



AESO / NERC CIP Compliance Through XQ Data Centric Governance

XQ aligns with **AESO-adopted NERC CIP requirements** by enforcing **data-centric Zero Trust controls** that operate independently of network location, cloud provider, or application layer. Below is how XQ maps to core **CIP obligations relevant to AESO-regulated entities**.

Data Protection (CIP-005, CIP-007, CIP-011)

- **Data-level encryption with customer-controlled keys** ensures BES Cyber System Information (BCSI) remains protected at rest, in use, and in transit.
- **External key management / HSM integration** prevents cloud providers, SaaS vendors, or administrators from accessing plaintext data.
- **Cryptographic separation** ensures that even if perimeter or system controls are bypassed, data remains inaccessible.

Identity, Access Control, and Least Privilege (CIP-004, CIP-007)

- **Policy-based access enforcement (RBAC/ABAC)** ties data access to identity, role, attributes, and context (e.g., geography, device posture).
- **Zero Trust access decisions are made at the data layer**, not just at the network or application layer.
- Supports **privileged access restrictions** required for BCSI and critical operational data.

Information Protection & Governance (CIP-011)

- **Granular data labeling and governance policies** allow utilities to explicitly define how BES data may be accessed, shared, or exported.
- **Persistent controls follow the data**, including backups, replicas, analytics environments, and third-party integrations.





- Enables enforcement of **data retention, sovereignty, and controlled disclosure** requirements.

Monitoring, Audit, and Incident Response (CIP-008, CIP-010)

- **Cryptographic access logs** provide immutable audit trails showing who accessed which data, when, and under what policy.
- Enables **rapid containment** by revoking keys or policies without system shutdowns or infrastructure reconfiguration.
- Supports forensic and compliance reporting required by AESO audits.

Cloud and Third-Party Risk (CIP-013)

- XQ reduces supply-chain and vendor risk by ensuring **third parties never have implicit trust or data visibility**, even when systems are integrated.
- Allows AESO-regulated entities to use cloud and SaaS platforms **without ceding control of regulated data**.

Practical Outcome for AESO-Regulated Utilities

XQ provides a **defense-in-depth control at the data layer**, complementing existing CIP network, system, and procedural controls. This helps utilities:

- Meet AESO CIP expectations for BCSI protection
- Safely adopt cloud and analytics platforms
- Reduce audit scope and blast radius
- Demonstrate enforceable, provable Zero Trust compliance





XQ ↔ AESO / NERC CIP Requirements Mapping

CIP Standard	Requirement	AESO / NERC Expectation	XQ Control	Audit Evidence Produced
CIP-004-6	R2 – Personnel Risk Assessment	Access to BES Cyber System Information limited to authorized individuals	Data access enforced via cryptographic policy bound to identity, role, and attributes (RBAC/ABAC); access revocable at key level	Access policy definitions; identity-to-policy mappings; key revocation logs
CIP-004-6	R3 – Access Management	Provisioning/deprovisioning of access to BES systems and data	Immediate access revocation via policy or key invalidation without system changes	Deprovisioning event logs; key lifecycle records
CIP-005-7	R1 – Electronic Security Perimeter	Controlled access to BES Cyber Systems	Data remains encrypted and inaccessible outside policy regardless of network boundary	Encryption policy artifacts; access attempt logs
CIP-007-6	R5 – System Access Controls	Enforce least privilege	Fine-grained, data-level access controls independent of OS or application permissions	Policy evaluation records; denied-access logs
CIP-007-6	R6 – Monitoring & Logging	Detect unauthorized access attempts	Cryptographically enforced access logging at data layer	Immutable access logs; SIEM export





CIP-008-6	R1 – Incident Response Plan	Ability to contain and respond to cyber incidents	Rapid containment by revoking data access keys or policies without shutting down systems	Incident response playbooks; revocation timestamps
CIP-010-4	R1 – Configuration Change Management	Prevent unauthorized changes to BES systems or data controls	Policies and key changes are versioned, logged, and auditable	Policy version history; change approvals
CIP-010-4	R4 – Vulnerability Assessments	Minimize exploitable attack surface	Cryptographic data isolation reduces impact of system compromise	Architecture diagrams; threat model documentation
CIP-011-3	R1 – Information Protection	Protect BES Cyber System Information from unauthorized disclosure	Persistent encryption and policy enforcement follow data across environments	Data classification rules; encryption enforcement reports
CIP-011-3	R2 – Information Disposal	Secure handling and disposal of BCSI	Cryptographic erasure via key destruction renders data unreadable	Key destruction logs; retention policies
CIP-013-2	R1 – Supply Chain Risk Management	Manage third-party access to BES data	Vendors never receive plaintext access; no implicit trust	Third-party access policies; vendor isolation proofs
CIP-013-2	R2 – Vendor Risk Controls	Control vendor-initiated access	Time-bound, policy-based access enforced at data layer	Temporary access records; expiration logs





Auditor-Relevant Positioning (AESO Context)

- XQ **does not replace** required CIP network, system, or procedural controls.
- XQ provides a **compensating and complementary data-layer control**, reducing blast radius and audit scope.
- Controls remain effective in **cloud, hybrid, SaaS, backup, and analytics environments**, which AESO increasingly scrutinizes.

How Utilities Typically Present XQ in AESO Audits

- Mapped as a **preventive and detective control** for CIP-011, CIP-004, CIP-007, and CIP-013
- Used to demonstrate **defense-in-depth** beyond perimeter security
- Supports **objective evidence** requirements through cryptographic logs and policy artifacts

