NERC CIP Standards

CIP-002 Cyber Asset Identification	Requires the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System.
CIP-003 Security Management Controls	Requires that responsible entities have minimum security management controls in place to protect Critical Cyber Assets.
CIP-004 Personnel and Training	Requires that personnel with authorized cyber or unescorted physical access to Critical Cyber Assets, including contractors and service vendors, have an appropriate level of personnel risk assessment, training, and security awareness.
CIP-005 Electronic Security Perimeters	Requires the identification and protection of the Electronic Security Perimeters inside which all Critical Cyber Assets reside, as well as all access points on the perimeter.
CIP-006 Physical Security	Addresses implementation of a physical security program for the protection of Critical Cyber Assets.
CIP-007 System Security Management	Requires responsible entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the other (non-critical) Cyber Assets within the Electronic Security Perimeters.
CIP-008 Incident Reporting and Response	Ensures the identification, classification, response, and reporting of cybersecurity incidents related to Critical Cyber Assets.
CIP-009 Recovery Plan for Critical Cyber Assets	Ensures that recovery plans are put in place for Critical Cyber Assets and that these plans follow established business continuity and disaster recovery techniques and practices.

CANAUDIT
Information Security & IT Audit Consultants