AUDIT PROTOCOLS FOR INDUSTRIAL CYBER SECURITY

by Paul Baybutt
Primatech Inc.
paulb@primatech.com
614-841-9800
www.primatech.com

Abstract

Cyber security for industrial manufacturing and process control systems has not been considered in many facilities. Vulnerabilities to attack by terrorists, saboteurs, disgruntled insiders and others must be identified and measures taken to address them. This can be accomplished by performing vulnerability analysis. Alternatively, obvious weaknesses can be identified by performing a cyber security review or audit. In practice, both vulnerability analysis and audits are needed as part of a cyber security management program.

Keywords: Terrorism, cyber security, vulnerability analysis, auditing.

Introduction

Historically, cyber security has meant the protection of information stored in computer systems. However, there are broader concerns for manufacturing and process computer control systems and *industrial* cyber security should be defined as their protection from threats of:

C Cyber attack by adversaries who wish to disable or manipulate them.

C Physical attack by adversaries who wish to disable or manipulate them.

C Access by adversaries who want to obtain, corrupt, damage, destroy or prohibit access to valuable information.

Cyber support systems and utilities should also be protected. Essentially, this is a new discipline. Security vulnerability analysis (SVA) can be performed to identify flaws and weaknesses in cyber systems. However, at the present time, many control systems are not appropriately protected from cyber threats. Therefore, a suitable first step can be the performance of a cyber security review or audit. Various types of reviews, audits and inspections are needed as part of a cyber security program[1,2].

A *baseline review* is performed when a program assessment is needed to identify corrective actions required. It can be conducted at any time existing programs and practices need to be compared to best practices or new practices. *Periodic reviews* are used, often annually, to assess compliance with established requirements. Such reviews provide assurance that reasonable measures have been taken and that they are functioning. *Audits* are used to examine the design and implementation of the program to confirm compliance with established requirements and current practices. Usually, audits are performed every few years. The term “audit” is used herein to include reviews.

Audit methods and techniques are well established for safety, health, environmental, and quality audits(3,4,5), and they largely transfer over to cyber security. The key difference is in the standards against which audits are conducted and the protocols used. Unfortunately, there are no current standards for industrial cyber security, although the Instrumentation, Systems and Automation (ISA) Society is currently developing the standard ISA-SP99, Manufacturing and Control Systems Security(6), that may become a standard against which audits are performed. In the absence of standards, an audit protocol can be based on good cyber security practices and a knowledge of typical cyber vulnerabilities(7). Such a protocol is presented here. A protocol is a written document used by an auditor as a step-by-step guide in collecting information. It is a generic term that includes checklists, questionnaires and topical outlines.

Cyber Security Audits

Audits check conformance with *criteria*, or the requirements against which performance is evaluated. An audit produces *findings*, which are positive or negative conclusions based on the information collected and analyzed. A negative finding is called an *exception*. Information collected in the audit must be *verified* to confirm or substantiate the truth, accuracy, or correctness of the information by competent examination. Sometimes the information that must be examined is voluminous in which case *sampling* is used to select a portion of data to represent the full population. Both the design and implementation of the cyber security program must be audited to verify the program is properly designed, in place, and functioning effectively.

Auditors must have the proper skills and knowledge to audit effectively. This may require training. Auditors must be skilled in audit methods and knowledgeable of cyber security and computer systems. They should be impartial towards the facility being audited. Proper audit procedures and effective approaches for collecting and evaluating audit information must be used. For a small facility, a single individual may be able to conduct the audit. Larger facilities may require a team of people of an appropriate size. A management system is needed to ensure audits are conducted appropriately, particularly the follow-up on audit findings.

Preparation for a cyber security audit typically takes a few days. On-site work may take from several days up to a week or two depending on the complexity of the computer systems and the facility, the scope of the audit, and the number of auditors. A report should be prepared and this typically requires a few more days.

Audits should not be one-time studies. They must be performed periodically if they are to have lasting value. The frequency of performance depends on how rapidly the facility and cyber threats change. It may vary from once per year to once every few years. The frequency may also be influenced by the degree of facility risk and the maturity of the cyber security program. More frequent audits may be warranted for higher risk facilities and for new programs until confidence is established that they are working properly. Frequency may also be influenced by changes in the cyber security program or audit criteria, the results of prior audits, or incident history. Companies must watch out for complacency since it is easy to become convinced that all is well when that is not the case.

Audits offer various benefits in addition to a cyber security evaluation. They contribute to management control of the cyber security program and they help promote cyber security awareness.

Audit Approach

Audits follow these steps:

1. Selection
2. Preparation
3. Conduct
4. Documentation and reporting
5. Follow-up

Step 1. Selection

Computer systems to be audited must be selected. This can be accomplished using formal screening methods[8], or on the basis of perceived importance to the facility, or history of cyber attacks.

Step 2. Preparation

The purpose, scope and objectives of the audit must be defined to ensure the audit is well-focused and performed efficiently. The *purpose* is the reason the audit is being performed, for example, to comply with company policy and industry recommended practices, such as ISA SP99. Specifying the purpose helps ensure correct criteria and appropriate procedures are used. The *scope* of the audit covers the subject areas to be addressed and the boundaries of the systems. For example, it covers which policies, procedures and practices will be audited, and the depth of treatment, such as criteria detail and extent of sampling. Specification of scope helps avoid pitfalls such as misunderstandings among the auditors and management, inconsistent and inaccurate audit results, missing findings, and the inclusion of inappropriate observations. *Objectives* cover the specific systems to be audited. Defining objectives helps ensure proper coverage by the audit.

Often, a *fact sheet* is prepared. It provides basic information concerning the audit, such as the name and location of the facility audited; computer systems to be audited; names, titles, affiliations, addresses and telephone numbers of auditors, and area(s) of expertise; assignments for auditors; the date of the last audit, etc. It provides basic information the auditors need to know and may also be useful to facility management.

Auditing is often a team effort. Teams offer several benefits. They provide more than one perspective, an opportunity for discussion, and involvement of personnel with expertise in a variety of disciplines, different skills and experiences. Teams usually number 2 to 6 people depending on the size of the facility, the amount of work involved, the scope of the audit, the time period for the audit, the availability of qualified auditors, and the expertise of the auditors. Each team should have a *lead auditor* responsible for coordinating and managing the audit. The lead auditor plans and organizes the audit, coordinates with management, performs auditing, oversees meetings of auditors, performs quality control, prepares the audit report and communicates the audit results to management.

Auditors should be assigned specific tasks prior to arriving on-site and they should be informed of these assignments in advance so that they can properly prepare for the audit. These assignments are made by the lead auditor. Assignments should be made so that related parts of the audit are assigned to the same auditor and auditors should identify common areas between their assignments and coordinate with other auditors, as appropriate. Auditors should decide how they plan to use the time of the facility personnel since this is a particularly precious resource.

Auditors plan, organize and conduct the work assigned to them. They complete the parts of the audit protocol for their assigned areas and they usually assist in communicating the audit results. Ideally, auditors should not be from the facility being audited since this can lead to actual or perceived bias in the results and does not allow a fresh look at the facility. Conflicts of interest such as auditing their own, their manager's or prospective manager's work should be avoided. Auditors need to be trained or experienced in both cyber security and auditing.

Audits must be scheduled at appropriate times. Key factors in scheduling audits are the availability of facility personnel and auditors, and the need for the facility to be operating normally. Auditing during turnarounds or other plant shutdowns should be avoided.

Auditors must review background information including:

- Cyber security manual
- Relevant policies and procedures
- Applicable standards
- System architectures
- Network configurations
- Hardware and software used (operating systems, firmware, applications)
- Facility organization chart
- Facility plot plan
- Previous audit report(s)
- Action plan(s) from previous audits
- Incident reports

Auditors should identify the background information needed in advance of the audit. Reviewing it before arriving on site makes for a more efficient audit and better use of on-site time. Sometimes, an advance visit to the facility may be worthwhile to inform the facility manager and personnel about the audit purpose, scope, objectives and procedures, and to obtain facility information to aid in planning the audit. Such a visit can be made by the lead auditor alone, and is usually performed for large facilities with multiple computer systems. It can increase the overall effectiveness of the audit.

Facility personnel should be notified of the audit in advance. This can help prevent misunderstandings and anxiety during the audit. Facility management should carefully explain the purpose of the audit and emphasize that the facility wants to find any problems so they can be fixed, that personnel should not be concerned and should answer questions freely with the assurance of anonymity, that no one is looking to place blame, and that the objective is a safe and secure workplace.

An *audit plan* should be developed. This is an outline of all that needs to be done to accomplish the audit and includes:

- Policies, procedures, and other documentation to be reviewed
- Records to be sampled (e.g., training files)
- Personnel to be interviewed
- Schedule for interviews
- Sampling schemes to be used
- Protocols to be followed
- Operations the auditors will observe
- Any drills/demonstrations to be conducted

It is usually developed by the lead auditor in cooperation with the team members. Thorough preparation is necessary for a smooth-running and high quality audit.

Step 3. Conduct

Steps in conducting an audit are:

C Opening meeting
C Understanding the facility and its cyber security program
C Collecting and evaluating information
C Developing findings
C Closing meeting
C Quality Assurance

Opening meeting

The audit team meets with key facility personnel including management and other personnel involved with cyber security. The audit goals and approach are explained. It should be emphasized that the audit is not an inspection. Any special issues are discussed including facility concerns and the handling of feedback to facility personnel from auditors during the audit.

Understanding the Facility and its Cyber Security Program

The audit team must develop an understanding of how the facility and its systems are designed, operated, maintained, etc. This understanding is important to the performance of a quality audit and is developed through presentation(s) from the facility staff, a facility tour, meetings with facility personnel and a review of facility documentation. Auditors should begin to develop an initial understanding of the facility prior to arriving on site through the review of the background documentation described earlier. However, this understanding will inevitably develop further as the audit proceeds and questions arise.

The audit team must thoroughly understand the facility's cyber security program if they are to audit compliance with it. The audit team must review the program and understand both the formal and informal procedures that are used to implement it. Documentation of the program should be thoroughly reviewed by the auditors prior to the site visit. However, a complete understanding of the program procedures and their implementation can only be developed through meetings with facility personnel.

Collecting and Evaluating Information

Information is needed to understand, evaluate and validate the functioning of the cyber security program. Information usually will reside in many locations. It may not be documented but rather exist in people's heads. Various sources of information need to be explored in addition to the background information discussed earlier. They include records reviews, interviews, informal meetings, inspections, observations and demonstrations/drills.

Records Reviews: Auditors should prepare lists of the records to be reviewed in advance of the facility visit. The facility should be informed in advance that records will be examined but it should *not* be informed of the *specific* records that will be examined. Records ideally should be examined in situ, where they are actually kept, and not brought to the auditor in a conference room.

Interviews: This is a common method of information collection in an audit.
Human verbal input is critical in an audit since programs may look great on paper but may not have been put into practice. The right people must be chosen. They must have appropriate knowledge and expertise, the ability to communicate, a willingness to provide information, objectivity and reliability. The opinions of other plant personnel as to the appropriateness of selected interviewees can be sought but care should be exercised to avoid deliberate or inadvertent bias. Information collected should be assessed considering the level of knowledge or skill of the individual questioned, their objectivity, consistency of the information provided with regard to other audit information obtained, logic and reasonableness of the response. In crucial matters, reliance should not be placed on a single source of information. Additional information should be obtained from independent sources. Information generated through interviews may not be as reliable as information generated in other ways. Auditors should recognize that it is human nature to want to describe facility practices in their best possible light. Auditors may be unaware that facility personnel have blind spots or biases that could contribute to missed or inappropriate findings.

Informal meetings: Often, useful information can be obtained through casual conversations with people. These conversations can take place in the field, at the coffee pot, in the lunch room, etc. Such opportunities should not be overlooked.

Observations: These are made while auditors are working within the facility. Examples include use of procedures, password practices, etc. Observation can be a very effective information collection technique. Auditors should try to avoid alerting individuals to their observations since it may affect the way workers perform their work.

Inspections: These are typically planned in advance. Usually, they are employed to verify that specific actions have been performed or to check on conditions. Examples include checking equipment configuration and location and confirming that password policies are followed.

Demonstrations/drills: These are planned activities to show performance that may not otherwise be audited, e.g. emergency response drills. They are not commonly used for information collection.

The veracity of the information collected needs to be determined. The audit protocol should specify acceptable confirmation or verification methods such as written requests with acknowledgment, certification, verbal, observation and checks. Cross-confirmation can be used to check the consistency of information across interviews and the comparison of information from different sources, e.g. interviews versus records, interviews versus observations.

It may not be possible to examine physically every piece of relevant information or interview every participating employee since the resources may not be available. Furthermore, this is not necessary for valid conclusions to be drawn. *Samples* can be taken using accepted practices for documents, records, or people. Sampling can be judgmental or systematic, such as random, block, stratification, or interval. Samples should be selected by the auditors, not by facility personnel., and sampling schemes should be documented.

Developing Findings

Collected information is used to complete the audit protocol. Answers to protocol questions generally fall into one of these categories:

Y	Positive/acceptable as is. (Full compliance with the criteria)
N	Negative/exception. (No compliance with criteria)
I/P	Incomplete/partial. (Partial compliance with criteria)
X	Not applicable. (Criteria not applicable)
U/O	Unknown. Not observed. (Written/verbal information was not complete. Criteria not addressed)

Answers to questions are insufficient alone. Auditors must develop written findings for answers that are “negative” or “incomplete”. Auditors should discuss their findings to ensure they are supportable and to reach conclusions as to their significance. They should look for trends since these can represent systemic problems. Auditors may also develop recommendations to remedy deficiencies, but this is usually done after the audit is complete.

Auditors need to decide what information will be communicated to facility management as the audit progresses. For longer audits, auditors should brief facility management periodically on the status of the audit. Often this is done on a daily basis. Such briefings help avoid blind-siding management at the closing meeting and allow early feedback on possibly erroneous conclusions.

Closing Meeting

The auditors should meet with facility management and key personnel to communicate the findings at the conclusion of the on-site audit. The lead auditor chairs this meeting. Findings are clarified, if needed. The meeting is routine if regular feedback has been provided throughout the audit. The disposition of findings may be discussed and the schedule for a report is agreed upon.

Quality Assurance

The integrity of the audit must be assured so that the cyber security program is credible. Those being audited and those relying on the results must have confidence the audit is being carried out in a consistent, thorough and fair manner. There are numerous factors that can result in a poor quality audit. They include inadequate planning, wrong audit team members, inadequate time, key records or information not available, facility staff not available for interviews, poor auditing technique, lack of objectivity, inadequate documentation and inadequate follow-up. These factors must be managed to ensure a credible audit. As a rule of thumb, the auditors should feel confident the audit is representative of the system at the completion of the audit.

Step 4. Documentation and Reporting

Documentation accomplishes several objectives. It complies with good auditing practices, helps with follow-up on findings, provides an audit trail, aids in the communication of audit results, provides a record for future reference, and facilitates review by interested parties.

Information is usually recorded by auditors as rough notes (also known as field notes) and in prepared protocols that often take the form of columnar/tabular worksheets. Protocols have a defined structure and content. Questionnaires, topical outlines and checklists lend themselves well to the use of standard forms. Such forms can help improve the efficiency and quality of audits and are almost always used in audits. They can be completed conveniently using personal computers. An example of part of a worksheet is provided in Figure 1.

Findings must be documented and are typically included in the protocol worksheet. Recommendations may also be included. It is good practice to make an entry in the Findings column whenever a question is answered “N” or “I/P”. Entries should not be made in the Findings column for other answers. Where appropriate, “Y” answers can be substantiated with an entry in a Remarks column.

Findings should be worded carefully so as not to imply more than was found. Ideally, a reference should be added at the end of each finding identifying the basis for it. When wording recommendations, the imperative should be used carefully to avoid constraining management to a particular solution. There may be other, possibly better, alternatives. Any recommendations where the answer is “Y/X/U/O” should be entered in the Remarks column to avoid confusion. Recommendations should not just repeat the finding but rather provide any insights on the nature of the problem and additional information to address findings. Findings and recommendations need to be specific (what, where, and maybe why), complete but concise, and able to "stand alone" so they can be placed in an action tracking system. Individual findings and recommendations should not be combined to facilitate tracking them individually.

A report of the findings should also be prepared together with information about how the audit was conducted. The report should be issued promptly on completion of the audit to facilitate the initiation of corrective actions. Usually, the report is issued in draft form for review. A standard outline is often used, for example:

Executive Summary

1. Introduction
2. Purpose, Scope and Objectives
3. Audit Approach
4. Audit Findings
5. Conclusions
6. Action Plan (Optional)

Appendices

A. Description of Audit Technique
B. Audit Worksheets
C. Action Items

It is advantageous to develop an initial draft audit report on site, before the audit team splits up, since it will take longer to write the report if it is done after the team members return to their normal jobs and other responsibilities. The team leader is usually responsible for submitting the final report.

Audit reports must be distributed to appropriate parties for follow-up action, otherwise the value of the audit may be compromised. Typical recipients are facility management, the people responsible for cyber security, and affected employees. An audit report documents deficiencies and its distribution may be a sensitive issue. However, the implementation of corrective actions is not likely to occur unless the information is communicated in written form. Document control procedures should be used. Audit documentation and reports may be subject to review by company legal counsel.

Companies should have an established policy on the retention of audit reports to allow comparison with prior audits and the identification of any continuing areas of concern. The policy may call for the permanent retention of audit reports, retention for a limited time, e.g. seven years, or retention until the next audit is complete.

Step 5. Follow-up

Findings and recommendations are often categorized to help in organizing the audit results for scheduling follow-up activities. Categorization can be based on the purpose, scope and objectives of the study. Prioritization of audit findings and recommendations helps in developing an action plan to correct deficiencies. Assignments of high/medium/low or other ratings can be used.

Corrective action normally begins with a management review of the audit to determine what actions are appropriate. A written action plan should be developed promptly both to *ensure* and *demonstrate* that audit findings are being addressed. The plan should cover actions to be taken as a result of the audit findings, the schedule for implementing follow-up actions, the person responsible for each action, and a method to confirm completion of action items. If it is determined that no action is necessary as the result of an audit finding, then that should be so noted to avoid reviewers reaching the conclusion that the finding was ignored.

The action plan is normally prepared by the facility manager. Action plans should be reviewed and approved by responsible management. It can be important to provide the audit team with the opportunity to review the action plan. This review provides additional assurance that the facility correctly understands the issues identified in the audit and the action plan will get to the root causes of the issues. Copies of the action plan should be distributed to all involved parties including individuals responsible for actions to be taken, management, auditors, and affected facility staff. Employees should be briefed on the results of the audit.

The implementation of actions must be monitored using a tracking system and the action plan should be updated regularly to identify and document completed items and the status of other items. Completion of corrective actions must also be verified and documented. Management of change procedures need to be used, as appropriate. Many deficiencies can often be acted on promptly, but some may require more detailed review. Actions should be completed within a reasonable time period.

Cyber Security Audit Protocol

A protocol is provided in Table 1. It has been organized according to a variety of categories. For consistency, and a more easily understood audit, questions are phrased so that all “No” answers are exceptions.

The protocol addresses vulnerabilities, countermeasures and cyber security management. Vulnerabilities are addressed by considering connections to other computer systems, control of access, account management, physical protection and backups. Countermeasures for prevention, detection and mitigation of cyber attack are addressed. Management systems for cyber security are evaluated by considering various elements including policies and procedures, employee involvement, threat monitoring, security information, risk analysis, cyber security procedures, training, contractors, systems integrity, change management, incident reporting, response and investigation, and audits.

Companies will undoubtedly develop their own protocols tailored to their specific needs and systems. The protocol in Table 1 provides a useful starting and reference point.

Conclusions

Reviews and audits are key parts of a cyber security program. Since many facilities have not yet addressed cyber threats to their control systems, baseline reviews to identify immediate corrective actions are desirable. These should be followed by audits at regular intervals to ensure programs continue to be implemented properly and address current threats.

Endnote

Additional checklists and templates for use in the evaluation of cyber security are available from Primatech. The templates used to illustrate the technique described herein were generated using Primatech's software product AuditWorks®. Other software products or paper worksheets can also be used.

References

1. P. Baybutt, Process Security Management Systems: Protecting Plants Against Threats, Chemical Engineering, p. 48, January, 2003.

2. P. Baybutt, "Cyber Security Management Programs for Process Control Systems", to be published, 2003.

3. Guidelines for Auditing Process Safety Management Systems, Center for Chemical Process Safety, 1993.

4. J. L. Greeno, G. S. Hedstrom and M. DiBerto, Environmental Auditing: Fundamentals and Techniques, Center for Environmental Assurance, 1987.

5. K. L. Arnold, The Manager's Guide to ISO 9000, Macmillan, 1994.

6. www.isa.org

7. P. Baybutt, "Making Sense of Cyber Security", to be published, 2003.

8. P. Baybutt, "Screening Facilities for Cyber Security Risk Analysis", to be published, 2003.

Table 1. Protocol for Auditing Cyber Security

Connectivity

Are connections to other networks minimized?
Are connections to the Internet avoided?
Are wireless network access points secured?
Are dial-up modems avoided wherever possible?
Are dial-up modems appropriately secured?
Is modem use monitored?
Are dedicated connections to other computer systems avoided?

Access

Are there policies and procedures to ensure there are no unattended, unsecure workstations?
Are there policies and procedures in place to manage backdoors?
Are computer facilities located away from the facility perimeter?
Are computer facilities sited away from remote areas?

Account Management

Is there an account management program?
Does it establish levels of privilege?
Does it employ minimum necessary access privileges?
Is there an account termination procedure?
Is there an account maintenance procedure?

Physical Protection

Is suitable physical protection provided for computer systems?
Are cables and wiring appropriately protected?
Are utilities, support, telecommunications and backup systems appropriately protected?

Backups

Are there backups for electrical power?
Are there backups for communications?
Are there backups for storage?

Prevention Countermeasures

Are system default configurations changed before commissioning?
Is there a policy on home use of PCs?
Are system vulnerability checks run after installation and maintenance work?

Is there a password policy and management program?
Are other authentication methods used?
Are screen-saver passwords used?
Are application log-outs used?
Is there a patch management program?
Are systems scanned for vulnerabilities?
Are precautions taken against war dialing and war driving?
Is war dialing used to identify unsecure or rogue modems?
Is encryption used?
Is encryption strong enough?
Are e-gaps or air gaps used?
Are modems secured?
Are wireless access points secured?
Are honeypots used?
Are precautions taken against sniffing?
Are precautions taken against spoofing?
Are firewalls used?
Is firewall activity audited?
Are DMZs used with bastion hosts?
Are VPNs used?
Are applications limited?
Are ports restricted on network devices?
Are maintenance operations secured?
Are countermeasures effective?
Are they maintained?

Detection Countermeasures

Are intrusion detection systems used?
Is there real time response to intrusion alarms?
Is IDS activity audited?
Is anti-malware used?
Is it updated regularly?

Mitigation Countermeasures

Is there an incident response program?
Is there an incident investigation program?
Is there a data recovery program?

Cyber Security Management System

Do cyber security policies and procedures exist?
Are they followed?
Are they revised as needed?

Are roles defined and responsibilities assigned?
Is authority provided?
Is supervision provided?
Are resources allocated?
Are people held accountable?

Employee Awareness, Education and Involvement

Is there security awareness training?
Does it cover:
S password practices?
S social engineering?
S document security practices?
S use of anti-malware?
Are reminders provided?
Is there regular refresher training?
Are contractors included?

Cyber Threat Monitoring

Does the facility stay abreast of new cyber threats?
Is there a patch management program?

Facility and System Information

Does the facility maintain a low profile?
Is information on company web sites controlled?
Are company newsletters, press releases, and articles screened for security violations?
Is sensitive trash shredded or incinerated?
Is computer equipment sent for sale or disposal sanitized?
Is access to sensitive information suitably controlled?
Do vendors control access to hardware and software design and operation information?
Is the public disclosure of information limited to what is absolutely necessary?
Is key information kept up-to-date?
Is there backup storage of electronic media?

Cyber Security Risk Analysis (CSRA)

Has a CSRA been performed?
Did it address relevant cyber threats?
Does it reflect the system as actually configured and operated?
Have recommendations from the CSRA been implemented?
Is it updated periodically?

Cyber Security Procedures

Are there written cyber security procedures?
Do they include procedures for:
S Personnel screening
S Information protection
S Document control
S Computer access
S Disposal of sensitive information
S Sanitization of storage media
Are they complete?
Are they written properly?
Are they followed?
Do they have a standard format and content?
Are they readily accessible by the people who need to use them?
Are procedures dated as needed?
Were affected personnel involved in their preparation?
Are old procedures purged?

Cyber Security Training

Are affected employees trained in cyber security matters, as appropriate?
Does training cover:
S Security awareness
S Security procedures
Are contractors included?
Is refresher training provided at appropriate intervals?

Contractors

Are the impacts of using contractors addressed?
Are subcontractors included?
Are contractor cyber security practices audited?
Is contractor access to computer systems controlled and limited?

Cyber Security Systems Integrity

Are cyber security systems properly designed, installed, operated, maintained, inspected and tested?
Are appropriate systems included?
Does it include support systems, backup systems and utilities?
Does it cover both cyber and physical protection?
Does the cyber security program address procedures, employee training, and quality assurance?
Are security-critical systems defined?

Cyber Management of Change

Are the possible security impacts of changes in the system and process considered in a management of change program?
Have types of change covered by cyber MOC been defined?
Are all pertinent changes reviewed?
Is a suitable method(s) used to evaluate the impact of changes on cyber security?

Cyber Security Incident Reporting and Investigation

Is there an incident reporting and investigation policy and procedure?
Are suspicious events and breaches of the cyber security program reported and investigated?
Are applicable corrective actions taken?

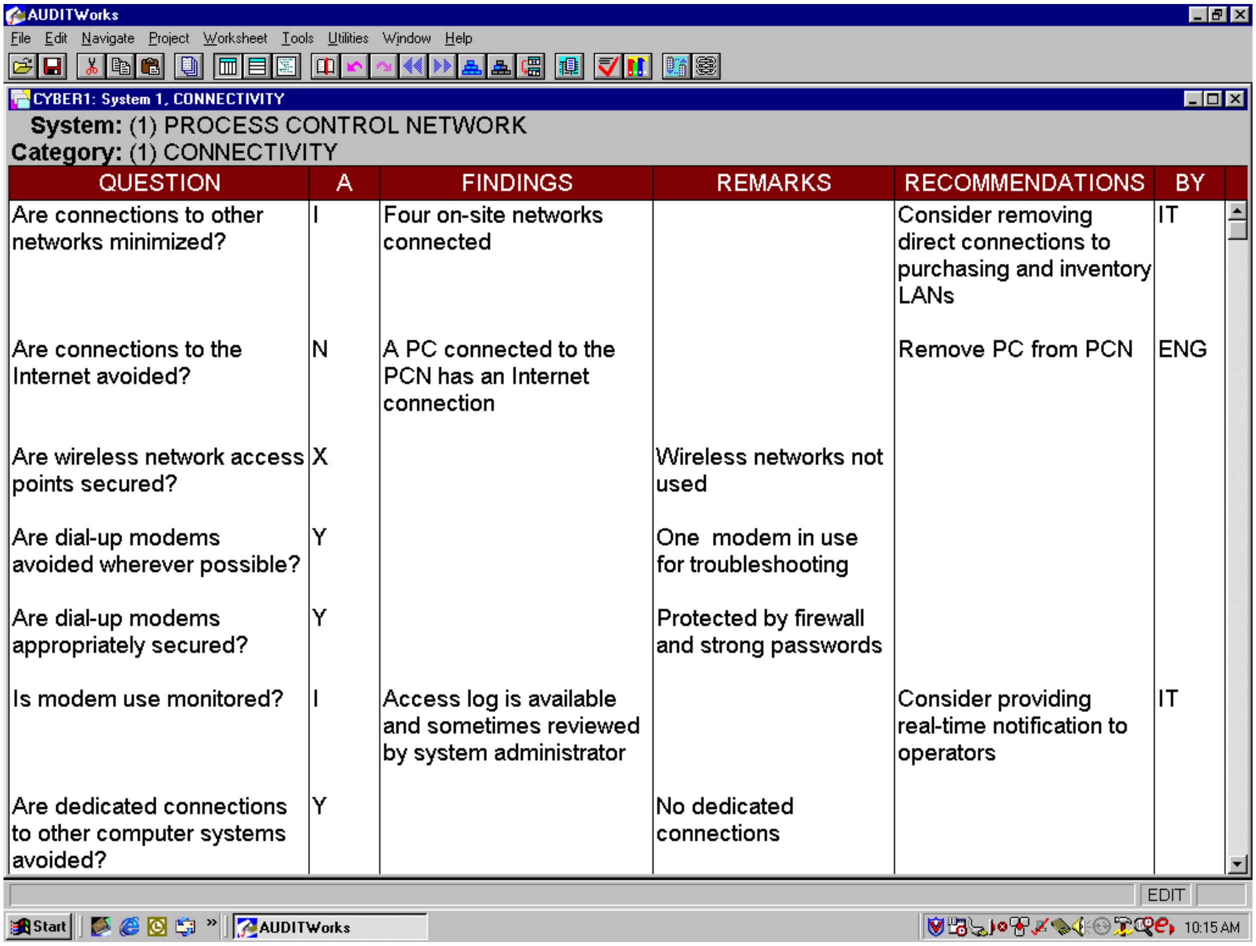
Cyber Security Incident Response

Is there a written response plan?
Has it been tested?
Is there a response team?
Are team members appropriately trained?
Is there coordination with law enforcement and Federal agencies?
Are there emergency backups for support systems and utilities?

Cyber Security Audits

Are periodic audits conducted?
Do they follow an acceptable procedure?
Is the audit protocol complete?
Is it applied properly?
Are the results documented?
Are corrective actions taken?

Figure 1. Example of a Cyber Security Audit Worksheet.


AUDITWorks
File Edit Navigate Project Worksheet Tools Utilities Window Help
CYBER1: System 1, CONNECTIVITY
EDIT
Start
AUDITWorks
10:15 AM

System: (1) PROCESS CONTROL NETWORK
Category: (1) CONNECTIVITY

QUESTION	A	FINDINGS	REMARKS	RECOMMENDATIONS	BY
Are connections to other networks minimized?	I	Four on-site networks connected		Consider removing direct connections to purchasing and inventory LANs	IT
Are connections to the Internet avoided?	N	A PC connected to the PCN has an Internet connection		Remove PC from PCN	ENG
Are wireless network access points secured?	X		Wireless networks not used		
Are dial-up modems avoided wherever possible?	Y		One modem in use for troubleshooting		
Are dial-up modems appropriately secured?	Y		Protected by firewall and strong passwords		
Is modem use monitored?	I	Access log is available and sometimes reviewed by system administrator		Consider providing real-time notification to operators	IT
Are dedicated connections to other computer systems avoided?	Y		No dedicated connections		