ICS Risk & Audit Methodology Project Template
SEC6084
Your Name

Table of Contents

List of Tables and Figures

Description of Industry

1. What type of industry is this?
2. What is the importance of this industry to society?

Industrial Control System Processes Employed

1. List industrial control system processes specific to industry.
2. List the control systems that control those processes and how they control those processes.
3. Create a network diagram displaying the interconnections of the industrial control system devices listed in item 3.

    a. For example: Use ICS CERT CSET, Visio, Excel, Word, etc.

Profile ICS Devices

1. For each ICS device document:
    a. Logical Ports
        For example, 80, 443, etc.
        http://www.digitalbond.com/tools/the-rack/control-system-port-list/
    b. Protocols Running
        For example, SMTP, SNMP, DNP3, Modbus, Fieldbus, Ethernet, etc.
    c. Physical Connection Types
        For example, serial, RJ45, USB, parallel, etc.
        http://www.digitalbond.com/tools/the-rack/control-system-port-list/
    d. Default Accounts:
        Research the manufacturer's information on the device. Look for default account information to login with.
        Check "Default Password List" for an entry:
        http://www.defaultpassword.com/
    e. Services
        Research manufacturer's information on the device and document services running.
    f. Authentication
        Research manufacturer's website for the device and locate information on how the device authenticates users.
    g. Use of Encryption
        Research manufacturer's website for the device and locate information about encryption. For example, does the device use encrypted connections? Is the back-end database encrypted? What type of encryption does it use? Is public/private key encryption like RSA?

h. Logging Capability

Research manufacturer's website for the device and locate information about logging. Answer questions like is logging enabled? Are logs stored locally or remotely?

i. Other Security Documentation

Does the manufacturer have any security related documentation not provided above that would be of use?

Identify Security Controls

1. Select security controls based on results from "**Industrial Control System Processes Employed" and "Profile ICS Devices"**:
Reference either ICS CERT CSET or NIST 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

Apply ICS Security Best Practices

1. NIST 800-82, Industrial Control System Security, http://csrc.nist.gov/publications/drafts/800-82r2/sp800_82_r2_draft.pdf
2. Identify unremediated risks and choose risk strategy: Accept risk, avoid risk, mitigate risk, share risk, transfer risk, combination.
Reference: NIST 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r1.pdf

Identify Vulnerability Continuous Monitoring Strategy

1. Examples:
   a. Nessus - Bandolier modules.
   b. Metasploit – ICS exploits.
   c. Snort
   d. Nmap – Identify ICS "friendly" scans.
2. Are these IA certified tools? How so?
   a. For example:
      i. NIAP: https://www.niap-ccevs.org/CCEVS_Products/pcl.cfm
      ii. Common Criteria: https://www.commoncriteriaportal.org/products/
   b. For example: Are these tools SCAP-compliant?
3. Create script rules for baselining each ICS system.
   a. For example scripts rules should audit:
      i. Installed programs.
      ii. Users, groups.
      iii. Shares.
      iv. Services.
      v. Processes.
      vi. Etc.

Reference

Appendix