WECC

Internal Control Documentation Guidance
Frequently Asked Questions and Examples

FAQ: What is the recommended form for documenting the design of controls?

Management must carefully consider the extent of the documentation that it maintains to demonstrate the design and effectiveness of internal controls. Too much detail will result in excess documentation, which may lead to unnecessary testing of controls. Documentation of the design of controls should be detailed enough to allow a person who knows little about the process and operational risks to evaluate whether the controls are designed effectively. This level of detail allows that person to create a test plan to assess whether the controls are operating effectively and as management intends. Too little documentation will limit management's ability to convey the control processes to the organization and to monitor the effectiveness of internal controls.

Using process narratives, flowcharts, and detailed risk and control matrices are typical means to document the understanding and evaluation of controls. All three types of documentation have been used effectively for many years and in many industries.

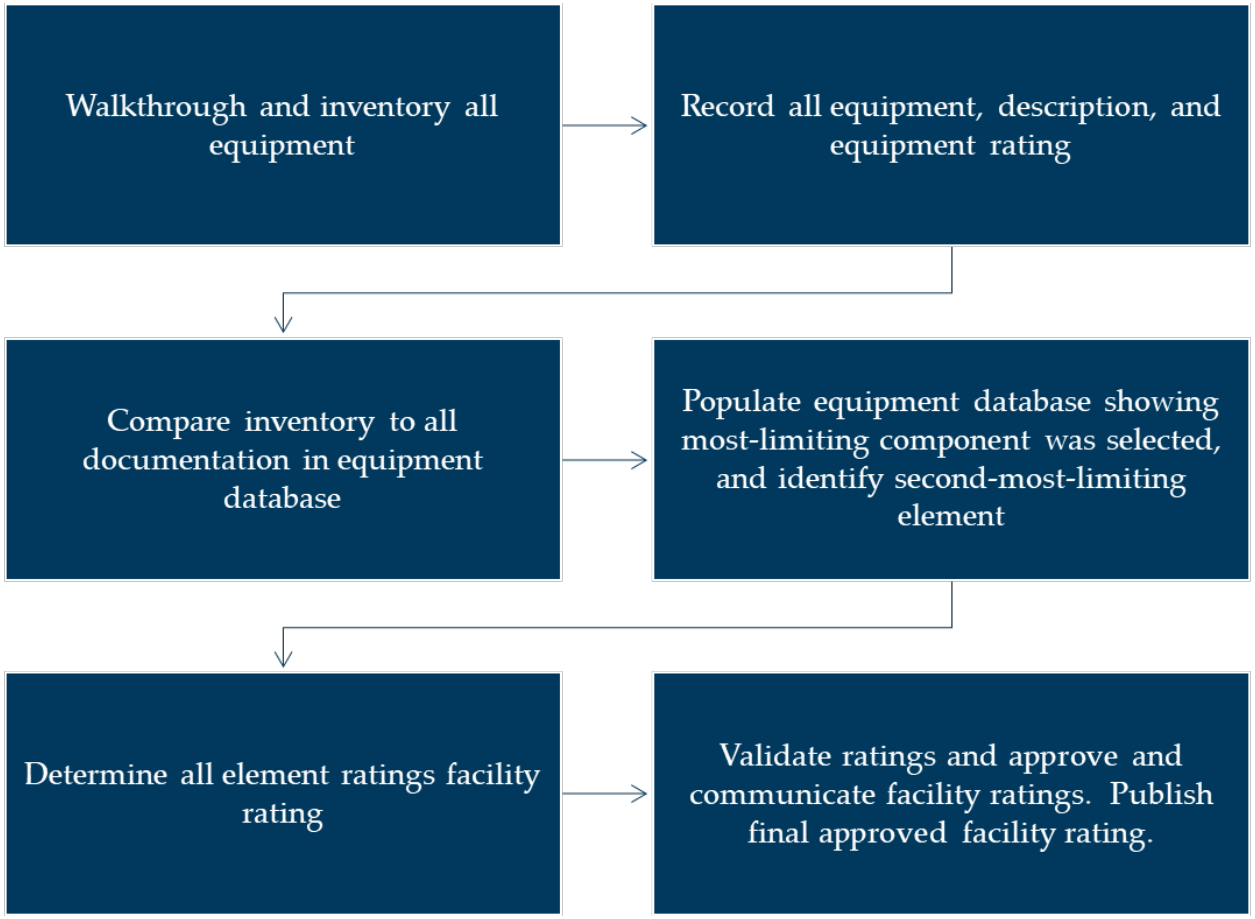
Narratives, flowcharts, and matrices are beneficial because they provide—

- A framework to ensure that all relevant and entity-specific controls that contribute to the reliability and security of the BPS are identified and documented adequately;
- A mechanism for detecting control deficiencies; and
- A mechanism for developing test plans to assess the operating effectiveness of controls.

Forms of Internal Control Documentation

- Narrative
- Flowchart
- Risk and Control Matrix

Process Flow and Narrative Example



Field Inspection—Process Narrative

Field Engineers walk down the plant and identify all elements and record all the details on a spreadsheet. Photos of nameplates are taken and filed in the equipment database. Engineering drawings are used to ensure all elements are identified and any elements not on the drawing is also documented in the spreadsheet. Once the walkdown is complete, all the data is entered from the spreadsheet into the equipment database. The rating process is used to rate all the elements and identify the most limiting and next limiting element. All this data is maintained in the equipment database. Automated processing determines the facility normal and emergency ratings. Once approved by the rating change committee, the facility rates are published and communicated to all personnel requiring this data to perform their job responsibilities. Any rate changes must follow the change control process.

Risk and Control Matrix Example

Process Subprocess	Risk	Control Objective	Description and Frequency of Control Activity	Standard Requirement Risk Category	Automated or Manual Control	Related System for Automated Control
Facility Rating	Site Facility Rating is not accurate	All elements at the site are verified against site documentation for accurate and complete site Facility Ratings information of each element	Biannually a physical site walkthrough takes place to verify elements at the site reconcile to one-line drawing details. Note: Reconciliation direction is from elements to documentation, not vice versa	FAC-008 Asset System Management and Maintenance	Manual	N/A
Physical Access	Failure to ensure the physical protection of BES assets could lead to unauthorized access	All BES cyber assets are physically protected from unauthorized access	Physical access controls limit access to sites, buildings, and rooms containing BES cyber assets	CIP-004 CIP-006 Asset System Physical Protection	Automated	ACME Physical Access Control System