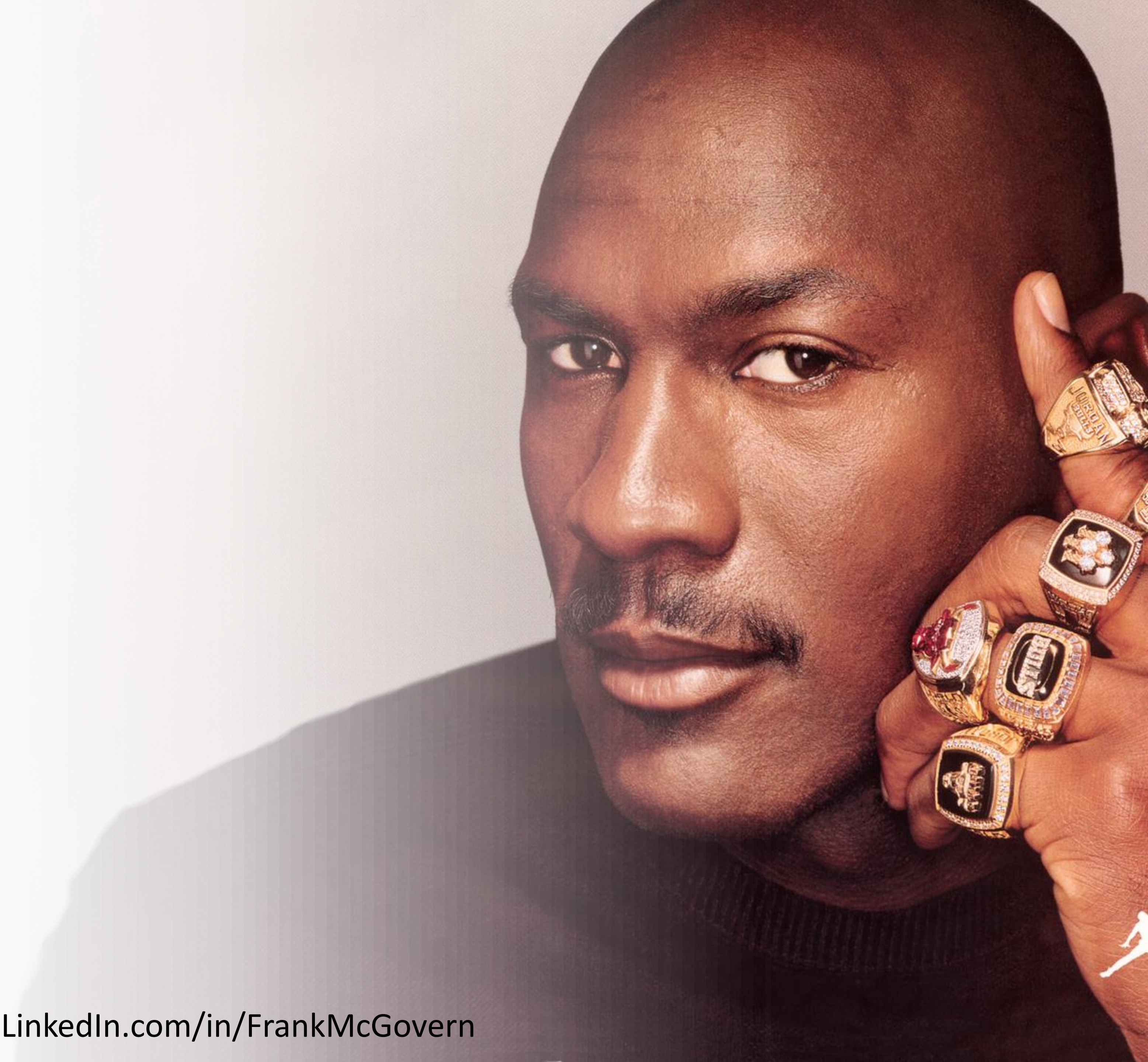
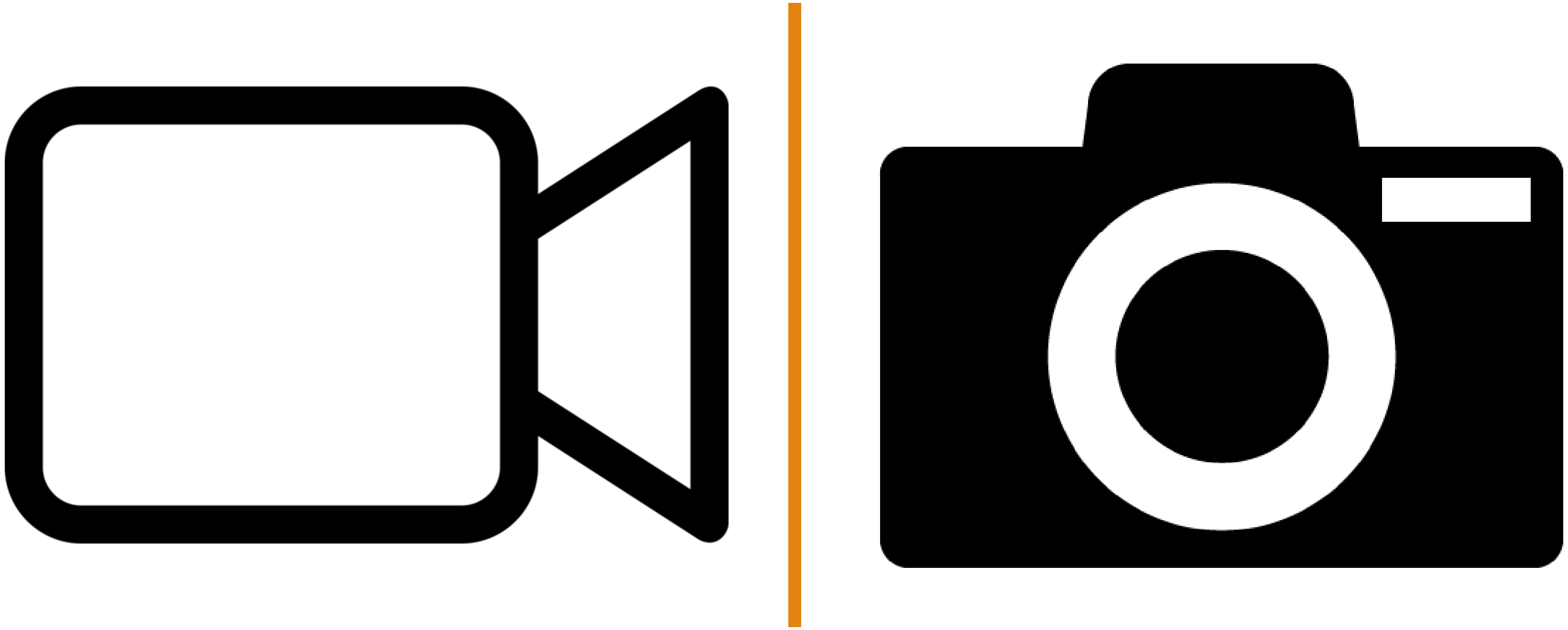
Writing Cybersecurity Policies: You Don't Have to be Michael Jordan



Frank McGovern

FrankMcG.com @FrankMcG LinkedIn.com/in/FrankMcGovern



Photos and Recording Allowed

whoami

Frank McGovern – Chicago, IL
CISSP, CISM, CSM

Former USMC 0231

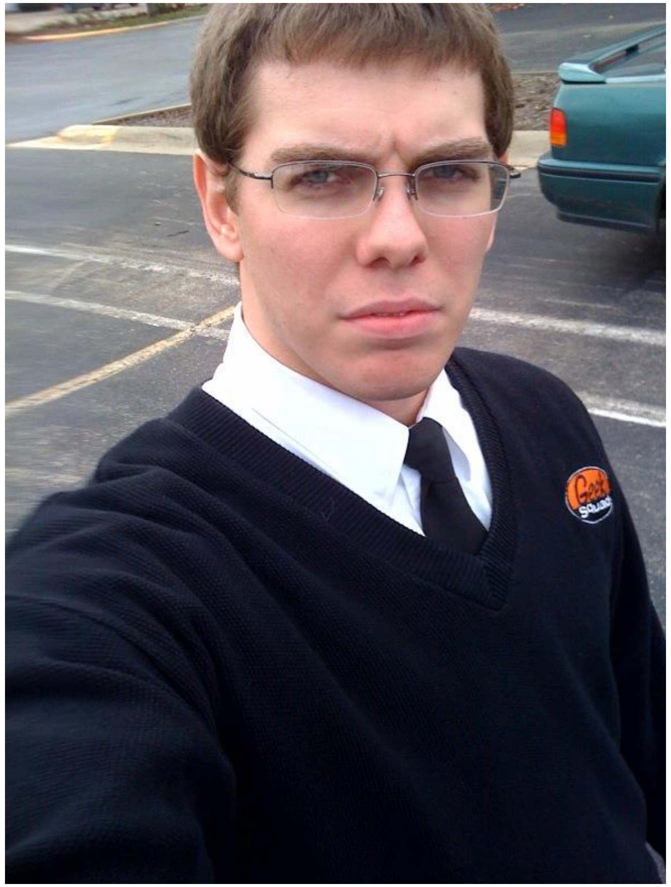
Walsh Construction: 2010 to 2020

- Help Desk -> Infrastructure Engineer -> Network Security Engineer -> Information Security Engineer -> Sr. Information Security Engineer

StoneX: 2020 to Present

- Cybersecurity Architect

Blue Team Con Founder



Why?

Documentation.

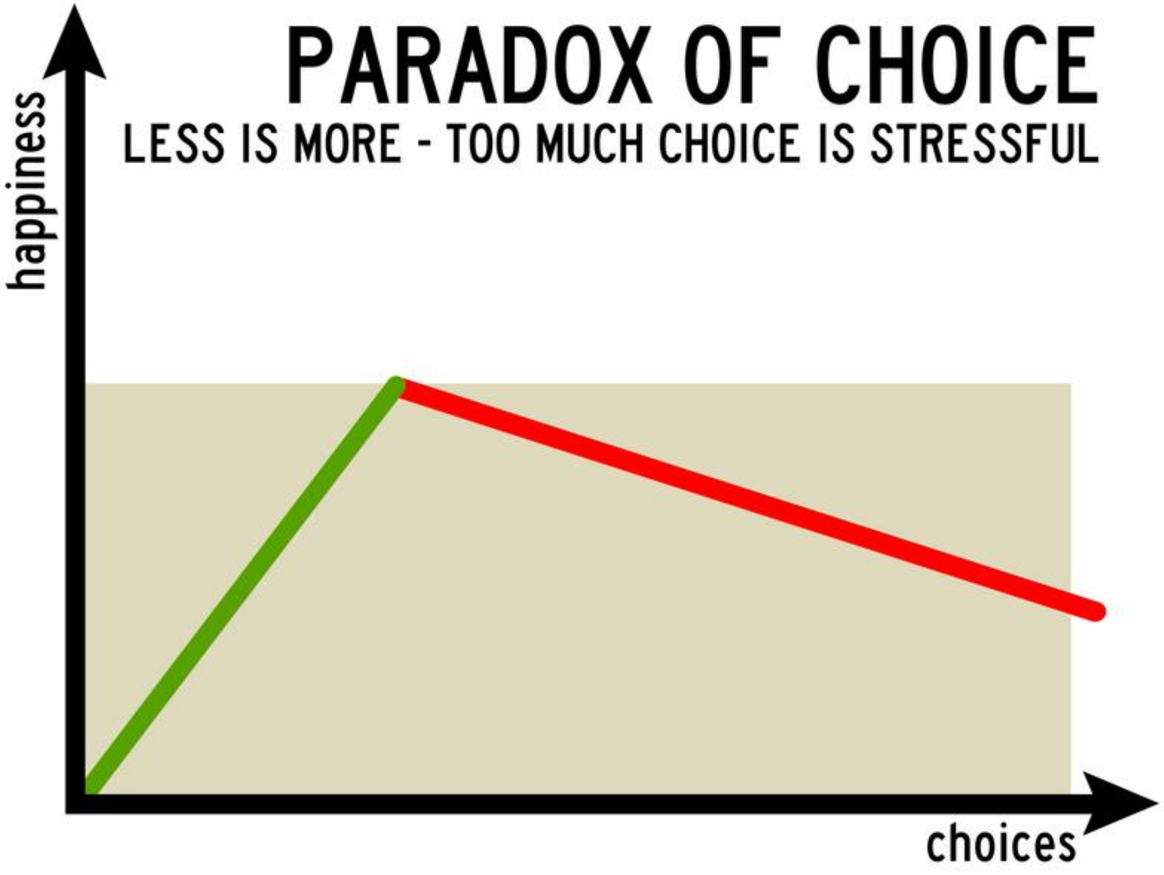
Documentation.

Documentation.

Terminology

GUIDELINES
PROCEDURES
CONTROL OBJECTIVES
RISKS
FRAMEWORK
STANDARDS
INFLUENCERS
METRICS
CONTROLS
POLICIES
REGULATIONS
THREATS

Analysis Paralysis



Understanding The Hierarchical Nature of Cybersecurity & Privacy Documentation

Version 2021.1

COMPLIANCE FORGE

The **ComplianceForge** Hierarchical Cybersecurity Governance Framework™(HCGF) takes a comprehensive viewtowards the necessary documentation components that are key to being able to demonstrate evidence of due diligence and due care. This framework addresses the interconnectivity of policies, control objectives, standards, guidelines, controls, risks, procedures & metrics. The Secure Controls Framework (SCF) fits into this model by providing the necessary cybersecurity and privacy controls an organization needs to implement to stay both secure and compliant. ComplianceForge has simplified the concept of the hierarchical nature of cybersecurity and privacy documentation in the following diagram to demonstrate the unique nature of these components, as well as the dependencies that exist:

Influencers (Internal & External)

Hierarchical cybersecurity governance starts with external influencers – these establish what is considered necessary for due diligence and due care for cybersecurity operations. These include statutory requirements (laws), regulatory requirements (government regulations) and contractual requirements (legally-binding obligations) that organizations must address.

External influencers usually impose meaningful penalties for non-compliance. External influencers are often non-negotiable and are the primary source for defining a need for a policy and provide scoping for control objectives.

Internal influencers focus on management's desire for consistent, efficient and effective operations. This generally takes the form of:
- Business strategy
- Goals & objectives (e.g., customer satisfaction / service levels, budget constraints, quality targets, etc.)

Policies

Policies are high-level statements of management intent from an organization's executive leadership that are designed to influence decisions and guide the organization to achieve the desired outcomes.

Policies are enforced by standards and further implemented by procedures to establish actionable and accountable requirements.

Policies are a business decision, not a technical one. Technology determines how policies are implemented. Policies usually exist to satisfy an external requirement (e.g., law, regulation and/or contract).

Control Objectives

Control Objectives are targets or desired conditions to be met. These are statements describing what is to be achieved as a result of the organization implementing a control, which is what a Standard is intended to address.

Where applicable, Control Objectives are directly linked to an industry-recognized secure practice to align cybersecurity and privacy with accepted practices. The intent is to establish sufficient evidence of due diligence and due care to withstand scrutiny.

Standards

Standards are mandatory requirements in regard to processes, actions, and configurations that are designed to satisfy Control Objectives.

Standards are intended to be granular and prescriptive to establish **Minimum Security Requirements (MSR)** that ensure systems, applications and processes are designed and operated to include appropriate cybersecurity and privacy protections.

Guidelines

Guidelines are recommended practices that are based on industry-recognized secure practices. Guidelines help augment Standards when discretion is permissible.

Unlike Standards, Guidelines allow users to apply discretion or leeway in their interpretation, implementation, or use.

Controls

Controls are technical, administrative or physical safeguards. Controls are the nexus used to manage risks through preventing, detecting or lessening the ability of a particular threat from negatively impacting business processes.

Controls directly map to standards, since control testing is designed to measure specific aspects of how standards are actually implemented.

Control testing is routinely used in pre-production testing to validate a project or system has met a minimum level of security before it is authorized for use in a production environment. Recurring testing is often performed on certain controls in order to verify compliance with statutory, regulatory and contractual obligations.

SCF SECURE CONTROLS FRAMEWORK

Procedures

Procedures are a documented set of steps necessary to perform a specific task or process in conformance with an applicable standard.

Procedures help address the question of how the organization actually operationalizes a policy, standard or control. Without documented procedures, there can be defendable evidence of due care practices.

Procedures are generally the responsibility of the process owner / asset custodian to build and maintain, but are expected to include stakeholder oversight to ensure applicable compliance requirements are addressed.

The result of a procedure is intended to satisfy a specific control. Procedures are also commonly referred to as "control activities."

Risks

Risks represent a situation where someone or something valued is exposed to danger, harm or loss (noun) or to expose someone or something valued to danger, harm or loss (verb).

In practical terms, a risk is associated with a control deficiency? (e.g., if the control fails, what risk(s) is the organization exposed to?)

Risk is often calculated by a formula of *Threat x Vulnerability x Consequence* in an attempt to quantify the potential magnitude of a risk instance occurring.

While it is not possible to have a totally risk-free environment, it may be possible to manage risks by avoiding, reducing, transferring, or accepting the risks.

Threats

Threats represent a person or thing likely to cause damage or danger (noun) or to indicate impending damage or danger (verb).

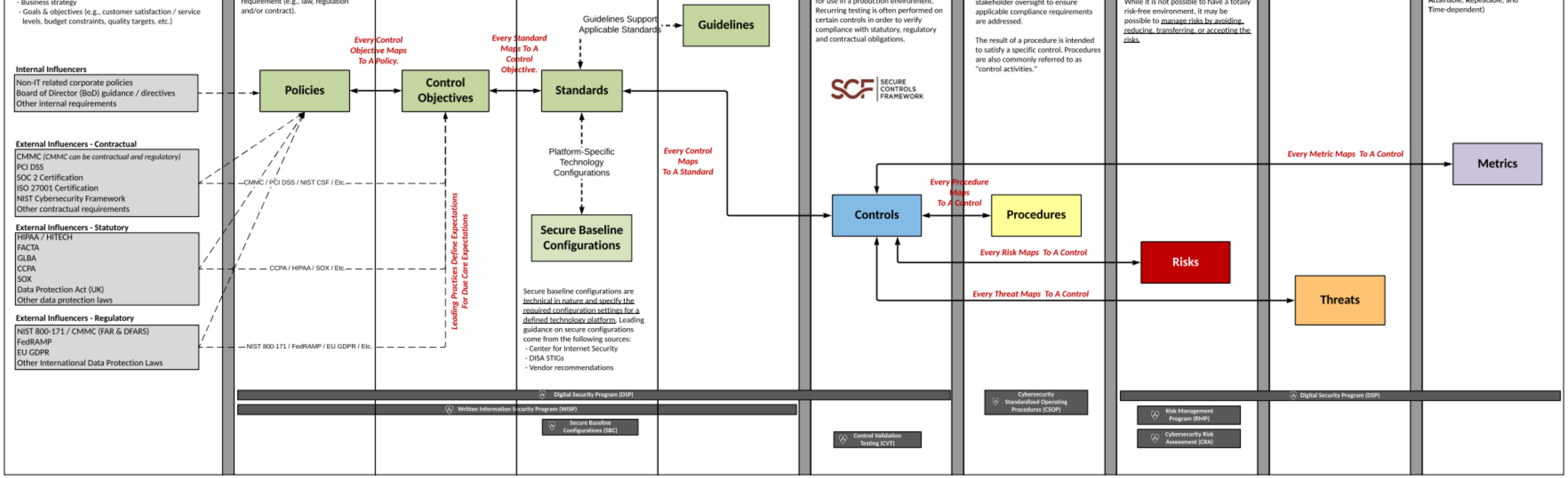
In practical terms, a threat is a possible natural or man-made event that affects control execution. (e.g., if the threat materializes, will the control function as expected?)

Metrics

Metrics provide a "point in time" view of specific, discrete measurements, unlike trending and analytics that are derived by comparing a baseline of two or more measurements taken over a period of time. Analytics are generated from the analysis of metrics.

Analytics are designed to facilitate decision-making, evaluate performance and improve accountability through the collection, analysis and reporting of relevant performance-related data.

Good metrics are those that are **SMART** (**S**pecific, **M**easurable, **A**ttainable, **R**epeatable, and **T**ime-dependent)



Internal Influencers

Non-IT related corporate policies
Board of Director (BoD) guidance / directives
Other internal requirements

External Influencers - Contractual

CMMC *(CMMC can be contractual and regulatory)*
PCI DSS
SOC 2 Certification
ISO 27001 Certification
NIST Cybersecurity Framework
Other contractual requirements

External Influencers - Statutory

HIPAA / HITECH
FACTA
GLBA
CCPA
SOX
Data Protection Act (UK)
Other data protection laws

External Influencers - Regulatory

NIST 800-171 / CMMC (FAR & DFARS)
FedRAMP
EU GDPR
Other International Data Protection Laws

Secure baseline configurations are technical in nature and specify the required configuration settings for a defined technology platform. Leading guidance on secure configurations come from the following sources:
- Center for Internet Security
- DISA STIGs
- Vendor recommendations

Policies
Control Objectives
Standards
Guidelines
Secure Baseline Configurations
Controls
Procedures
Risks
Threats
Metrics
Every Control Objective Maps To A Policy.
Every Standard Maps To A Control Objective.
Guidelines Support Applicable Standards
Platform-Specific Technology Configurations
Every Control Maps To A Standard
Every Procedure Maps To A Control
Every Risk Maps To A Control
Every Threat Maps To A Control
Every Metric Maps To A Control
CMMC / PCI DSS / NIST CSF / Etc.
CCPA / HIPAA / SOX / Etc.
NIST 800-171 / FedRAMP / EU GDPR / Etc.
Leading Practices Define Expectations For Due Care Expectations
Digital Security Program (DSP)
Written Information Security Program (WISP)
Secure Baseline Configurations (SBC)
Control Validation Testing (CVT)
Cybersecurity Standardized Operating Procedures (CSOP)
Risk Management Program (RMP)
Cybersecurity Risk Assessment (CRA)
Digital Security Program (DSP)

Top-Down Process Flow of Cybersecurity & Privacy Governance Concepts

Internal & External Influencers primarily drive the development of cybersecurity and privacy policies. This requirements analysis is a component of governance, risk and compliance management practices to appropriately scope security program requirements.

Policies define high-level expectations and provide evidence of due diligence to address applicable requirements (internal and external).

Control Objectives support Policies and provide scoping for Standards, based on industry-recognized secure practices.

Standards operationalize Policies by providing organization-specific requirements that must be met.

Guidelines provide useful guidance that provides additional content to help operationalize Standards.

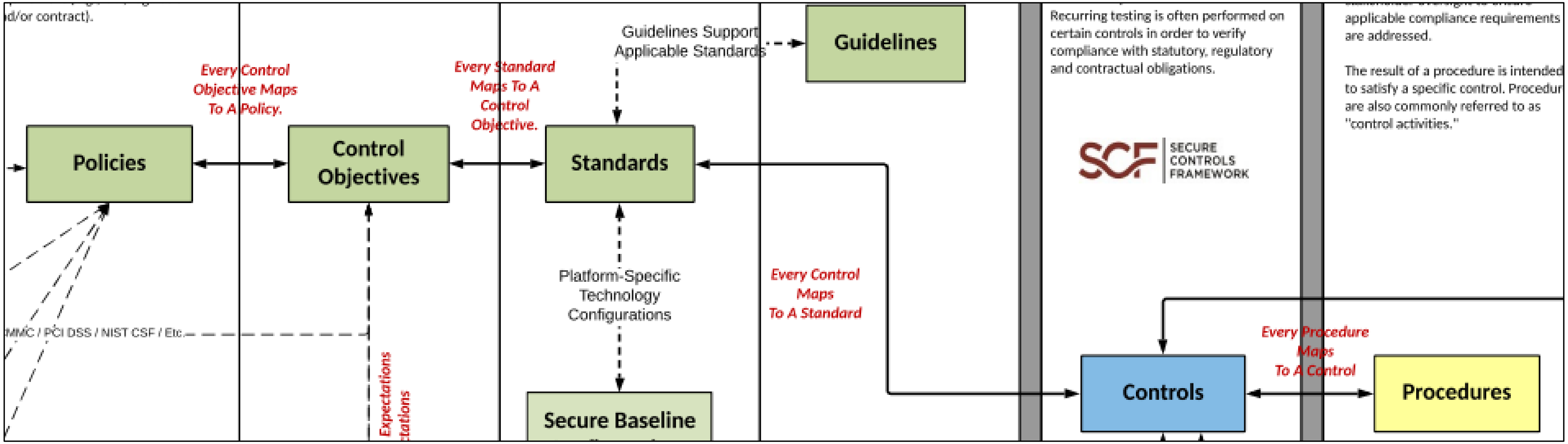
Controls are assigned to stakeholders to assign responsibilities in enforcing Standards.

Procedures operationalize Standards and Controls. The output of Procedures is evidence of due care to demonstrate that requirements are enforced.

Structuring controls as questions is often used to in questionnaire format to evaluate the implementation of a control.

Metrics provide evidence of an oversight function for the cybersecurity and privacy program by measuring criteria to determine performance.

The Basics

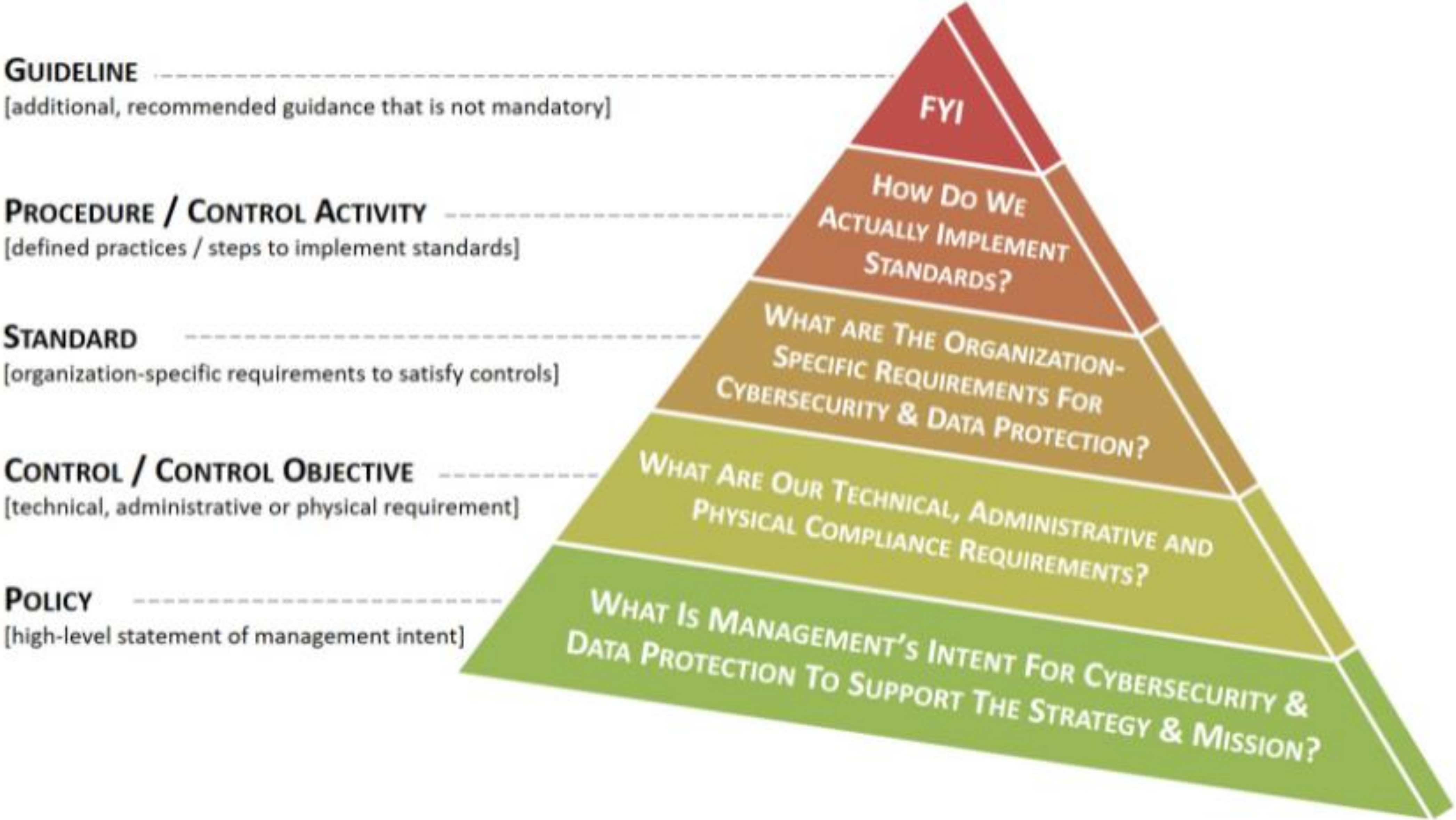


d/or contract).
Every Control Objective Maps To A Policy.
Every Standard Maps To A Control Objective.
Guidelines Support Applicable Standards
Guidelines
Policies
Control Objectives
Standards
Platform-Specific Technology Configurations
Secure Baseline
MMC / PCI DSS / NIST CSF / Etc.
Expectations
tations
Every Control Maps To A Standard
SECURE CONTROLS FRAMEWORK
Every Procedure Maps To A Control
Controls
Procedures

Recurring testing is often performed on certain controls in order to verify compliance with statutory, regulatory and contractual obligations.

applicable compliance requirements are addressed.

The result of a procedure is intended to satisfy a specific control. Procedur are also commonly referred to as "control activities."



Guideline
[additional, recommended guidance that is not mandatory]

Procedure / Control Activity
[defined practices / steps to implement standards]

Standard
[organization-specific requirements to satisfy controls]

Control / Control Objective
[technical, administrative or physical requirement]

Policy
[high-level statement of management intent]

FYI

How Do We Actually Implement Standards?

What are The Organization-Specific Requirements For Cybersecurity & Data Protection?

What Are Our Technical, Administrative and Physical Compliance Requirements?

What Is Management's Intent For Cybersecurity & Data Protection To Support The Strategy & Mission?

1984-1985
AIR JORDAN
1 ROOKIE OF THE YEAR

Example – Auto Detailing

Policy

- All vehicles will be properly washed prior to customer delivery.

Standards

- Every vehicle will follow the entire 21-step wash process.
- Wheels will be washed with Sonax Full Effect and scrubbed with a Wheel Woolie Brush.
- A foam cannon will be used with Feynlab Pure Wash (2021 Edition) on all exterior panels.

Controls

- Cameras will monitor the wash bay. (Physical)
- All employees will be taught the proper 21-step wash process by a senior detailer. (Administrative)

Example - IAM

Policy

- All laptops issued by the organization must have identity and access controls in place.

Standards

- All laptops are configured to ensure complex, 15-character passwords using Active Directory.
- All laptops are fitted with a biometric reader and a TPM 1.2 chip to store those biometrics.

Controls

- Group Policy is set to require the 10-character password. (Technical)
- New laptops are purchased with biometric reader and TPM 1.2 chip. (Administrative)

Policy Timeline

- Current State (n+1)
- Future State (n+5)

Recommended Policy Building Process

1. Follow a Framework – *NIST CSF*
2. Follow a Standard that has Control Objectives – *NIST 800-53*
3. Solo Write Policies
4. Collaborate those Policies
5. Obtain Senior Leadership Approval

Guided Example – Control Objective

NIST 800-53 #AC-17

The organization:

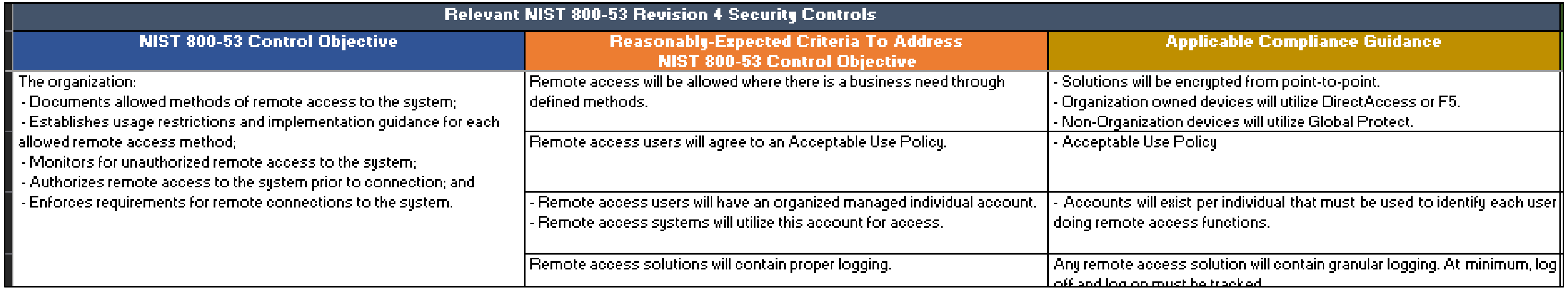
- Documents allowed methods of remote access to the system;
- Establishes usage restrictions and implementation guidance for each allowed remote access method;
- Monitors for unauthorized remote access to the system;
- Authorizes remote access to the system prior to connection; and
- Enforces requirements for remote connections to the system.

Guided Example – Policies

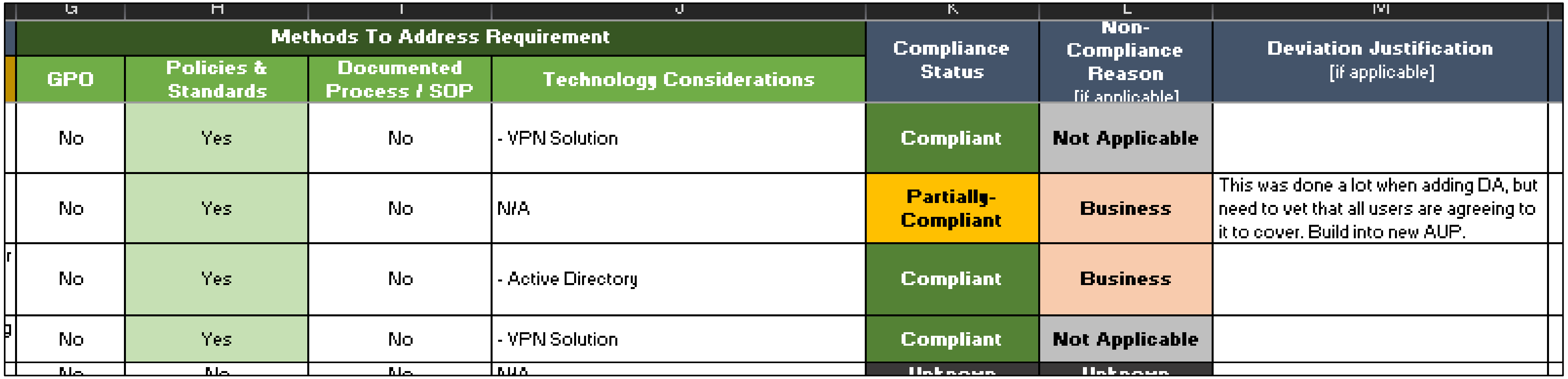
- Remote access will be allowed where there is a business need through defined methods.
- Remote access users will agree to an Acceptable Use Policy.
- Remote access users will have an organized managed individual account.
- Remote access systems will utilize this account for access.
- Remote access solutions will contain proper logging.

...and I took that personally

Compliance Tracking



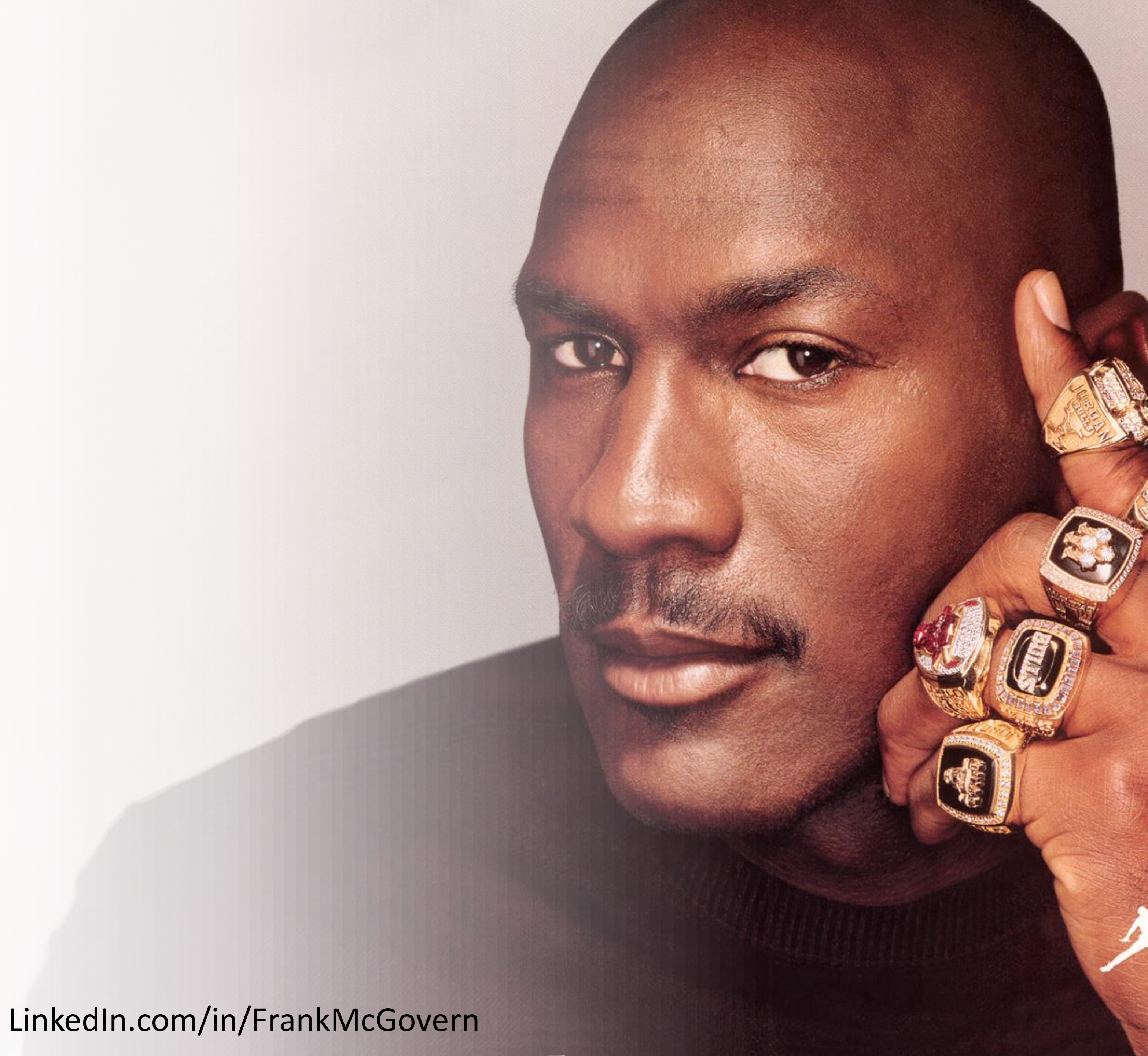
Relevant NIST 800-53 Revision 4 Security Controls		
NIST 800-53 Control Objective	Reasonably-Expected Criteria To Address NIST 800-53 Control Objective	Applicable Compliance Guidance
The organization: - Documents allowed methods of remote access to the system; - Establishes usage restrictions and implementation guidance for each allowed remote access method; - Monitors for unauthorized remote access to the system; - Authorizes remote access to the system prior to connection; and - Enforces requirements for remote connections to the system.	Remote access will be allowed where there is a business need through defined methods.	- Solutions will be encrypted from point-to-point. - Organization owned devices will utilize DirectAccess or F5. - Non-Organization devices will utilize Global Protect.
	Remote access users will agree to an Acceptable Use Policy.	- Acceptable Use Policy
	- Remote access users will have an organized managed individual account. - Remote access systems will utilize this account for access.	- Accounts will exist per individual that must be used to identify each user doing remote access functions.
	Remote access solutions will contain proper logging.	Any remote access solution will contain granular logging. At minimum, log off and log on must be tracked.



G	H	I	J	K	L	M
Methods To Address Requirement				Compliance Status	Non-Compliance Reason [if applicable]	Deviation Justification [if applicable]
GPO	Policies & Standards	Documented Process / SOP	Technology Considerations			
No	Yes	No	- VPN Solution	Compliant	Not Applicable	
No	Yes	No	N/A	Partially-Compliant	Business	This was done a lot when adding DA, but need to vet that all users are agreeing to it to cover. Build into new AUP.
No	Yes	No	- Active Directory	Compliant	Business	
No	Yes	No	- VPN Solution	Compliant	Not Applicable	
No	No	No	N/A	Unknown	Unknown	

Writing Cybersecurity Policies: You Don't Have to be Michael Jordan

Frank McGovern



FrankMcG.com   @FrankMcG   LinkedIn.com/in/FrankMcGovern