

Security Guidelines for the Electricity Sector: Cyber — Risk Management

NERC	Guideline
Guideline Title: Cyber — Risk Management	Version: 1.0
Revision Date:	Effective Date: June 14, 2002

Purpose:

A risk management program is critical for any Information Technology and Services organization to successfully implement and maintain an acceptable level of security. This document will identify resources that are available for an IT organization to develop a risk management program to effectively identify, assess, and mitigate cyber risks to its computing infrastructure.

Applicability:

This guideline is applicable to anyone who owns and/or manages information systems and/or services that support the electric infrastructure.

A computer system environment is as critical as its most critical component and as vulnerable as its most vulnerable component. Therefore this guideline would be applicable across the enterprise.

Guideline Statement:

A successful IT risk management program is more than a simple checklist of do's and don'ts, and a handful of policies and procedures. It is a proactive, ongoing program of identifying and assessing risk, and weighting business tradeoffs on acceptable levels of risk against ever changing technologies and solutions.

Extensive documentation is available on IT risk management and conducting IT self-assessments. It is recommended that IT organizations that support the Electric Infrastructure avail themselves of this documentation in developing their own risk management program to address the following key elements^[1]:

- System Characterization
- Threat Identification
- Vulnerability Identification

¹ *Risk Management Guide for Information Technology Systems*, National Institute of Standards and Technology, Special Publication 800-30, January 2002

Security Guidelines for the Electricity Sector: Cyber — Risk Management

- Control Analysis
- Likelihood Determination
- Impact Analysis
- Risk Determination
- Control Recommendations
- Results Documentation

Risk assessment should consider the threat, system characteristics, and the physical and cyber environments in which those systems operate.

Related Documents:

- *Risk Management Guide for Information Technology Systems*, National Institute of Standards and Technology, Special Publication 800-30, January 2002
<http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf>
- *Security Self-Assessment Guide for Information Technology Systems*, National Institute of Standards and Technology, Special Publication 800-26, November 2001 <http://csrc.nist.gov/publications/nistpubs/800-26/sp800-26.pdf>
- NIST Special Publications, NIST documents of general interest to the computer security community,
<http://csrc.nist.gov/publications/nistpubs/index.html>
- *Information Security Primer*, Electric Power Research Institute, April 2001
<http://www.nerc.com/~filez/cipfiles.html>
- Security Guidelines for the Electricity Sector: Guideline Overview
- Security Guidelines for the Electricity Sector:
 - Vulnerability and Threat Assessment
 - Threat Response
 - Emergency Plans
 - Continuity of Business Processes
 - Communications

Version 1.0
June 14, 2002

Security Guideline:
Cyber — Risk Management
Page 2 of 3

Security Guidelines for the Electricity Sector: Cyber — Risk Management

- Physical Security
- Cyber Security
- Employment Background Screening
- Protecting Potentially Sensitive Information

— *An Approach to Action for the Electricity Sector, Version 1*, NERC, June 2001, <http://www.nerc.com>

— *Threat Alert Levels and Physical Response Guidelines*, NERC, November 2001, <http://www.nerc.com>

— *Threat Alert Levels and Cyber Response Guidelines*, NERC, March 2002, <http://www.nerc.com>

Revision History:

Date	Version Number	Reason/Comments