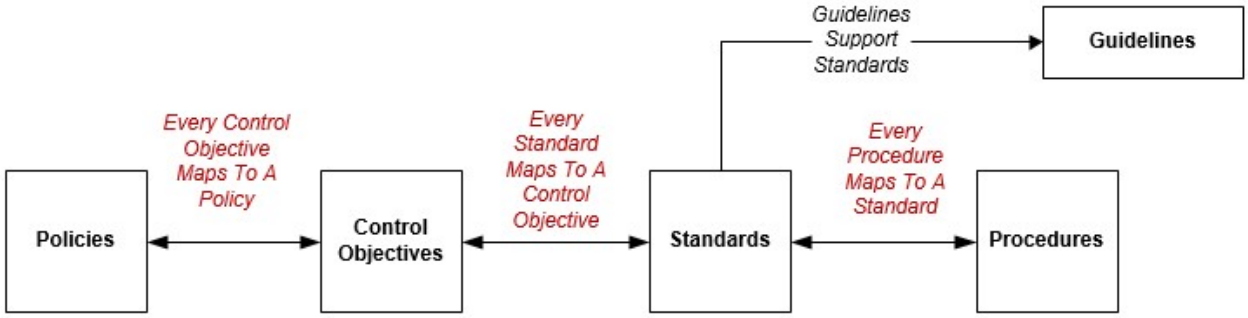
Procedures should be both clearly-written and concise. Procedure documentation is meant to provide evidence of due diligence that standards are complied with. Well-managed procedures are critical to a security program, since it represents the specific activities that must be performed to protect systems and data.

Procedures are not meant to be documented for the sake of generating paperwork - procedures are meant to satisfy a specific operational need that must be complied with:

- If procedures exist and are not tied to a standard, then management should review why the procedure is in place.
- A procedure that lack a mapping to a standard may indicate "mission creep" and represent an opportunity to reassign the work or cease performing the procedure.



From a due care and due diligence perspective, it can be thought of this way:

- Certain standards require procedures to exist *(due care – evidence demonstrates standards exist).*
- Performing the activities outlined in a procedure and documenting the work that was performed satisfies the intent of the requirement *(due diligence – evidence demonstrates the standard is operating effectively).*

HOW TO WRITE A GOOD PROCEDURE (CONTROL ACTIVITY)

Note - In many organizations, procedures are commonly referred to as "control activities" since these documented actions help provide evidence of controls being met. Procedures and control activities can be used interchangeably.

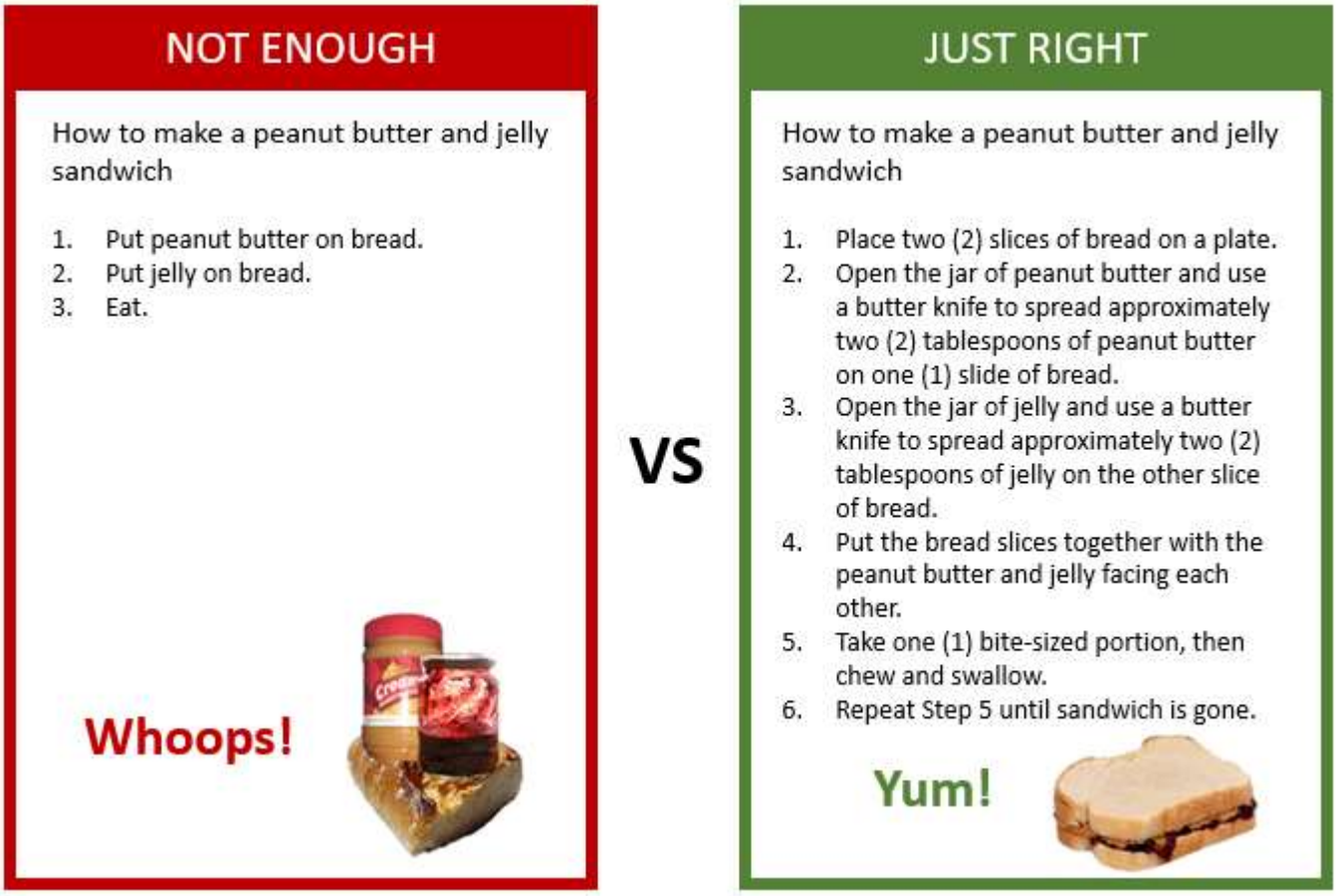
1. Be concise and clear in describing the main elements of the procedure.
2. Include at least the following elements:
    a. **Why** the procedure exists *(what requirement compels the work to be performed?)*
    b. **Who** operates the procedure *(who is actually going to do the work?)*
    c. **What** the assigned operator does *(what is the activity intended to do?)*
    d. **How** the assigned operator does it *(what are the actual steps being performed?)*
    e. **When** the procedure occurs *(what is the event trigger or frequency?)*
3. Strive to show how completely the activities of the procedure meets the control objective that it is intended to address.
    a. Good procedures have details!
    b. Keep in mind - details need to be pertinent to address the control objective.
4. The procedure needs to "stand alone" in describing how the procedure works:
    a. It should not describe surrounding processes.
    b. It should not reference other processes or documentation.
5. Use descriptive language in "present tense" grammar, as if writing a newspaper article about something occurring right now:
    a. Use verbs like "is," "does," "tests," "reviews," and "approves."
    b. Avoid verbs in "future tense" like "will do" or "will review" since the reader needs to know about "now."

NOTE - This guide is for educational purposes only. You are highly encouraged to work with a cybersecurity or audit professional to validate any compliance-related assumptions.

6. Make use of simple grammar and sentence construction:
    a. Assigned operator first (person doing the work), followed by action verb, followed by object.
    b. See example below for how a proper sentence is constructed in this context.
7. Avoid "passive voice" grammar (e.g., object before verb, "actor" missing, etc.)
    a. Example passive voice sentence: "The test plan is approved."
        i. There's no "do-er" (assigned operator) identified; and
        ii. The verb is the last two words of the sentence.
8. Describe the team's actions, not organizational structures or assertions about other teams.
    a. Example to avoid: "XYZ is some-other-team's responsibility."

How Much Detail Is Enough?

The example below shows a good amount of detail that can serve as a handy reference for writing cybersecurity procedures.



When you write procedures, focus on getting the job done – it should clearly establish the steps and concisely provide guidance to successfully complete the requirement.

NOTE - This guide is for educational purposes only. You are highly encouraged to work with a cybersecurity or audit professional to validate any compliance-related assumptions.

Procedure Mapping – Breaking Out The Requirements

- Control Objective: Only personnel who have a valid business reason are permitted access to applications, systems and resources.

- Standard: At the start of each quarter, managers review the list of team member access rights and documents issues that are not appropriate for corrective action.

- Validation of needed elements to develop the procedure:
  - Why: Addresses a quarterly requirement from the Access Control Policy to review access rights.
    - Policy #2: Access Control Policy
    - Standard #2.6.2: Periodic Review
  - Who: The team manager operates the procedure / control activity.
  - What: A periodic review is performed to ensure proper access rights are granted.
  - How: Managers review the access permissions within the XYZ application specific to his/her team members.
  - When: At the start of each quarter.

Example Procedure (How It All Comes Together)

During the first week of each quarter, ABC Team Manager shall:

1. Review ABC team member access rights during the first week of the FY quarter and document issues that are not appropriate for corrective action.
2. Using [company name]'s Governance, Risk & Compliance (GRC) tool, document the review occurred and note findings.
3. If necessary, request corrective action to address inappropriate ABC team member access to XYZ application.
4. If necessary, validate corrective action occurred to appropriately modify ABC team member access rights to XYZ application.
5. If necessary, document results of corrective action in [company name] GRC tool and notes findings. If necessary, request additional corrective action to address inappropriate ABC team member access to XYZ application.

Considerations When Scoping Procedures

Considerations for internal reviews:

- Describe checks that are carried out to validate the data produced by measurement equipment.
- Describe checks that are carried out to confirm that the information technology system is working correctly.
- Describe how maintenance and calibration records are reviewed.
- Describe how training records are reviewed.
- Describe how the measurement and reporting procedures are reviewed.
- Describe how records of corrective actions are reviewed.

Considerations for records keeping and documentation:

- Identify all documents and records related to performing operations. This might include management procedures, operating procedures, equipment specifications, equipment manuals, calibration and maintenance certificates and records, responsibilities and training records of personnel, contracts for out-sourced services, data reports and logs, fault reports.
- Describe how different versions of the documents are identified.
- Describe how current versions of documents are identified and access to outdated documents is restricted.
- Describe how documents are reviewed and updated and how new versions are authorized before use.

NOTE - This guide is for educational purposes only. You are highly encouraged to work with a cybersecurity or audit professional to validate any compliance-related assumptions.

Considerations for segregation of duties:

- Describe the responsibilities and required competencies of all personnel involved in data flow activities.
- Describe how it is ensured that only personnel with the necessary competencies carry out the relevant responsibilities for data flow activities.
- Describe how process responsibilities are segregated from control responsibilities (duties devolved to different persons).
- Describe how personnel changes are managed.

Considerations for information technology systems:

- Describe the measures undertaken to ensure that equipment is correctly installed and operated, in accordance with the manufacturer's recommendations so that it can achieve the necessary recording frequency, data storage quantity and data processing requirements.
- Describe how individual equipment items (components) are identified and recorded so that they are traceable.
- Describe measures such as backup power supplies installed to ensure security ofoperation.
- Describe measures such as data back up and off-site storage to ensure data security.
- Describe the arrangements for maintenance, including how maintenance is scheduled and recorded and how it is ensured that scheduled maintenance activities are carried out.
- Describe backup data recording and processing arrangements that can be used if the information technology system malfunctions.

NOTE - This guide is for educational purposes only. You are highly encouraged to work with a cybersecurity or audit professional to validate any compliance-related assumptions.

www.ComplianceForge.com – *Where Your Security Documentation Is Made!*