Internal Compliance Program Self-Assessment

August 2025

An effective Internal Compliance Program (ICP) helps entities prevent and detect noncompliance and promote a culture of commitment to reliability and security. The following self-assessment is based on WECC observations during CMEP engagements. Consider these prompts when establishing and evaluating your ICP.

Effective ICPs are as diverse as the entities that adopt them. Decisions about what is appropriate for your entity will depend on many factors, including the scale and scope of your operations and your organizational structure. Each section of this self-assessment includes examples that distinguish between what may be appropriate for entities with high **(HIR)** or low **(LIR)** inherent risk and centralized **(CM)** or decentralized **(DM)** organizational models.

This document is for informational purposes only and is not a basis for enforcement determinations.

Policies and Procedures

Prompt	Examples
Do you reinforce policies and procedures with operational internal controls?	**(HIR)** Establish a change control board with oversight over operations technology resources. Adopt a charter or policy to establish and define the board's authority. **(LIR)** Assign standard owners, compliance officers, or CIP Senior Managers to provide final approval of changes affecting areas of NERC compliance.
Do you make documentation accessible and measure awareness?	**(CM)** Provide a central repository for all policies, procedures, and related documentation that is easily accessible to the appropriate staff. Include feedback mechanisms in regular training to measure awareness of the repository. **(DM)** Ensure individual business units provide easy access for staff to relevant policies, procedures, and related documentation. Require managers to provide regular training on priority knowledge and skills.

Prompt	Examples
Do you monitor vendor adherence to policies and procedures?	**(CM)** Assign compliance team to ensure authorized vendors receive appropriate access to and training on applicable policies and procedures. Perform internal audits or spot checks on identified risk areas. **(DM)** Send business unit managers or subject-matter experts to perform field visits during projects to ensure vendors adhere to safety and compliance rules specified in the scope of work.

Program Governance

Prompt	Examples
Do you document all compliance matters and follow reporting channels?	**(HIR)** Establish a dedicated governance framework accessible to all staff to support centralized tracking and resolution of reliability and security risks. **(LIR)** Use existing frameworks (safety, IT help desk, etc.) accessible to all staff to aggregate reporting for various issues to include reliability and security risks. Maintain board-level oversight of these frameworks.
Do you integrate compliance and risk management?	**(CM)** Clearly document how compliance, reliability, and security elements from organizational risk assessments support holistic understanding of their parent risks. **(DM)** Encourage standard owners to demonstrate a holistic approach to addressing corporate risk by integrating compliance, reliability, and security complications in risk assessments.
Do you ensure adequate resources, knowledge, and skills?	**(HIR)** Schedule regular compliance assessments focused not only on whether you are compliant but also (1) training efficacy and business unit knowledge retention, (2) participation in ERO Enterprise and industry work groups for knowledge sharing, and (3) documentation of identified risks or deficiencies and mitigation tracking. **(LIR)** Introduce a “learning loop” model into business unit knowledge retention processes, where two or more standard owners peer review each other’s performance, provide back-up during absences, etc.

Training and Incentives

Prompt	Examples
Do you use a risk-based approach to training?	**(HIR)** Implement a formal, curriculum-based training program for all applicable staff prior to performing in a NERC-impact role. Require periodic re-training on a rolling basis. **(LIR)** Take advantage of free or low-cost training and knowledge materials related to NERC compliance, including those provided by WECC.
Do you have a communication plan for your ICP?	**(HIR)** Host quarterly roundtables to discuss corporate performance trends, program changes, and lessons learned from near-misses and potential noncompliance. **(LIR)** Use existing channels and technology (newsletters, message boards, safety meetings, etc.) to share procedure updates and follow-up actions or changes resulting from lessons learned.
Do you measure the effectiveness and impact of training?	**(CM)** Measure human performance during regular compliance assessments to provide business units feedback on strength and maturity based on pre-defined performance indicators. **(DM)** Require standard owners to evaluate tools, products, and human performance as part of regular compliance assessment, with reference to KPIs and goals.
Do you encourage compliance through incentives?	**(HIR)** Use corporate programs to mandate performance goals or KPIs tied to organizational compliance goals and achievements. **(LIR)** Use lower-cost incentives (extra time off, gift cards, etc.) to reward individuals or groups for performance in areas with high risk of noncompliance.
Do you build incentives (and consequences) into vendor contracts?	**(CM)** Give contract administrators template language for agreements related to compliance with reliability standards. Establish end-of-contract performance bonuses or clear consequences for vendor actions which may lead to noncompliance and criteria to avoid breach of contract. **(DM)** Require business units to tailor contracts to meet specific department needs or scope of work with reliability standards or risk-based deliverables. Measure compliance-related performance with bonuses or withheld payment for milestone (non-)completion.

Investigations and Potential Noncompliance

Prompt	Examples
Do you have a reporting program or hotline?	**(HIR)** Use secure, anonymous reporting services or existing fraud, waste, and abuse hotlines for reporting potential noncompliance. Establish a documented program for how reports are received, investigated, and resolved. **(LIR)** Adopt an "open door" reporting policy with formal non-retaliation provisions to allow staff to raise concerns with any supervisor. Establish a documented program for how reports are received, investigated, and resolved.
Do you have a lessons-learned program?	**(CM)** Assign a compliance or internal audit group to identify lessons learned after investigations. Track and verify implementation by appropriate business units. **(DM)** Encourage business units or standard owners to identify and implement lessons learned from investigations, including peer checking. Empower supervisors to enact appropriate changes. Share lessons learned across business units.
Do you investigate both noncompliance and near-misses?	**(HIR)** Conduct extent-of-condition and root-cause reviews for potential noncompliance and near-misses. Document results and disseminate within the organization. **(LIR)** Define a sustainable methodology for identifying and documenting near-misses (with and without NERC impact), including peer-checking.

Continuous Improvement

Prompt	Examples
Do you audit and test internal controls?	**(CM)** Assign compliance or internal audit teams to test and measure compliance and internal controls on a rolling schedule. Verify controls for all standards and requirements at least once every three years, and high-risk requirements at least annually. Implement lessons learned as appropriate. **(DM)** Require business unit leaders or standard owners to conduct regular spot checks for the standards and requirements they are responsible for. Perform sampling equivalent to WECC audits for all requirements at least once every three years. Implement lessons learned as appropriate.

Prompt	Examples
Do you monitor the development of and integrate new standards?	**(HIR)** Encourage compliance and internal audit staff to regularly attend standard development workshops and webinars and participate in industry implementation discussions. Include compliance and internal audit staff with SMEs in noncompliance or near-miss investigations to identify opportunities to leverage corporate improvement initiatives. **(LIR)** Use lower-cost services to aggregate information and stay informed of industry changes. Adapt existing remediation to include identification of compliance-related processes and procedures.