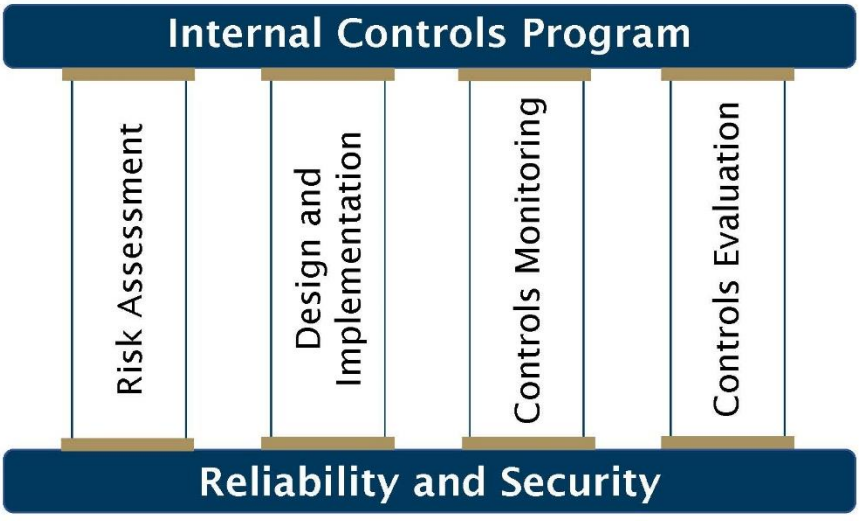
The Four Pillars of Internal Controls

An entity's system of internal control consists of policies and procedures designed to give management a reasonable assurance that the company achieves its objectives. In reference to the NERC Reliability Standards, two objectives are essential: compliance and operations.

- Compliance objective: Controls are designed and implemented to support entities' compliance (reporting) obligations.
- Operations objective: Controls are designed and implemented to achieve the reliability and security objectives of the requirement(s).

Industry groups and standards organizations have developed internal controls frameworks to help organizations manage risk. It is important for entities to understand and consider these frameworks as they develop their internal controls programs. However, entities may find that they do not need to implement all parts of these frameworks to mitigate their reliability and security risks.

When developing an internal controls program, entities should consider which parts meet their needs. At a minimum, an entity should consider how its internal controls program will: 1) assess activity and process-level risk, 2) design and implement internal controls, 3) monitor whether controls are operating as designed, and 4) evaluate control efficacy. These program elements are the four pillars of internal controls.



1—Risk Assessment

The entity should define its approach for identifying activity and process-level risk related to its business practices and governance. It is important that the risk assessment consider "first line of defense" or requirement-level risks. Identification of activity and process-level risk is a critical step in defining controls that cover the risks.

The risk assessment occurs in two steps:

1. Review the activities and processes in operation. For a requirement-level risk assessment, these are the activities your entity does to meet the reliability and security objectives of the requirement.
   a. Identify all practices.
   b. Document entity practices for use in the risk assessment process.
2. Identify potential failure scenarios that might stop you from achieving objectives.
   a. Potential failure points.
   b. Potential causes of failure points.
   c. Risk targets.
   d. Practices aligned and mapped to risks.
   e. Gaps addressed.

2—Design and Implementation

Identify, Design, Document, and Implement Controls

The entity's internal controls program should define its process to identify, document, and verify activities and processes operating within its internal control environments. This includes capturing current internal controls and developing new controls for mitigating specific risks, while addressing business and governance goals. The entity should consider controls formally laid out in process and procedure documents and ad hoc activities that informally function as controls.

The entity should define a process to assess whether the designed controls cover identified risks and whether they meet the risk targets.

Document Controls Information

Documenting controls is critical to understanding them. The entity should document attributes and details of the internal controls. Documentation should include a description of the controls, source documents that reference the control, risks mitigated, frequency of operation, responsible personnel, and control classification (such as corrective, detective, or preventative, and key or non-key). Documentation should include the "Who, What, Where, When, How, and Why" of all activities.

Communicate the Controls Design

Controls should be included in the entity's formal policy, process, and procedure documents. Including pertinent details of the controls in documents that control performers use for reference helps ensure the controls are repeatable and sustainable. Making sure control performers understand they are accountable is critical to the effective operation of a control. The entity should develop programs that teach first-line control performers how the control should operate and make them aware of their responsibility to perform the control.

3—Controls Monitoring

The entity's internal controls program should define processes for performing internal reviews and testing control performance. The entity should choose monitoring methods appropriate to the goals, complexity, and identified risks of the organization. Monitoring methods should define an appropriate frequency, scope, and placement to detect control failures. Effective monitoring creates the opportunity to detect and correct issues *before* controls fail.

4—Controls Evaluation

Because business environments change over time, controls can become ineffective or obsolete. The entity's internal controls program should define a process to assess control design and implementation to identify whether controls continue to meet risk objectives. To mitigate the risk of ineffective or obsolete controls, the entity's internal controls program should include processes to evaluate control effectiveness. These evaluations may start in response to changes in the operational and governance environments, control failures, changes in operational responsibilities, system events or compliance activities, and process improvements.

Conclusion

Entities that design their internal controls program to address the four pillars of internal controls will be able to identify and prioritize risk and develop systems of internal control that effectively mitigate risk. By implementing processes to monitor and evaluate internal controls, entities can ensure that the controls are meeting risk objectives efficiently and are responsive to the organization's changing needs.