Welcome SoCo ISSA

7 October 2025

Structured IT Documentation: The Backbone of Cyber Resilience for IT Operations

Prepared by: Michael Lamb-Rollison
6 OCT 2025

Objective:

Discuss how IT Documentation brings technology environments to the next level by improving efficiency, enabling compliance, and strengthening cyber resilience capabilities.

Agenda

1.- Why IT Documentation Matters

2.- Uniform Formats, Storage, and Locations

3.- Configuration Templates and Scheduled Reviews

4.- Standard Operating Procedures (SOPs)

5.- Network Diagrams and Switch Interface Descriptions

6.- Hardware and Server Documentation: Real-World Impact

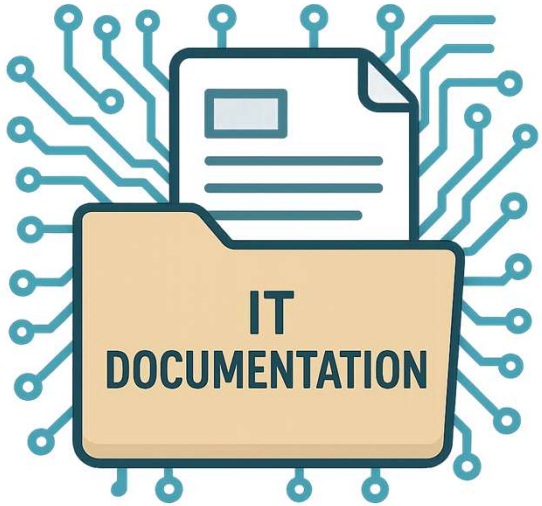
7.- Wireless, WAN, and Network Shares

8.- Phones, Ticketing, and Change Management

9.- Key Takeaways and Q&A

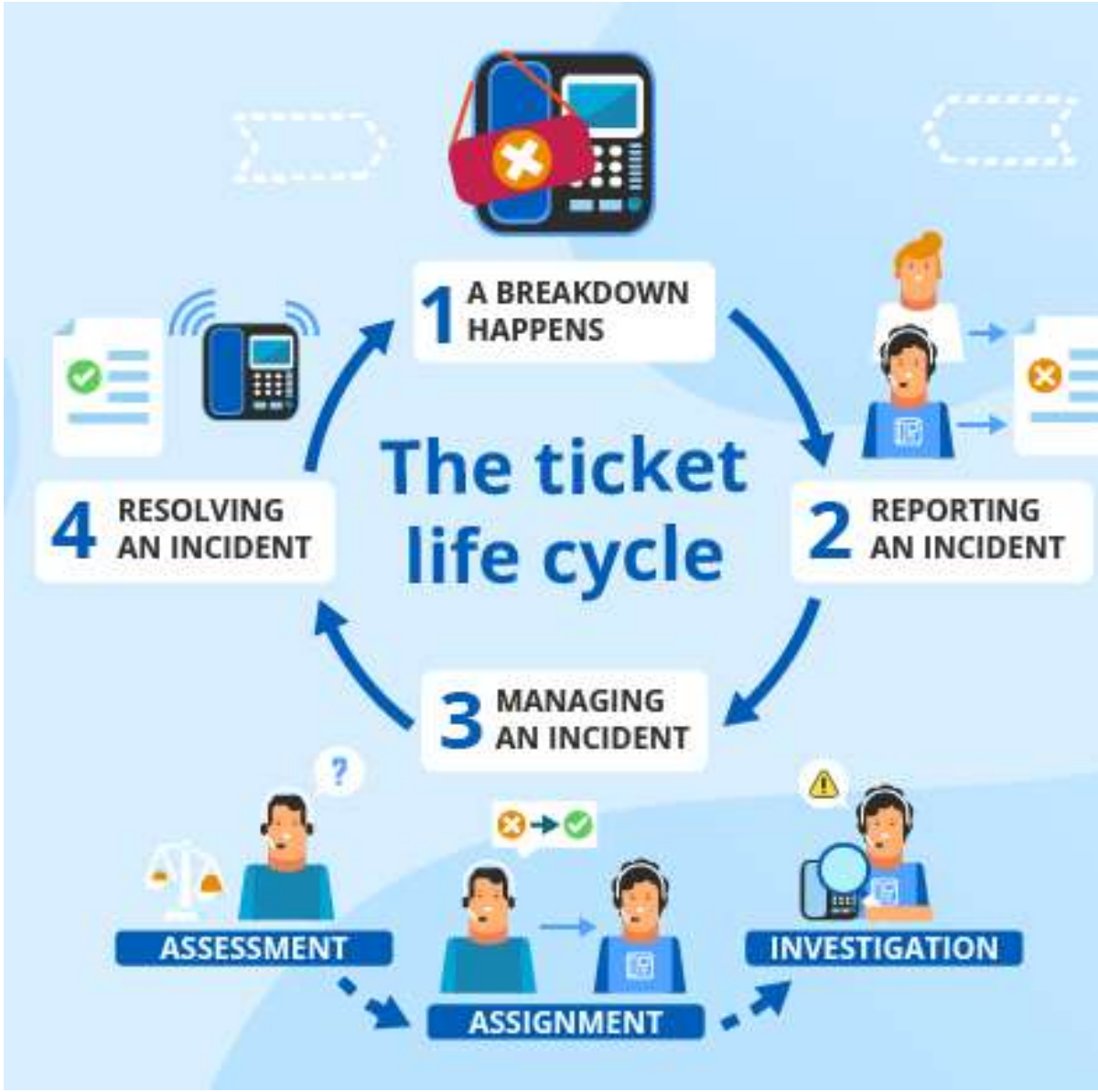
Why IT Documentation Matters

- Foundation of Cyber Resilience: Enables quick incident response, reduces downtime, and required for compliance (NIST, ISO 27001, SOC 2).
- Incident Response: Effective documentation allows for quick escalations, notifications, and mitigations.
- Efficiency Gains: Speeds up troubleshooting, onboarding, and future planning.
- Enhances team coordination and stakeholder trust.



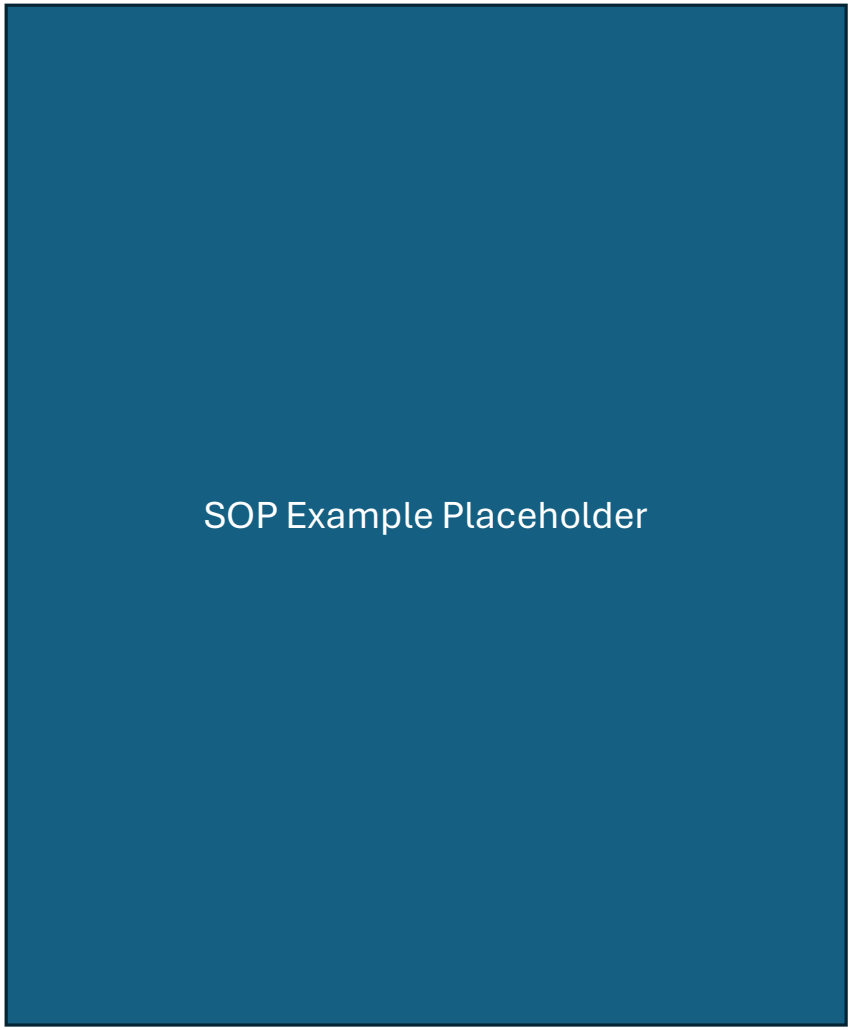
The Simplest Form of IT Documentation: Tickets!

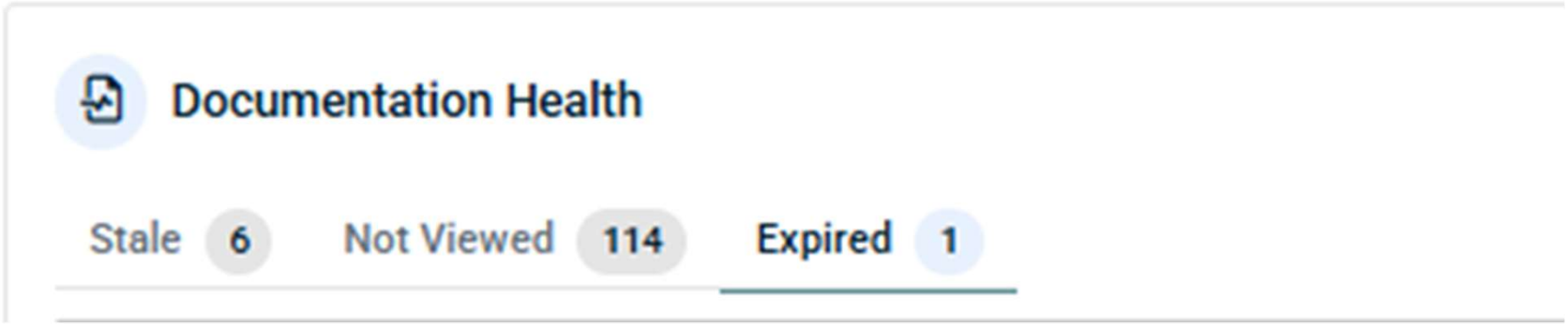
- Centralized issue tracking
- Records who has issues, who solves them, and how.
- Prioritization
- Trend Analysis
- Auditable



Uniform Documentation: Format, Storage, and Locations

- Standard Formats: Use templates like, Word docs, or fillable forms for consistency (e.g., sections for purpose, steps, updates, **Contacts**).
- Centralized Storage: Use a single, easily searchable location for all SOPs and other documentation. Popular examples are SharePoint, ITGlue, or simple Network Shares.
  - ITFlow is an open-source, self-hosted option.
- Categorize by type, like network or servers
- Use search-friendly naming conventions.
  - This means have a naming convention





Scheduled Reviews for Documentation

- Established Frequency: Quarterly for high-risk areas, annually for others.
- Process: Assign owners and POCs, use checklists, and track changes in a log.
- Tools: Use a tool that allows you to set an expiration date, or a review date.
- Consider building documentation updates into your SOPs.

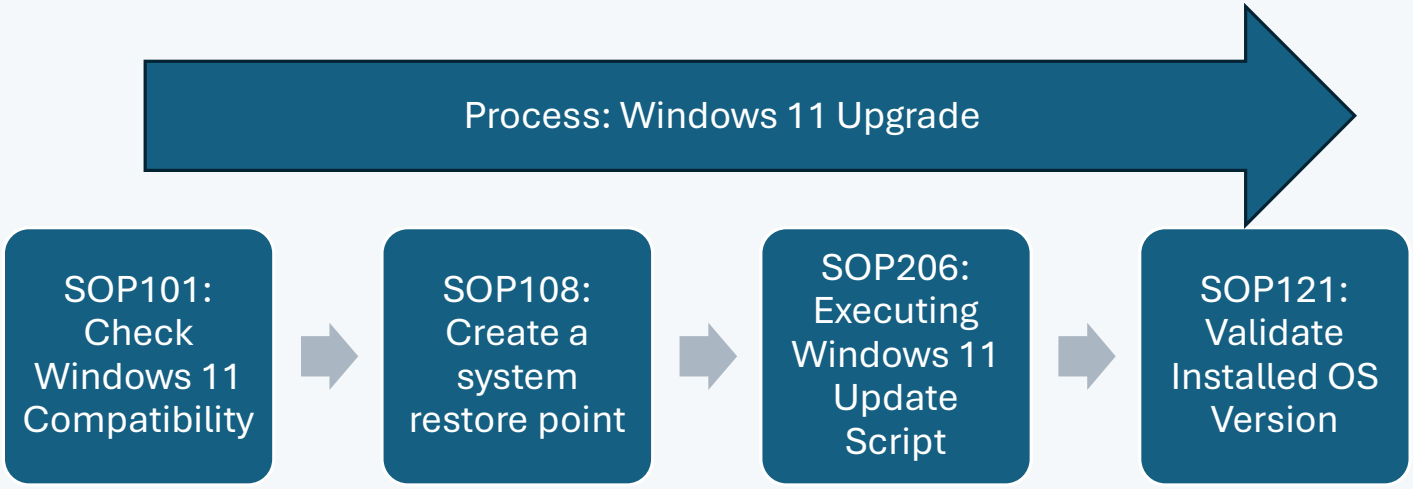
Configuration Templates

- Purpose: Pre-defined setups for devices (firewalls, switches, etc.) to ensure consistency and security baselines.
- Key Elements: Include everything that may be included in an approved configuration. Highlight key areas to modify. Instruct technicians to remove anything not necessary to the deployment.
- Use tools like Ansible to automate configurations. Consider tools like Cisco Prime Infrastructure, or Aruba NetEdit to monitor baselines, and identify deviations.
- Win: Prevents configuration drift.

Process vs. Procedure

- A Process is built of multiple procedures.
  - Think of your process as a task to complete
  - Procedures are the steps you will take to accomplish said task.

  - A process may be just one procedure, or it may be 20 of them.

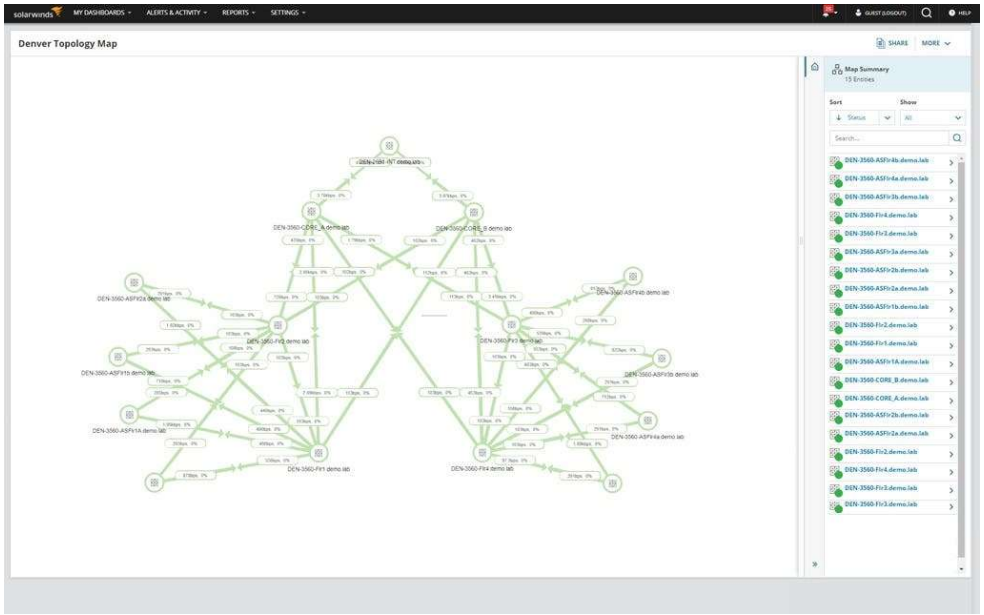


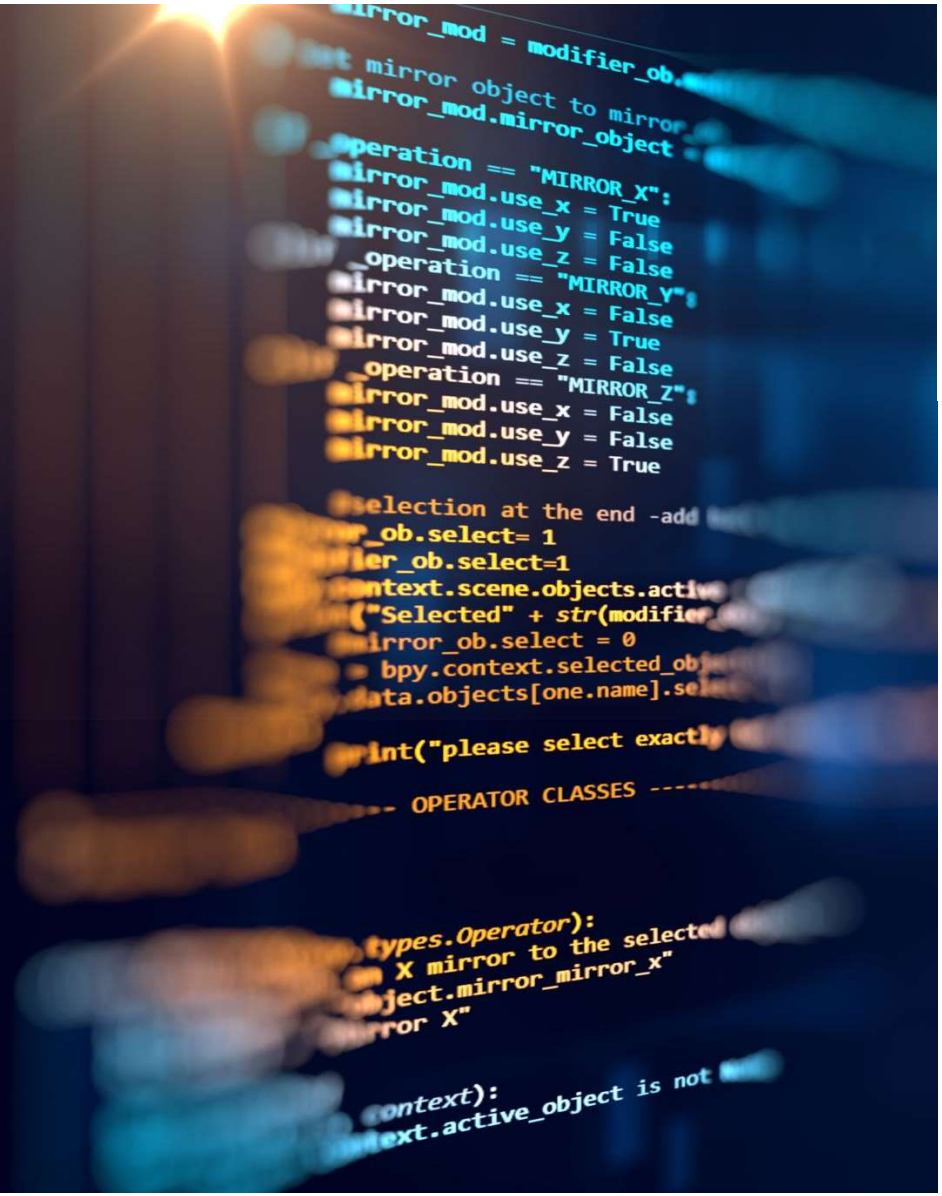
Standard Operating Procedures (SOPs)

- Step-by-step guides for routine tasks (e.g., ticket escalations, incident response, backups).
- Include scope, responsibilities, steps, and **a point of contact.**
- Best Practices: Make them actionable, visual, and testable via drills.
- Maintain baselines, standards, and **CYA**

Network Diagrams and Switch Interface Descriptions

- Network Diagrams: Visual maps of topology include IPs, hostnames, etc.
- Switch Interfaces: Use interface descriptions, have an SOP with a naming convention.
- Maintenance: Update your diagram after changes, leverage auto-discovery tools like SolarWinds, but don’t rely on them.
- Real-World Impact: In outages, accurate diagrams cut resolution time in half.





Hardware and Server Documentation

- Hardware: Inventory lists with serial numbers, warranties, and locations.
- Server Docs: OS versions, installed software, dependencies, and backup schedules.

Documenting Wireless, WAN, and Network Shares

- Wireless: SSIDs, encryption, WAP locations, MAC address and guest policies.
- WAN: ISP contact, circuit IDs, SLA, speeds
- Network Shares: Permissions, mappings, use-case

Phones, Ticketing, and Change Management

- Phones/VoIP: Call routing, Extensions, configs, and emergency routing, dependencies.
- Change Management: Processes for approvals, testing, and rollback
  - Integrate with your ticketing system, require techs to define the SOPs to be followed.
- Ensures auditable changes - prevents incidents due to unauthorized or untested changes.

Key Takeaways

- Structured docs build cyber resilience by enabling fast, consistent responses.
- Prioritize uniformity, templates, reviews, and specifics like networks and servers.
- Real-world impacts: Reduced downtime, compliance, and breach mitigation.
- Action Item: Review some of your docs this quarter!

ISSA

COLORADO