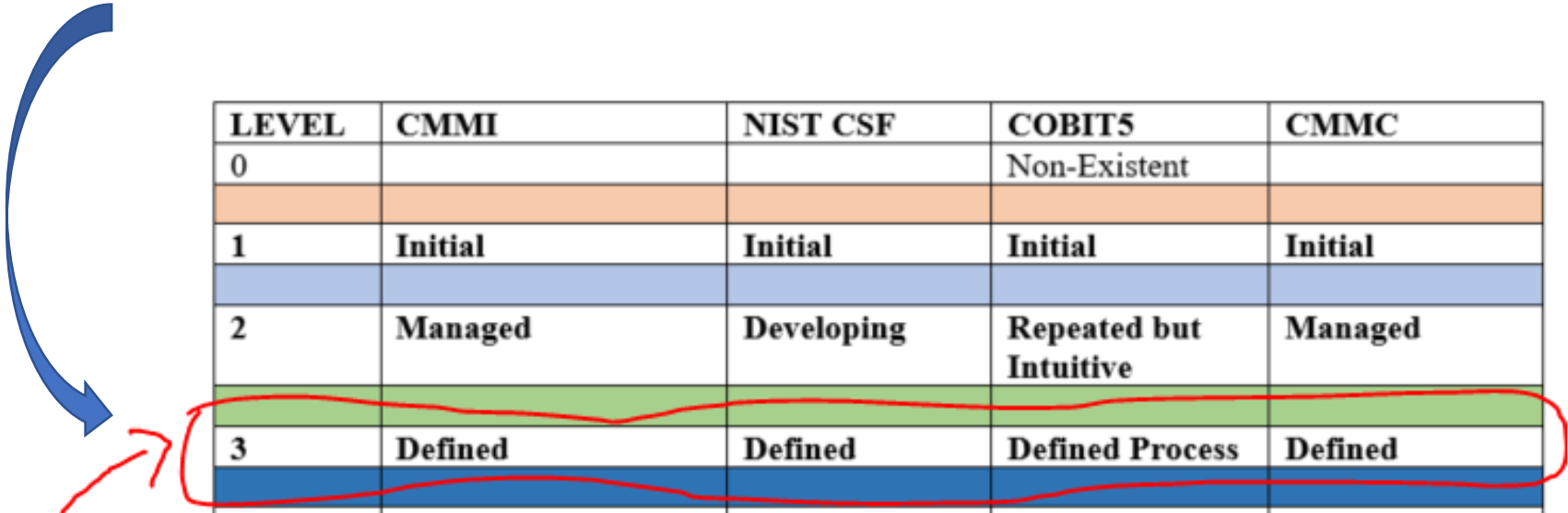
Exchange of information and software

1. Information and software exchange agreement

- a) Is there any formal or informal agreement between the organizations for exchange of information and software?

Cybersecurity Models and Framework Levels

- › **01: Inventory and Control of Enterprise Assets:** Enterprise assets (end-user devices, including portable and mobile
 - network devices;
 - Internet of Things (IoT)
 - servers
 - VMs
 - Remote Devices
 - cloud environments



LEVEL	CMMI	NIST CSF	COBIT5	CMMC
0			Non-Existent	
1	Initial	Initial	Initial	Initial
2	Managed	Developing	Repeated but Intuitive	Managed
3	Defined	Defined	Defined Process	Defined
4	Quantitatively Managed	Managed	Managed and Measurable	Quantitatively Managed
5	Optimizing	Optimized	Optimized	Optimizing

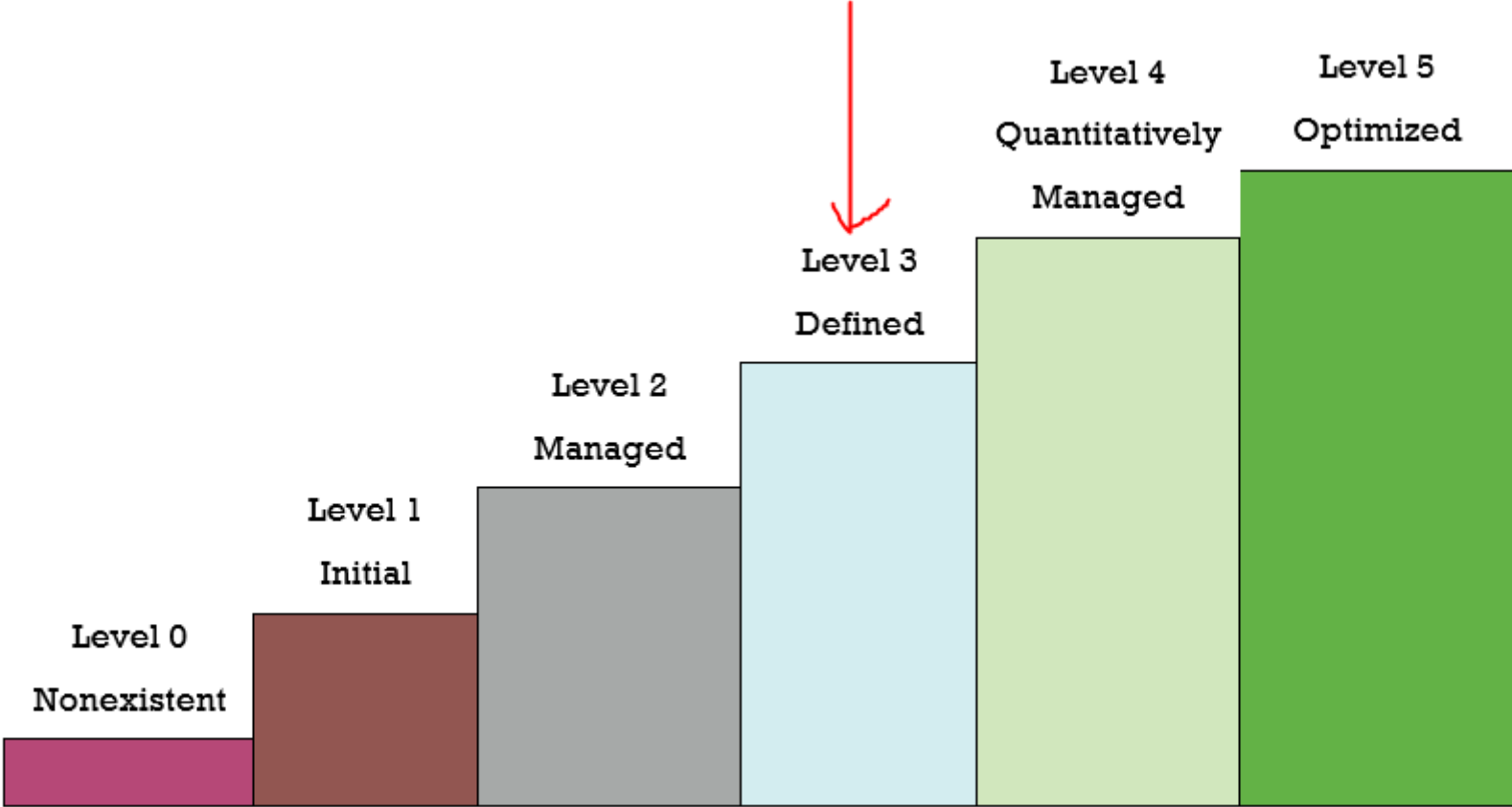
InfoSec Program using the Security Controls Level

Security Control	Level Achieved	Corrective Action Plan
Enterprise Hardware Assets Inventory	3	<ul style="list-style-type: none">• Improvement of policies• Training and Awareness• Update assets databases
Continuous Vulnerability Management	2	

InfoSec Program Model and framework

NIST CSF Tier	CMMI Maturity Level	COBIT 5 Maturity Level	Description	Categories
Tier 4 - Adaptive	5 – Optimizing	5 - Optimized Process	Stable and flexible: The process is defined, meets its outcomes, and is continuously improved to meet relevant current and projected business goals	0
	4 – Quantitatively managed	4 - Predictable Process	Measured and controlled: The process operates within defined limits to achieve its process outcomes	0
Tier 3 - Repeatable	3 – Defined	3 - Established Process	Proactive, rather than reactive: The process is implemented using a defined process that is capable of achieving its process outcomes	0
Tier 2 - Risk Informed	2 – Managed	2 - Managed Process	Managed on the project level: The process is implemented in a managed fashion and its work products are appropriately established, controlled, and maintained	0
Tier 1 - Partial	1 – Initial	1 - Performed Process	Unpredictable and reactive: The implemented process achieves its process purpose	0
	0 – Incomplete	0 - Incomplete	Ad hoc and unknown: The process is not implemented or fails to achieve its process purpose	0
	N/A - Not	N/A - Not Applicable	Control does not apply	0

InfoSec Program Graphical Presentation





Milton Kabia
ISSO/IT Security Director ANTHC
mkabia@anthc.org