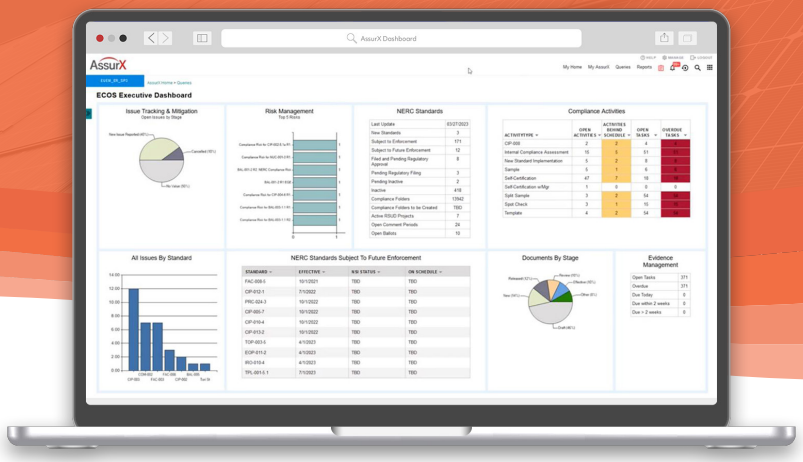
BROCHURE

AssurX ECOS

Manage NERC and regional compliance standards with risk-driven internal controls and workflows.



AssurX Enterprise Energy Compliance System (ECOS) is a system of integrated solutions that enable energy companies to meet compliance requirements for NERC O&P and CIP requirements including Regional variations and other federal and state regulations. ECOS creates an ecosystem of integrated processes that build a mature, resilient model for evidence management, assessments, issue management and mitigation.

AssurX ECOS helps manage operations, identify risk, and demonstrate compliance across all critical operations through automated workflow processes that connect compliance and risk data. Easily scales to securely manage compliance for a single department or across multi-entity organizations. Available both on-premises and the cloud.

AssurX was built to be user-configurable, does not affect the source code, and is always forward compatible. This user configurability provides AssurX customers with the flexibility required to adapt over time as business requirements change.

AssurX ECOS is uniquely designed with a high level of configurability and unmatched ease of deployment. Build integrated, precision compliance systems that rapidly adapt to change.

One Platform. Every Solution.

NERC RELIABILITY COMPLIANCE

- Automatically coordinate, track, and assess activities to ensure compliance, maintain reliability, and meet stringent NERC and Regional standards.
- Tasks are assigned, monitored, and documented in a central repository.
- Evidence, compliance narrative, and applicable policies and procedures are linked to each requirement.

NERC RELIABILITY STANDARDS UPDATE SERVICE

- The AssurX service monitors the NERC website for new or revised reliability standards, then parses the information, including PDFs and RSAWs, into AssurX-ready format so your system can be brought up to date in minutes.
- Automatically import NERC Standard, Requirement, Measure and Compliance Level data, Standard PDFs and RSAWs.

EVIDENCE MANAGEMENT

- Assign tasks, gather evidence into a central repository, associate it to the applicable regulatory requirement(s), so you can find it when you need it.
- Send notifications as tasks are due, alert supervisors of late tasks and review requests, and document regulatory submissions.

COMPLIANCE WORKFLOW AND RSAWs

- Simplify complicated activities such as audits, self-certifications, and internal compliance assessments.
- Template-driven workflows guide the activity from start to finish, assign tasks to individuals by role, and allocate due dates for each phase of the workflow to ensure that the entire activity is completed on time.
- Automated RSAW feature with auto-population of RSAW template and single-click download of an evidence package for a standard using the reviewed/approved content.

ISSUE TRACKING AND MITIGATION

- Compliance issues are documented, investigated, and supporting evidence gathered.
- Self-Reports, Mitigation Plans, and Milestones go through an internal collaboration and approval process before submitting to the Region, then tracked and managed to ensure that due dates are met, with the appropriate narratives and evidence vetted in advance of the due date.

INTERNAL CONTROLS AND RISK

- Supports Risk Assessments for NERC Requirements, identifying one or more controls to reduce the risk, evaluating the effectiveness of the controls, and seeing the calculated residual risk.
- Risk ranking is used to prioritize efforts.

PROTECTION SYSTEM MAINTENANCE

- Provides a single hub for NERC PRC standards compliance
- Gather data related to physical devices and assets affecting the BES—such as work orders, maintenance activities, test results, and supporting evidentiary documentation—from across the organization and delivering real-time status of compliance.

ASSET MANAGEMENT

- Harmonize IT and OT asset data from varying sources (integration, data import, manual entry) for convenient reporting on BES Assets, Cyber Assets, BES Cyber Systems, Electronic Security Perimeters, Physical Security Perimeters, Transient Cyber Assets, Removable Media, BCSI Designated Storage Locations, and more.
- Maintain approved asset baseline, including information on operating system, software, firmware, patches, and open ports.

ACCESS MANAGEMENT

- Manage Access Change Requests to grant, modify, or revoke user access to one or more electronic systems, physical systems, BCSI DSLs, or shared accounts.
- Monitor user personnel risk assessment and CIP training dates or integrate with the AssurX Training Management solution to provide CIP training.
- Change requests include justification for access and necessary approvals.

PATCH COMPLIANCE MANAGEMENT

- For each patch cycle or as needed, assign patch source review tasks for known software/ firmware or seamlessly integrate with a patch discovery service.
- Document the evaluation and approval of applicable security patches.
- Create and monitor mitigation plans for patches that cannot be installed within the required timeframe.
- Initiate Asset Change Management process to install the approved patch.
- Dashboards provide up-to-date status, access to relevant data, show compliance to ensure nothing is overlooked.

ASSET CHANGE MANAGEMENT

- Manage asset change activities in accordance with NERC CIP requirements
- Workflows aligned by asset type, impact rating, and type of change.
- Document the justification, approval, security controls, testing, implementation, and validation of asset changes including baseline configuration changes, onboarding assets, and retiring assets.
- Link one or more assets to the workflow for maximum efficiency.
- When used to install security patches, the record is linked to the patch information.

SUPPLY CHAIN RISK MANAGEMENT

- Track vendors and their products and services that affect the reliability of the Bulk Electric System.
- Log agreements, communication, incidents and any other related documentation.

CIP EVIDENCE REQUEST REPORTS

- Automate and centralize CIP data collection, neatly cataloging and cross-referencing the data to supply to regulators and auditors whenever requested.
- Populate the NERC CIP Evidence Request Tool (ERT) first- and second-level data requests.

Cyber security is an important and challenging undertaking in today's world, with constantly evolving technology, security measures, and cyber criminals. NERC's cyber security standards are based on the NIST cyber security framework (CSF), and become a first-line defense against cyber attack.

AssurX ECOS Features

- Dashboards enabled with Business Intelligence for real-time NERC Compliance visibility.
- Flexible and all-inclusive handling of unlimited number of processes/forms as needed.
- Integrate with additional AssurX modules to seamlessly manage audits, document control, change control and training from one system.
- Integrates with any external system – ERP, MES, SCM, Asset Management, internally developed databases, and others. Works with any reporting tools – SAP Crystal Reports, IBM Cognos, Microsoft BI, etc.
- Sophisticated access restrictions including both record level and field level and can be based on groups, departments, personalities and/or employees.
- Complete audit trail of all interaction with the system.
- Launch action plans from any point in any process. Import any data from spreadsheets or delimited files.
- Export tabular displays to CSV and archive/purge records as-needed.
- Automate unlimited processes with risk-focused internal controls that drive compliance, reliability, and efficient functioning of the enterprise.

AssurX

www.assurx.com

Want to learn more?

Connect with AssurX today.