System Security Planning

…the beginning

171Comply

www.171Comply.com

Effective System Security is the result of a **plan and a process**.
Our planning and process are built on:

Three Tenets of System Security Planning

Documentation

- Know what you have?
- Know who is using the system?
- Know the requirements, what do you have to do?
- Build a plan, and a plan of action.

Implementation

Action of:

- Control Access
- System Elements
- Encryption
- MFA
- Segmentation
- Protect:
  - Electronic Data
  - Physical Data

Sustainment

- Lifecycle Support
- Training
- Updates – HW, SW, Documentation
- Configuration Management
- Media:
  - Electronic Data
  - Physical Data

Documentation

Documentation

- Documentation = **the stuff, the requirements, baselines and assessments, and policies** that constitute the cybersecurity plan, includes a time-phased plan for implementation.
  - The documentation phase components are the foundation of the cybersecurity plan.
- Documentation – Know What You Have – Who is Using it
  - Baseline and Assessments, the configurations (HW & SW) and status of the information management system, system users, the cost estimates to upgrade, security review, and templates.

Documentation

- Documentation Phase Components:

The assessments and baseline reports provide the foundation for policy and for the plan of action.

- Policy, 60% of compliance is policy, the outline of the cybersecurity process and plan, the how the plan meets the requirements
  - Policy is dependent on the baseline and assessment reports, these describe the cybersecurity environment that is governed by policy
- Plan of Action and Milestones the plan of action will list the near-term, intermediate, and long-term goals. These are goals are driven by company resources, and strategic direction.

Documentation
The Detail

Documentation Phase

Documentation Phase Components:

- Baseline and Assessment, and reports
- Policy development
- Plan of Action and Milestones
- End state

Baseline and Assessment (Documentation)

- Where do you begin?
  - Know what you have.
  - Know who is using the resources that define the information management system.
    - Document what you have, and who is using the system.

Baseline and Assessment (Documentation)

- **Know what you have**, and who is using what resources that define the information management system.
  - ❑ Know what you have, it is more than an inventory, it is assessments, upgrade-updates, and a gap-analysis of the system.
  - ❑ Know who uses the system, it is about what resources are required for each job and who needs them.
  - ❑ Baseline and Assessment Reports:
    - Hardware
    - Network
    - Software
    - Physical Controlled Information
    - User Identity Matrix
    - Role-based Access Matrix
    - Map System Configuration

Baseline and Assessment (Documentation)

- Know what you have, Inventory and Assessment of hardware, network, physical inventory, and software.
  - Inventory hardware, physical documents, and network, look for what belongs and what is not needed, the goal is to reduce the information management system footprint.
  - Inventory software applications, reduce software to that is only needed.
  - Update or upgrade systems, determine the cost model associated with hardware and software updates and upgrades. Establish system baselines.

Baseline and Assessment (Documentation)

- Know who uses your system, what are the important tasks, who needs access, and who is responsible
  - User role-based access assessments is concurrent with hardware and software assessments.
  - Goal is to restrict access, and to eliminate user universal access.
  - Principal of the rule of least privilege, meaning when users are given access to resources, they are granted access to only the resources they need for their job. This is data, and physical access.

Policy (Documentation)

- The policies make the System Security Plan, they describe how the system meets the various cybersecurity requirements.
  - Policy is dependent on the baseline and assessment reports, these describe the cybersecurity environment that is to be governed by policy.
  - Policies are to be simple so that they can be followed, onerous policies will not be followed.
  - In terms of effort, 60% of compliance is policy, policy outlines the cybersecurity process and plan, policy is how the plan meets the requirements
  - Policies should complement the business environment and support the business strategic objectives.

Plan of Action and Milestones (POAM)

Establish a plan of action and milestones (POAM) to map out and track progress to implementation

- **3.12 SECURITY ASSESSMENT**
- **3.12.2** Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.

- The POAM is at the end state of the documentation phase:
  - A foundation for the POAM are the baseline and assessments reports, and policy
    - These determine compliance tasks completion over time (near-term, intermediate, long-term)
  - Includes sustainment tasks, training, follow on assessments, policy reviews, etc.

Documentation (End State)

- Completed Baseline and Assessment Reports (knowing what you have and knowing who is using the system and its resources) for: hardware, software, networks, diagrams of the system and networks, user role-based access.
- List of policy documents that are completed, or to be completed. First are the policies that are system independent, then focused on the policies that are information system dependent. Policy writing is the longest duration in this phase, and some policy sections will not be complete until the sustainment phase.
- Time phased schedule, many compliance tasks can be completed quickly, others take time and resources and there are intermediate or long-term goals. This time phased schedule is the foundation of the POAM.

Implementation

Implementation

- Implementation = **the action of meeting policy requirements**, it is the work of information management system set-up and configuration
  - The assessment and baseline reports and the cybersecurity policy define the cybersecurity system architecture. Meeting the cybersecurity requirements is implementation.
    - Implementation requires decision making in terms of the information system, ex. is the Information Management System In-house/Out-sourced, physical security considerations, etc.
    - It is the establishment of user role-based access to resources.
    - It is a contributor to the plan of action, as compliance requirements are met, and as resources are consumed or become available.

Implementation
The detail.

Implementation Phase

Implementation Phase:

- Putting into practice the compliance measurements of policy.
- Driven by the Plan of Action.
- Requires active participation of the business owner.
- The most challenging of all phases.
- End state.

Implementation, first step

- Implementation is completely dependent on the value of the cybersecurity polices as outline in the documentation phase.
  - The implementation requirements are defined by the plan of action, in the system security plan.
    - The ability to meet compliance is dependent on time and resources, compliance tasks are ordered in time.
  - Implementation is setting up the information management system to meet the policy requirements in terms of: systems, physical information (documents), and user access.
  - Implementation is where plan meets reality, and the plan of action is adjusted to reflect the realities of compliance.

Implementation, first step

- Implementation is the most difficult of the three phases, it is dependent on a number of factors.
  - The health of the system, older systems with out of date hardware and software will need to be upgraded or replaced.
  - The business owner is required to be an active participant in the implementation process, making decisions on: user role-based access, to keep the system in-house or out-sourced, the addition or removal of hardware or software, physical security, etc.
  - These issues will arise and will need to be scheduled or re-scheduled in the plan of action.

Implementation (End State)

- The end state is 100% compliance which could take considerable time.
- Some implementation tasks can be long-term compliance tasks, it is controlled by the plan of action.
- In general implementation is putting into practice the compliance measures as outlined in the policy.
- Implementation can be the most difficult task, in terms of setting up user roles, system boundaries, security measures for physical security and digital security, etc.

Sustainment

Sustainment

- Sustainment = **maintaining the cybersecurity plan over time and developing a culture of cybersecurity**.
  - Training is an essential element of sustainment, it is focused on developing and maintaining a cybersecurity culture.
  - Sustainment is maintaining the system with current software patches and versions.
  - Sustainment is assessing the system for risk and assessing company policies and procedures ensuring they are current.
  - It is the plan of action that guides implementation toward full compliance and ensures the project management milestones are meet in terms of annual assessments and actions focused on monitoring, and other processes.

Sustainment
The detail.

Sustainment Phase

Sustainment Phase Components:

- Driven by the Plan of Action.
- Completing compliance requirements.
- Includes training, system upgrades, monitoring.
- End state, a continuous phase.

Sustainment, first step

- Sustainment is not the last step in the process, it is an enduring process that continues throughout the lifecycle of the system.
- Sustainment actions include:
  - Training on the cybersecurity plan, and general cyber awareness to include: social engineering, phishing, user responsibilities, email best practices, etc.
  - Information system assessment, ensuring the system components are running current versions of the software and are patched.
  - Conducting periodic vulnerability and risk assessments to ensure the organization is addressing possible risk.

Sustainment, first step

- A point to consider is that these sustainment actions are to matched or scaled to the information management system.

  In smaller systems with fewer components and fewer users, there should be less time devoted to assessments; than to larger system with many components and many users.

Sustainment, (End State)

- The sustainment phase does not end, it is continuous throughout the system's life cycle.
- Elements of sustainment are established in this phase, to include:
  - Completing compliance requirements milestones (intermediate, and long-term).
  - Software and system maintenance schedules, the vulnerability and risk assessment schedules, incident response reviews, other policy reviews and updates, etc.
  - Training class schedules.
  - Other sustainment elements

Planning Considerations

Where do you begin (General Considerations)

- Essential is the active participation of the system or business owner.
- About 60% of compliance is policy, many policies are independent of the information management system, develop policies concurrently, i.e. Acceptable Use, Incident Response, etc.
- Full compliance is when the policy and information management system complement one another. What policy directs, the information management system implements.

Planning (General Considerations)

- Use a concurrent approach. Many tasks can be accomplished at the same time.
- What existing plans are there, that can be used for cybersecurity planning?
- Information management systems hardware and network system configurations, and software tools are about 40% of compliance, they are the most difficult to accomplish.
- Task are dependent on one another, poorly executed tasks will have negative effects on related tasks.