

Security Best Practices for Utilities

Comparison of Security Standards

Security standards provide a comprehensive set of controls to guide organizations on effectively protecting the confidentiality, integrity and availability of their critical data and to meet regulatory compliance. This table summarizes the three major security standards available for Utility organizations for protecting their SCADA networks, process management systems and critical infrastructures.

The most comprehensive and effective set of security standards is ISO 17799, a globally accepted standard. ISO 17799 provides guidance to Utility organizations on effectively protecting the confidentiality, integrity and availability of their SCADA networks and process management systems. The ISS ADDME(TM) (Assess, Design, Deploy, Manage and Educate) approach simply and effectively captures ISO 17799, as well as the other two standards shown here, in a five-step process.

The ISS ADDME™ approach captures ISO-17799, NERC and COSO standards in a five-step process:

- Phase 1: **Assess** the current level of information security
- Phase 2: **Design** and document policies, processes and solutions to ensure protection
- Phase 3: **Deploy** protection technology and services
- Phase 4: **Manage and Support** the security program to serve business goals
- Phase 5: **Educate** the organization on security best practices and best-of-breed technology

North American Electric Reliability Council (NERC) - Urgent Action Standard 1200	Committee of Sponsoring Organizations of the Treadway Committee (COSO)	International Standard ISO 17799
Section 1201: Cyber Security Policy	Section 1: Internal Environment- Risk Management Philosophy, Organizational Structure and Risk Culture.	Section A.3.1: Security Policy
Section 1202: Critical Security Assets	Section 2: Objective Setting	Section A.4: Information Security Infrastructure
Section 1203: Electronic Security Perimeter	Section 3: Event Identification	Section A.4.2: Information Security Infrastructure- Security of Third-Party Access
Section 1204: Electronic Access Controls	Section 4: Risk Assessment	Section A.4.3: Outsourcing
Section 1205: Physical Security Perimeter	Section 5: Risk Response	Section A.5: Asset Clarification and Control
Section 1206: Physical Access Controls	Section 6: Control Activities	Section A.6.1: Personnel Security- Security in Job Definition and Resourcing
Section 1207: Personnel	Section 7: Information and Communication	Section A.6.2: Personnel Security- User Training
Section 1208: Monitoring Physical Access	Section 8: Monitoring and Testing	Section A.6.3: Personnel Security- Responding to Security Incidents and Malfunctions
Section 1209: Monitoring Electronic Access		Section A.7: Physical Security
Section 1210: Information Protection		Section A.8.1: Communications and Operations Management- Operational Procedures and Responsibilities
Section 1211: Training		Section A.8.2: Communications and Operations Management- System Planning and Acceptance
Section 1212: Systems Management		Section A.8.3: Communications and Operations Management- Protection Against Malicious Software

**North American
Electric Reliability
Council (NERC) -
Urgent Action
Standard 1200**

**Committee of
Sponsoring
Organizations
of the Treadway
Committee (COSO)**

**International
Standard ISO 17799**

Section 1213: Test Procedures		Section A.8.4: Communications and Operations Management- Housekeeping
Section 1214: Electronic Response Incident Procedures		Section A.8.5: Communications and Operations Management- Network Management
Section 1215: Physical Incident Response Procedures		Section A.8.6: Communications and Operations Management- Media Handling and Security
		Section A.8.7: Communications and Operations Management- Exchanges of Information and Software
		Section A.9.1: Access Control- Business Requirements
		Section A.9.2: Access Control- User Access Management
		Section A.9.3: Access Control- User Responsibilities
		Section A.9.4: Access Control- Network Access Control
		Section A.9.5: Access Control- Operating System Access Control
		Section A.9.6: Access Control- Application Access Control
		Section A.9.7: Access Control- Monitoring System Access and Use
		Section A.9.8: Access Control- Mobile Computing and Telecommuting
		Section A.10.1: System Development and Maintenance-Security Requirements of Systems
		Section A.10.2: System Development and Maintenance- Security in Application Systems
		Section A.10.3: System Development and Maintenance- Cryptographic Controls
		Section A.10.4: System Development and Maintenance- Security of System Files
		Section A.10.5: System Development and Maintenance- Security in Development and Support Processes
		Section A.11: Business Continuity Management- Aspects

**The ISS ADDME™
approach captures
ISO-17799 Standards
in a five-step process:**

- Phase 1: **Assess** the current level of information security
- Phase 2: **Design** and document policies, processes and solutions to ensure protection
- Phase 3: **Deploy** protection technology and services
- Phase 4: **Manage and Support** the security program to serve business goals
- Phase 5: **Educate** the organization on security best practices and best-of-breed technology