Scope of an IT Compliance Audit

Content

1) What must to do to be in Compliance?
   - Protecting and Securing Privacy Data
   - Designing and Implementing Proper Security Controls
2) Auditing within IT Infrastucture

3) Maintaining IT Compliance
   - Conducting Periodic Security Assessments
   - Defining Proper Security Controls
   - Creating an IT Security Policy Framework

Introduction

- Audit comes in all sizes and shapes.
- Regardless of size, Audit represent a systematic and measurable assessment of the environment of an organization.
- Auditing for IT compliance is part of the ongoing process to ensure an organization is putting in place and maintaining effective security policies and controls.
- The audit makes use of various tools, but is primarily concerned with how the security policies are actually used.
- The IT environment is vast, and can be broken down into manageable and auditable chunks or domains.

Must Do to be in Compliance

❑What Must Your Organization Do to Be in Compliance?

- Achieving compliance with external standards and regulations must be a first consideration in assembling a policy infrastructure.

- Being in compliance also means making sure the organization meets the expectations of the policy by enforcing the infrastructure put into place.

- An organization must consider current laws and industry standards along with the organization's mission.

Must Do to be in Compliance

- **Organizational policies** provide general statements that address the operational goals of an organization. The role of information technology is to help accelerate the business.

- At the same time, consider security and compliance with laws and regulations to safeguard data. Specifically, IT and IT security policies provide the same high-level directives.

- This includes sensitive intellectual property of the organization and data that is commonly protected under privacy laws, such as personal information about individuals..

Must Do to be in Compliance

- Complying with an organization's internal policy requires standards.

- **Internal standards** describe mandatory processes or objectives that align with the goal of the policies.

- Establishing both policies and standards is critical for ensuring the success of the organization as well as compliance with the myriad regulations with which organizations must comply.

Must Do to be in Compliance

- A good starting place is with a solid organizational governance **framework**.
- This framework considers the applicable laws and regulations and then sets the high-level requirements to secure and control the IT infrastructure.
- Frameworks such as COBIT provide a blueprint for implementing high-level controls within an organization.
- Further, control standards such as ISO/IEC 27002 and NIST 800-53 provide more specific security controls.

Must Do to be in Compliance

❑When policies and control framework are in place, organizations can start implementing **specific controls**.

- Perhaps one of the greatest challenges is determining what specific controls to apply. Always consider what is reasonable and appropriate for your organization.

- Too often, organizations spend too much time and money implementing controls that go beyond the requirements.

- Many organizations may get compliance tunnel vision and they lose sight of really addressing risk, and are concerned only with being compliant.

Must Do to be in Compliance

- Consider that organizations are often required to comply with many different regulations.
- Many of these may have overlapping goals and intent. Therefore, you want to avoid chasing each one individually.
- By having sound policies in place and a framework for the application of controls, you will be able to map existing controls to each regulation, including future regulations.
- Thereafter, organizations perform a gap analysis to identify anything that is missing. A gap analysis is a comparison between the desired outcome and the actual outcome.

Must Do to be in Compliance

- Compliance with internal policies and compliance with legal requirements should be closely tied together.
- Each of these can be divided into two high-level control objectives.
- Compliance with legal and regulatory requirements.
- Compliance with security policies and standards and technical compliance.

Protecting and Securing Privacy Data

- In general, it is understood that **privacy data** must be protected. Depending on the environment in which an organization operates, privacy can take on different meanings

- "the rights and obligations of individuals and organizations with respect to the collection, use, disclosure, and retention of personal information." - AICPA

- There are numerous methods used to protect privacy data.

Protecting and Securing Privacy Data

❑A privacy audit focuses on the following:

- Which privacy laws apply to the organization?
- Are the organizational responsibilities defined and assigned (for example, for the privacy officer and the legal department)?
- Are policies and procedures for creating, storing, and managing privacy data applied and followed?
- Are specific controls implemented, and are compliance tasks being followed? For example, is privacy data encrypted? Are there privacy statements and an opt-out mechanism on the organization's Web site?

Designing and Implementing Proper Security Controls

- Information security is largely about managing risk. That means IT controls are implemented depending on the risk they are designed to manage.

- The focus is on **mitigating risk** by implementing appropriate security controls, there are other ways to deal with risk.

  I. Risk can be **Avoided**
  II. Risk can be **Transferred**
  III. Risk can be **Accepted**

Designing and Implementing Proper Security Controls

- Driving a vehicle poses many **risks**. Consider the risk of loss due to theft or an accident. Most people choose to **transfer the risk** by purchasing insurance. Others might **accept the risk** by not purchasing insurance. Still others might **avoid the risk** altogether by choosing not to drive.

Designing and Implementing Proper Security Controls

- Managing risks involves making tradeoffs.
- It is necessary to properly assess and prioritize risk.
- The process of selecting security controls needs to be part of an overall framework for risk management.

Designing and Implementing Proper Security Controls

- The following activities consider the implementation of controls within the context of such a framework:

I. Discover and classify data and information systems
II. Select security controls
III. Implement security controls
IV. Assess security controls
V. Authorize the controls
VI. Monitor the controls

Designing and Implementing Proper Security Controls

- Selecting security controls is best approached by first adhering to a common set of basic or baseline controls.
- You might need to apply additional controls that are specific to the system or application.

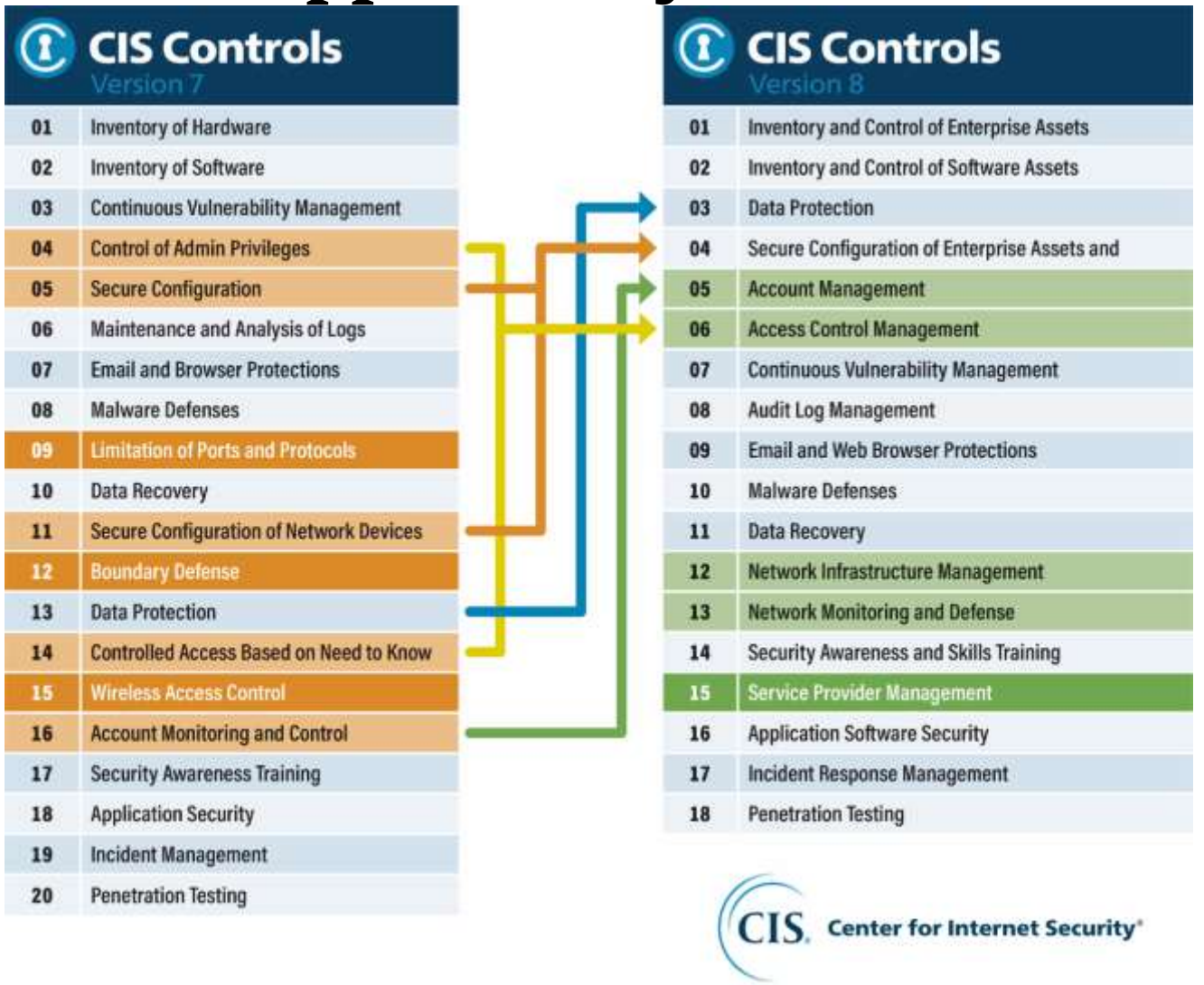
Designing and Implementing Proper Security Controls

- Some common control baselines from the **NIST Standard 800-53:**

CONTROLS FAMILY	CONTROL EXAMPLES
Access Control	Account Management; Separation of Duties; Least Privilege
Awareness and Training	Security Awareness; Security Training; Training Records
Audit and Accountability	Audit of Record Retention; Auditable Events
Security Assessment and Authorization	Plan of Action and Milestones; Security Authorization
Configuration Management	Baseline Configuration; Configuration Change Control
Contingency Planning	Contingency Training; Alternate Storage Site
Identification and Authentication	Identifier Management; Cryptographic Module Authentication
Incident Response	Incident Handling; Incident Monitoring; Incident Reporting
Maintenance	Controlled Maintenance; Maintenance Tools
Media Protection	Media Access; Media Marking; Media Storage
Physical and Environmental Protection	Physical Access Controls; Visitor Control; Fire Protection
Planning	System Security Plan; Privacy Impact Assessment
Personal Security	Personnel Screening; Personnel Termination
Risk Assessment	Security Categorization; Vulnerability Scanning
System and Services Acquisition	Allocation of Resources; Security Engineering Principles
System and Communications Protection	Denial of Service Protection; Boundary Protection
System and Information Integrity	Malicious Code Protection; Spam Protection; Error Handling
Program Management	Enterprise Architecture; Risk Management Strategy

Designing and Implementing Proper Security Controls

- Some Critical Security Controls from the **CIS Supported by SANS**:



Auditing Within the IT Infrastructure

- Across the infrastructure, an audit should focus primarily on the following three objectives:

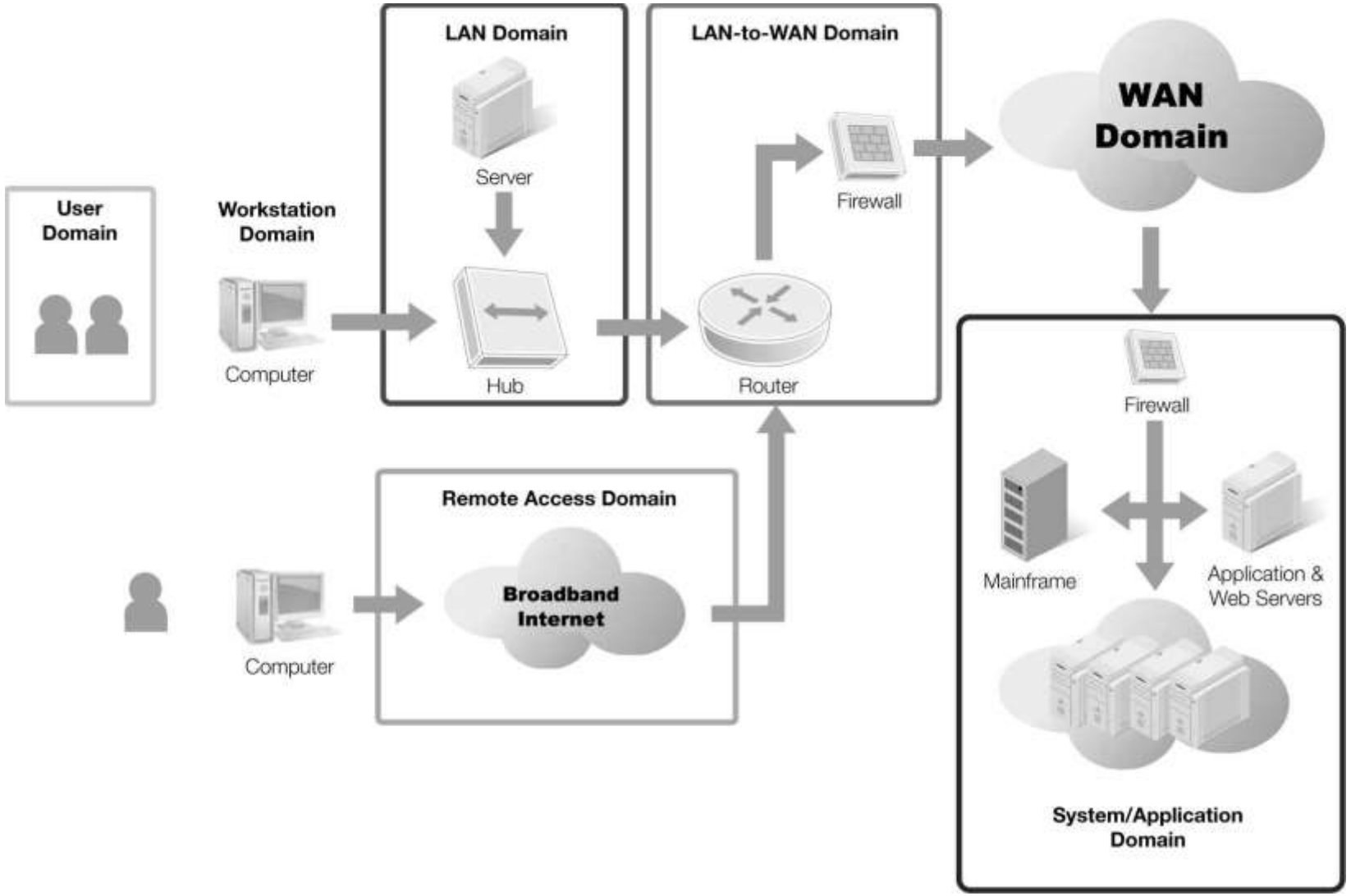
I. Examine the existence of relevant and appropriate security policies and procedures.

II. Verify the existence of controls supporting the policies.

III. Verify the effective implementation and ongoing monitoring of the controls.

Auditing Within the IT Infrastructure

❑7 Domains of IT Infrastructure:



Auditing Within the IT Infrastructure

❑7 Domains of IT Infrastructure:

I. **User Domain**—The end users of the systems, including how they authenticate into the systems.

II. **Workstation Domain**—The end users' operating environment.

III. **LAN Domain**—The equipment that makes up the local area network (LAN). A LAN is a computer network for communications between systems covering a small physical area.

IV. **LAN-to-WAN Domain**—The bridge between the LAN and the wide area network (WAN). A WAN is a network that covers a large area, often connecting multiple LANs.

Auditing Within the IT Infrastructure

❑7 Domains of IT Infrastructure:

V. **WAN Domain—**The equipment and activities outside of the LAN and beyond the LAN-to-WAN Domain.

VI. **Remote Access Domain—**The access infrastructure for users accessing remote systems.

VII. **System/Application Domain—**Systems on the network that provide the applications and software for the users.

Auditing Within the IT Infrastructure

❑User Domain:

- The User Domain covers the end users of information systems.
- This includes not just employees but nonemployees as well, such as contractors and consultants.
- This domain considers the roles and responsibilities of the users. It should examine all policies that relate to them—specifically, access policies by which the user authenticates to resources.
- Acceptable use policy (AUP), System access policy, Internet access policy, E-mail policy

Auditing Within the IT Infrastructure

❑Workstation Domain:

- The Workstation Domain comprises the desktop environment of an end user's computing environment and includes the following.

- Desktop computers
- Laptop computers
- Printers
- Scanners
- Handheld computers and mobile devices
- Modems
- Wireless access points

Auditing Within the IT Infrastructure

❑Workstation Domain:

- Each of these devices should be authorized to access and connect to the organizational network and information resources.
- An audit of this domain would also ensure proper procedures and controls around maintaining the system hardware and software defined by the policy and standard.
- Audit would take into consideration those security and configuration controls like standard operating system, patch management, anti malware, desktop firewall.

Auditing Within the IT Infrastructure

❑LAN Domain:

- A LAN is typically made up of computing and networking equipment in close proximity, such as a single room or building.

- LANs provide each computer on the network access to centralized resources, such as file servers and printers. Other elements like wiring, and networking equipment, such as hubs and switches.

- An audit of the LAN Domain can examine various elements, such as the following:
- Logon mechanisms and controls for access to the LAN
- Hardening and configuration of LAN systems
- Backup procedures for servers
- The power supply for the network

Auditing Within the IT Infrastructure

❑LAN to WAN Domain:

- A WAN can connect multiple LANs together with equipment like router or a firewall.
- The WAN Domain is considered an untrusted zone. The area between the trusted and untrusted zone, the LAN-to-WAN Domain, is protected with one or more firewalls. This is also called the boundary, or edge.
- Organizations should carefully manage the configurations of all devices in this domain, such as firewalls, routers, and intrusion detection systems.

Auditing Within the IT Infrastructure

❑WAN Domain:

- A WAN can connect multiple LANs together this environment includes routers, firewalls, and intrusion detection systems, but also has many more telecommunications components.
- For many businesses, the WAN is the Internet.
- Internet to be attacked even if that just means it is scanned for open ports and vulnerabilities. A significant amount of security is required to keep hosts in the WAN Domain safe.

Auditing Within the IT Infrastructure

❑Remote Access Domain:

- The Remote Access Domain is made up of the authorized users who access organization resources remotely.
- Remote access solutions, such as a virtual private network (VPN), can create an encrypted communications tunnel over a public network such at the Internet.
- A common control applied to VPN authentication requires the use of two-factor authentication.

Auditing Within the IT Infrastructure

❑System/Application Domain:

- It is made up of the many systems and software applications that users access. This, for example, includes mainframes, application servers, Web servers, proprietary software, and applications.

- Like the desktop operating system, server operating systems should be hardened to authorized baselines and configured according to policies and standards with the appropriate controls.

Maintaining IT Compliance

- Simply achieving compliance is not enough. Compliance is an ongoing process that should be treated as a continuous function within the organization.
- The following are primary examples of why organizations must maintain IT compliance as an ongoing program:
  - Organizations are dynamic, growing environments.
  - Threats evolve.
  - Laws, regulations, and industry standards continue to evolve, and new ones are introduced.
  - Many regulations require annual audits.

Maintaining IT Compliance

- Maintaining compliance requires a well-defined programmatic approach that involves processes and technology.

  - Regular assessment of selected security controls
  - Configuration and control management processes
  - Change management processes
  - Annual audit of the security environment

Maintaining IT Compliance

- **Conducting Periodic Assessment:**
- Security assessments provide valuable metrics for maintaining compliance.
- In general, an assessment should address people, operations, applications, and the infrastructure throughout the organization.
- Generally, a security assessment is grouped into different types:
  - High-level security assessment – overall view
  - Comprehensive security assessment – targeted, concise
  - Preproduction security assessment – for new system prior to production.

Maintaining IT Compliance

- **Creating an IT Security Policy Framework:**

- To maintain compliance, organizations should create a framework for IT security.

- A policy framework provides for a structured approach for outlining requirements that must be met.

Maintaining IT Compliance

- **Framework:** The framework starts on the top with very clear and concise objectives or requirements. A framework is a structured approach or system that provides the underlying structure for implementing policies, guidelines, and standards.

- **Policy:** The policy regulates conduct through a general statement of beliefs, goals, and objectives. It provides a clear direction for decision-making and behavior, ensuring alignment with the organization's objectives and values.

  - Users are required to use strong authentication when accessing company systems.

Maintaining IT Compliance

- **Standard:** The standards are mandated activities or rules. It specifies the exact criteria or specifications to be met.
  - Users are required to use two-factor authentication when accessing the remote network, combining a physical one-time token code with a personal identification number.

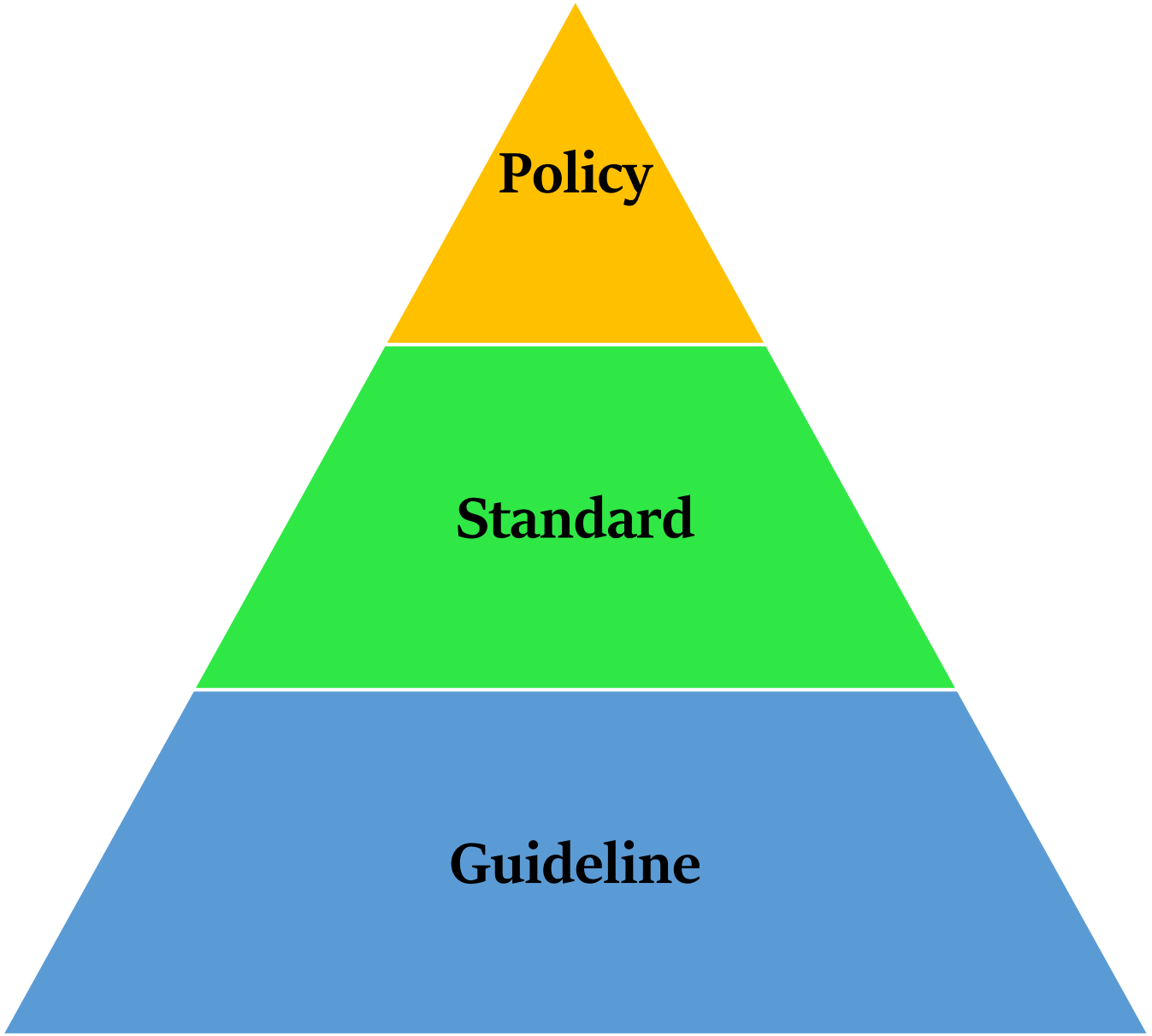
- **Guideline:** Guidelines provide general statements of guidance, but are not mandatory. It offers recommended advice to help achieve the policy objectives.
  - Always keep your token within your possession and be aware of your surroundings when entering your personal identification number.

Maintaining IT Compliance

- **Procedure:** A procedure provides step-by-step instructions that support the policy by outlining how the standards and guidelines are put into practice.

- A framework might state, for example, that systems should be protected from unauthorized access.
- As a result, an organization develops several policies that pertain to enforcing authorized access to its systems. One such policy states that individuals are assigned unique user names and passwords for the system.
- In turn, a standard may dictate specific parameters—for example, usernames must follow the format of first initial preceded by last name and be at least eight alphanumeric characters.
- Finally, a procedure indicates how to apply the requirements on a particular system.

Maintaining IT Compliance



References

[1] Weiss, M., & Solomon, M. G. (2015). Auditing IT infrastructures for compliance. Jones & Bartlett Publishers.

[2] GIPHY gifs

Truth, Transparency and Tactics Are the Characteristics of a good Auditor