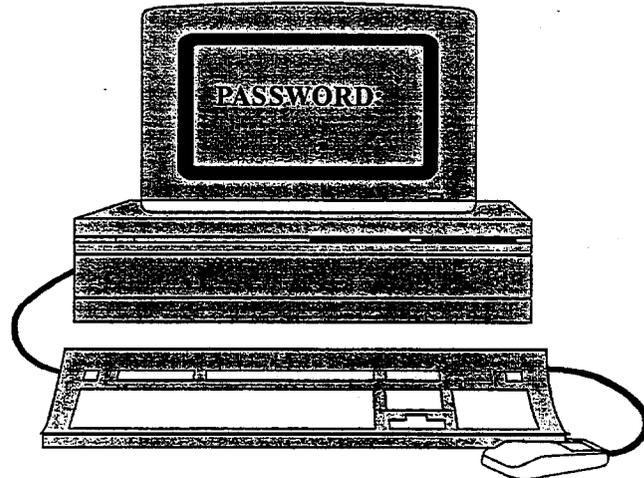


U.S. ARMY ARMOR CENTER AND FORT KNOX



INFORMATION SYSTEMS SECURITY PROGRAM

Prepared by

Security Division

G3/Directorate of Plans

Training, and Mobilization

Fort Knox, Kentucky 40121-5000

HOME OF MOUNTED WARFARE

Headquarters
U.S. Army Armor Center and Fort Knox
Fort Knox, Kentucky 40121-5000
14 July 1995

* USAARMC Pamphlet 380-19

Security

INFORMATION SYSTEMS SECURITY

Summary. This pamphlet is published by the Security Division, G3/Directorate of Plans, Training, and Mobilization (G3/DPTM) as a reference to security for information systems that process classified and unclassified information. It provides techniques that should be considered when data is processed on an information system. These guidelines are presented for consideration and appropriate application, keeping in mind that each operating environment is different. This pamphlet may be tailored by your activity Information System Security Coordinator (ISSC) to address the specific needs and procedures of your activity. Please note that information system security policies, procedures, and safeguards must be cost effective, practical, and must not impede efficient operation. AR 380-19, 1 Aug 90, Information Systems Security, is the primary publication for information security.

Applicability. The procedures outlined in this pamphlet are applicable to all units and activities assigned to USAARMC and Fort Knox.

Suggested improvements. The proponent of this pamphlet is the Security Division, G3/DPTM. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) to Commander, U.S. Army Armor Center and Fort Knox, ATTN: ATZK-PTF-I.

CONTENTS	PAGE
1. Introduction.....	2
2. Minimum Requirements.....	2
3. Physical/Environmental Security.....	3
4. Personnel Security/Training.....	5
5. Information Security.....	5
6. Communications Security.....	8
7. Software Security.....	8
8. Emergency Procedures.....	8
9. Prevention of System Misuse.....	8
10. Environmental Considerations.....	8
11. Conclusion.....	9

Appendix A - References

Appendix B - SOP for Information Systems

Appendix C - Accreditation Format for Information Systems

Appendix D - Risk Management Review

*This pamphlet supersedes USAARMC Pamphlet 380-1, 23 November 1988.

1. Introduction. In recent years, there has been a significant increase in the use of Information Systems in the workplace. Regulatory security requirements for information systems are covered in AR 380-19, which establishes the responsibilities to protect classified and unclassified sensitive data from unauthorized access, disclosure, alteration, destruction, or misuse.

a. It is evident in today's information age that the key to protecting data, hardware, and software is for users and managers to develop a security mindset. We must recognize that information is a critical resource of any organization.

b. When microcomputers and word processors first came into use, they were used by individuals in connection with their jobs, but only for their own sphere of needs -- ancillary tools. If something negative happened to the equipment or data, it was a personal crisis affecting only one individual. Today, the data in an information system could represent the entire activity and/or installation and is critically important.

c. This document establishes security guidelines for the use of information systems. The procedures contained in the pamphlet provide guidance in protecting hardware, software, and information. The responsibility for this protection extends directly to the end user.

d. Information systems security must be approached with three objectives in mind. They are: (1) CONFIDENTIALITY of classified, personal, proprietary, or otherwise sensitive data handled by the system; (2) INTEGRITY and ACCURACY of data and the processes that handle the data; and (3) AVAILABILITY of systems and data or services to the functions they support.

2. Minimum Requirements. All information systems processing classified or unclassified sensitive information will achieve the following minimum requirements:

a. Accountability. Safeguards will be in place to ensure that persons having access to an information system will be held accountable for their actions on the system. All systems except small stand-alone computers will provide an audit trail to provide a documented history of system usage.

b. Access. Each system will have an access control policy. Each user will be positively identified before authorizing access.

c. Security training and awareness. All persons accessing an information system will receive initial computer security awareness training and periodic/recurring training at least annually.

d. Physical Controls. Information systems hardware, software, documentation, and all classified and unclassified-sensitive data processed by the system will be protected to prevent unauthorized disclosure, destruction, or modification.

e. Marking. Markings on classified and unclassified-sensitive output will reflect the sensitivity of the information as required by existing directives.

f. Least privilege. The system will function so that each user has access to all the information required, but no more.

g. Data continuity. An owner will be identified for each file or data grouping on the system.

h. Data integrity. Safeguards will be in place to detect inadvertent or malicious modification or destruction of data.

i. Contingency planning. A plan will be developed so that if data is lost, recovery procedures are available. (Backup routines).

j. Accreditation. Accreditation is the formal process granting approval to operate an information system in a given security mode using a prescribed set of safeguards. Each system will be accredited under a set of security safeguards approved by the Designated Approval Authority (DAA). An accreditation format is at appendix C.

k. Risk Management. A risk management program will be in place to determine the level of protection required, how much exists, and the most economical way of providing the needed protection.

l. Security Planning. An information system security plan will be developed and maintained for the life of the system. The security plan becomes the accreditation document.

3. Physical/Environmental Security. When an information system is assigned to an individual, the individual becomes responsible for the system. It is the individual's responsibility to protect the system and its data. The following protective safeguards must be implemented to prevent loss from natural hazards, fire, theft, and malicious acts.

a. When the system is not attended, lock buildings and/or rooms where the hardware is located. If this is not possible,

purchase commercially available physical restraining devices or a local alarm. Implement an end-of-duty-hours security check using SF 701 (Activity Security Checklist).

b. Know everyone who has routine access to the area.

c. Supervise the use and maintenance of information systems.

d. Ensure there is a fire protection system (fixed or portable) within the building or room housing information systems. All personnel must be familiar with fire emergency procedures and equipment. In most instances, your existing unit or activity fire emergency plan is sufficient. Incorporate information systems into the plan.

e. Implement an inventory system so all equipment and software is accounted for at least once a month. Each component will be permanently marked by engraving the unique identifier S50KX and the last five digits of the equipment serial number on the right or left side of a permanent or semi-permanent part of the equipment.

f. If equipment or software is stolen, immediately report the theft to the proper authority in your organization.

g. Smoke can damage disks. Food and ashes that are dropped on the keyboard can work down under and around the keys, causing them to malfunction and resulting in expensive repairs, as well as loss of equipment use. If liquids are spilled on the hardware or removable media (tapes, disks, diskettes), irreparable damage can occur to the equipment. Smoking, eating, and drinking must be prohibited in the immediate vicinity of information systems.

h. Never use unauthorized software. Use only trusted and proven software provided by your Information Management Officer. Approved software must be listed in the accreditation document. Do not bring software from your home. Do not copy licensed software packages or use copies someone else has made. Computer software is protected by Title 17 of the U.S. Code. Violating copyright agreements is illegal and is punishable fines of up to \$20,000 per violation and possible criminal prosecution with a maximum penalty of 5 years imprisonment.

i. Information systems that have nonremovable media upon which classified files reside must be stored in an area or container approved for safekeeping of classified information per AR 380-5.

j. Diskettes and other media should be stored in closed, locked containers to protect them from contaminants, unauthorized access, disclosure, damage, modification, or destruction.

k. Approved virus detection software will be installed and operational on information systems. Computer viruses are a major threat to our information systems. It is imperative that any media brought into your activity/organization be scanned for viruses before use.

4. Personnel Security/Training. All personnel within your organization or work area will probably not have the authority to access the same data. To ensure the information and systems requiring protection are not accessed by unauthorized individuals, you can:

a. Ensure the person wishing to access your system is approved to do so by your Information Systems Security Officer (ISSO) or an authorized designee. Your organization must have a security clearance system and screening procedure to ensure that people with access to systems and data are trustworthy. The individual requesting access to your system should be authorized to do so only after a preemployment screening, local records check, and appropriate security investigation has been completed.

b. You must ensure the individuals accessing your system are properly trained so that they understand the criticality of protecting the system and data as well as system usage. The Information System Security Officer should give the individuals a copy of these guidelines and they are required to read them.

c. Section VI, AR 380-19, addresses the Personnel Security Standards required for sensitive ADP positions. Additional guidance for personnel managing, supervising, and occupying ADP I, II, III positions are found in AR 380-67, chapter 9.

5. Information Security. Classified and unclassified sensitive information processed on information systems must be protected from unauthorized access, disclosure, and destruction. The following procedures can be used to minimize the possibility of these occurrences.

a. Use of passwords. User identification and password systems support the minimum requirements of accountability, access control, least privilege, and data integrity. The ISSO oversees generation, issuance, and control of passwords. This control includes keeping a copy of the password in a sealed envelop to prevent loss. After generation, passwords will be handled and stored at the level of the most sensitive data contained in the system.

b. Storage Media. The storage media containing your data must be removed from the system when it is not in use in all systems. The storage media must be protected as specified in paragraph 5g(2) below. Due to the large number of systems in many organizations,

it is unrealistic to expect each user to go to the ISSO for a randomly generated password to protect each of the data files. The users can create their own data-file passwords, but sequential numbers should be avoided (i.e., 123456) to preclude compromise. Other names to avoid are birthdates, user's name, spouse's name, child's name, address, etc. In this case, the user should select random letters or numbers for a password.

c. Protection of Passwords. If another individual demonstrates a work-related need to access your password-protected data file, you should make a backup copy of your data file (without password) and instruct that person to create their own password to protect their copy of the data file. That person should also be instructed in all procedures to adequately protect the information in the file. Passwords should not be posted on terminals, blackboards, bulletin boards, etc. Place them in a sealed envelope and keep them in a locked depository (file cabinet, safe, etc.).

d. Protection of Information Displayed on Terminal Screen. In an ideal situation terminals should be positioned to minimize unauthorized viewing of the screen. This can be accomplished by facing the screen away from doorways and windows. The ability to blank the screen should be sufficient when unauthorized individuals (persons without authorized access, security clearance or need-to-know) enter the work area. Also, dividers and partitions work well.

e. Protection of Information Transferred from a Mainframe Computer. Information systems may enable a person to transfer or download data from a mainframe computer to their work area. You must be sure to protect the transferred information. If information is transferred to a mainframe computer, it must also be protected. The responsibility for the security of sensitive data shifts from the computer center to the user after the data has been transferred.

f. Protection of Hardcopy Material. Original source material, whether handwritten notes or hardcopy output, should be handled the same as disks (see paragraph 5g(2) below). When printing information, protect the information from unauthorized individuals by attending the printer, closing the door, and/or facing the printer away from doorways so the output cannot be read by the passerby. Protect electronically generated data in the same manner you would protect any other hardcopy data.

g. Protection and Handling of Disks, Diskettes, and Tapes.

(1) Labeling of Storage Media. Disks, diskettes, and or tapes must be labeled according to their classification or

sensitivity (i.e., Secret, For Official Use Only, etc.). Series 700 Forms should be used for exterior labeling of media.

(2) Storage. Diskettes are fragile. To ensure your recorded data is reliable, take care of the diskettes when they are out of storage to prevent them from becoming damaged. Do not place diskettes on terminals, in books, under terminals or printers, use as a coaster for a drink, or toss loosely in a drawer. Natural skin oils can damage magnetic media, handle the diskettes only by their covers. Follow the manufacturers directions on the care and storage of media and keep diskettes in their containers when not in use. Media must be protected from inadvertent erasure. Avoid placing media near any magnetic source such as telephones, radios, tape recorders, or speakers of any kind. When unattended, storage media will be secured according to its classification and or sensitivity to prevent unauthorized access, disclosure, damage, modification, or destruction. Establish a filing system to account for storage media. Never lend diskettes to unauthorized individuals.

(3) Disposing of Storage Media. Don't throw disks, diskettes, and/or tapes (when they are no longer needed) into regular waste containers. They should be rendered useless through degaussing or shredding. Classified storage media must be protected according to AR 380-5 unless properly declassified or destroyed. Both shredders and a degausser are available for use at Security Division, G3/DPTM.

(4) Backups of Storage Media. Backup copies of important data should be created regularly, and stored away from your work area. Remember that backup copies of data must be protected in the same manner as the original data.

(5) Ribbons. Information system printer ribbons must be controlled and destroyed according to AR 380-5, paragraph 5-201c.

(6) Clearing the system of information. Because systems have residual memory, you must clear the memory after processing information. If this is not accomplished, anyone can use the equipment and read your data. The following procedures can be used to clear a system's memory.

(a) Remove all removable storage media.

(b) Power off the unit to clear any volatile memory (memory that is lost when power to the unit is off).

(c) Power the unit back on and proceed with the next job,
or

(d) Overwrite the portion of the permanent storage area with random patterns. Utilities programs are used to do this.

6. Communications Security. When transmitting information over unprotected communication lines there is an inherent risk of the information being intercepted. Classified information will be transmitted only by secure means. Protection of unclassified -sensitive information during transmission will be consistent with the risk of disclosure, loss, misuse, alteration, destruction, or nonavailability. National Security Agency approved encryption equipment that can either transmit or store data in encoded form is available and must be utilized as appropriate.

7. Software Security. To protect you and your organization from liability for copying or disclosing proprietary data, learn what restrictions exist. Commercial software is licensed and rights are reserved. Federal copyright laws must be adhered to. Individuals will be held accountable for illegal activity.

8. Emergency Procedures. To minimize the loss of both the system and data during an emergency (fire, earthquake, etc.) you should shut off the system and remove it to safety, if it is practical. To ensure that critical data and software programs are not lost during an emergency, backup copies should be made and stored in a separate area, away from the system. Contingency plans must be developed to limit the adverse effects of emergencies where equipment and information may be lost.

9. Prevention of System Misuse. Government systems are to be used only for official purposes. The information processed on a government system is subject to audits. If you have knowledge (or a suspicion) of someone misusing a system, you should report the incident to the proper authorities in your organization.

10. Environmental Consideration. Information systems are sensitive to the quality of electrical power. Avoid using electrical circuits that power heavy appliances and other office equipment. Power off systems during thunderstorm activity. The use of surge protectors/backup-power supplies is highly encouraged.

a. Electronic equipment can be affected by temperature. Be aware of the temperature operating range of your equipment and ensure your office temperature remains within that range.

b. Media can be affected by temperatures below 25 degrees Fahrenheit and above 125 degrees Fahrenheit. Never place media in direct sunlight or on radiators or heaters.

c. Work areas should be kept clean and free of dust.

11. Conclusion. Our installation has many different missions and environments. All of these environments are dependent on information systems. This document may be tailored by your activities ISSC/ISSO to address the specific needs and procedures in your activity. This document is intended to help users understand and implement information systems security responsibilities. If you have any questions, discuss them with your ISSC/ISSO.

FOR THE COMMANDER:



OFFICIAL:
JACK SKIDMORE
Colonel, GS
Chief of Staff

ROBERT L. BROOKS
Director, Information Management

DISTRIBUTION:
B plus
50 - ATZK-PTF-I less
CDR, USAREC

CF:
DCG, USAARMC

APPENDIX A

REFERENCES

Public Law 100-235, The Computer Security Act of 1987

AR 380-19, 1 Aug 90, Information Systems Security

AR 380-5, 25 Feb 88, Department of the Army Information Security Program

AR 380-67, 9 Sep 88, Department of the Army Personnel Security Program

AR 530-1, 1 May 91, Operations Security

AR 190-51, 30 Sep 93, Security of Unclassified Army Property (Sensitive and Nonsensitive)

AR 190-13, 30 Sep 93, The Army Physical Security Program

AR 340-21, 5 Jul 85, The Army Privacy Program

APPENDIX B

INFORMATION SYSTEM SECURITY STANDING OPERATING PROCEDURE (SOP)

1. Applicability. (State who the SOP applies to.)
2. Objectives. (State what the SOP is intended to accomplish.)
3. System. (Identify the system to which the SOP applies.)
4. Sensitivity. (State the highest level classification of information that may be processed on the system.)
5. Physical Security. (Briefly state the requirements for securing the equipment when left unattended and the key control procedures. Require an end-of-duty-hours security inspection utilizing SF 701.)
6. Environmental Security. (State location and type of emergency fire fighting equipment and responsibility for use. Advise against smoking, drinking, and eating at or near the system(s). Advise about locating system(s) near windows, doors, indirect sunlight, etc. Establish housekeeping functions and assign responsibilities for accomplishment. State actions to be taken in the event of electrical storm and power outages.)
7. Access Controls. (Establish a list of authorized users, attach a copy to the SOP, and post a copy on or near the system(s). If passwords are used, state system for which used files authorized to access for each user. Establish guidelines for sharing data. Explicitly state prohibition for use of equipment for other than official business and copying software as well as use of other than government-tested proven, purchased software. Assign responsibility for controlling access.)
8. Personnel Security. (State personnel security requirements of personnel. State procedures for screening and verifying eligibility.)
9. Software Security. (State requirements for securing software when not in use. State backup requirements and procedures. Indicate marking requirements and procedures. Allow zero tolerance of software copyright violations.)
10. Protection of Output. (Specify measures for marking, securing, and distributing output.)

11. Use of Antivirus Software. (State requirements for installation, updating with current versions, and establish procedures for distribution.)

12. Communications Security. (If the system communicates within network or other system, state procedures for protecting the data communications and procedures for disabling communications link when used in the stand-alone mode.) All classified data that is transmitted must be encrypted. Sensitive data that is transmitted must be encrypted or the requirement to be encrypted must be waived by the accreditation authority.

Signature and
Signature Block

APPENDIX C

SECURITY PLAN/ACCREDITATION DOCUMENT FORMAT

The format in this appendix is to be used as an outline when preparing accreditation documentation. Each paragraph of the format must be addressed with the exception of accreditation for small computers. The asterisk (*) at the beginning of the paragraph indicates this requirement is optional. The degree of detail required in each paragraph can and should vary with the system's size, complexity, sensitivity designation, mode of operation, and number of users. If a system processes SCI, WNINTEL data, or Special ACCESS Programs for Intelligence (SAPI) and is being accredited or reaccredited, all documentation must comply with DoDIIS Site Based Accreditation requirements using the guidance provided in DIAM 50-4 and AR 380-19.

Office Symbol (MARKS #)

Date

MEMORANDUM THRU (If applicable)

FOR G3/DPTM, Security Division, ATTN: ATZK-PTF-I, Fort Knox,
Kentucky

1. SUBJECT: Request for Accreditation (See AR 380-19, appendix C.)
2. List basic system information and identification as follows:
 - a. System name or title. (Make, model, and serial number may be used for the CPUs if the system has no name or title.)
 - b. System category. (Indicate whether or not the system(s) is a general AIS support system or has a specific application; for example, intelligence, personnel, financial, and so forth.)
 - c. Type accreditation. (Indicate whether or not this is a generic or operational accreditation. For operational accreditation, indicate whether or not a single identifiable system or a group of similar systems are covered.)
 - d. System status. (Indicate either "developmental" or "operational" as appropriate.)
 - e. System overview. (Provide a description of the function and purpose of the system.)

f. System Environment and special considerations. (Describe physical, operational, or other factors external to the system which affect its security. Describe system interfaces to other systems or networks.)

g. Information contacts. (List, as a minimum, the name and telephone number of the appointed ISSO.)

h. System identification. (The system(s) must be identified in the accreditation in a manner sufficient to determine which system(s) are governed by the particular accreditation. For operational accreditations, this will be done through a serial number listing of the CPUs of the AIS accredited or through another means that clearly defines the systems accredited. A separate enclosure may be used. For generic accreditations, use military nomenclature, a common accepted system acronym, or other method determined by the DAA.)

i. *Near and long-term goals. (Describe near-and long-term goals of the system and the contribution of this accreditation to accomplishing these goals.)

3. Sensitivity, Protection Requirements, Security Mode, and Minimum Trusted Class.

a. Sensitivity designation. (List the sensitivity designation of the system(s). Describe, in general terms, the nature of the information and the reason it requires protection. Cite appropriate laws requiring protection, such as the Privacy Act, if applicable.)

b. Protection Requirements. (Indicate whether the system protection requirements are based on the need for confidentiality, integrity or availability of the information. For each of these categories, indicate whether they are of primary, secondary, or no concern. There may be more than one primary concern designated. For example, confidentiality and integrity may be primary concerns and availability of information of no concern.)

c. Security mode of operation. (Indicate the security mode of operation from AR 380-19, para 2-2.)

d. Minimum trusted class. (Enter the required minimum trusted system class as determined from AR 380-19, appendix B. Include any applicable information regarding the use of approved NSA products.)

4. Risk Management review. (See appendix D). Include in this section a risk management review which includes an examination of

threats, vulnerabilities, and the resulting risks according to AR 380-19, chapter 5. In the next paragraph indicate the selected countermeasures that result in acceptable risk.)

5. Implementation of controls and countermeasures. (Include a description of measures taken in the areas of personnel, physical, environmental, procedural, hardware, software, TEMPEST, and communications security.)

6. *Certification. (Describe the certification testing which was accomplished to support the accreditation. Attach the certification plan for generic accreditations. For operational accreditations, attach a certification plan or describe the certification process in this paragraph. For dedicated mode, the certification will focus on the physical, procedural, and personnel security measures that ensure all users have the appropriate clearance, access approval, and need-to-know for all data on the system. Since the system is not required to separate users and data with technical security measures, the certification effort will not be extensive.)

7. Facility information. (As with all documentation associated with accreditation, the facility information should be tailored to the size, criticality, mode of operation, data sensitivity, and number of users for the AIS.) The following paragraphs will be addressed in compiling facility information:

a. Facility identification and location.

b. *Architectural drawings or building plans. (Plans of the building housing the facility should show the location of exits, guard posts, fire alarms and hoses, master utility panels, and facilities adjacent to, above and below the facility.)

c. *Facility floor plan. (The floor plan will show placement of all equipment, fire extinguishers and sprinklers, smoke and motion detectors, emergency lighting and so forth.)

d. *System interface description. (Include a diagram or a description of interfaces for all major equipment, processing units, terminals, peripherals, communications modems, controllers, concentrators, encryption devices, and other connections.)

e. *Other diagrams. (If applicable, diagrams will show specialized displays of communication, electrical wiring, special communication switching, or patching panels.)

f. *Operating system. (List the release or level number and date first put into operation on the system.)

8. *Network considerations. (This section should address the network's capability to provide communication integrity, protection against denial of service, and compromise protection. See AR 380-19, para 2-23.)

9. Attachments. (This section is not applicable while the document is serving as the security plan, however, when used as an accreditation document and forwarded to the Designated Approval Authority, the below items should be attached as applicable.)

a. Users Security Manual/SOP. (This is a mandatory and extremely critical item for generic accreditations. Recommended for operational accreditations although such procedures may be incorporated in other documents.)

b. FTA/RA to include the INSCOM review or the Commander/DAA statement if required by AR 380-19-1 (C).

c. Appointment orders for the ISSO or NSO, as applicable.

d. Approved waivers (for example, COMSEC waivers approved per AR 380-19, chapter 4, TEMPEST waivers approved per AR 380-19-1 (C), trusted computer class waivers approved per AR 380-19, para 2-3, and so forth.)

e. *Certification plan.

f. Security Classification Guide.

g. Contingency Plan.

APPENDIX D

RISK MANAGEMENT REVIEW

1. PURPOSE. The purpose of the Risk Management Review is to conduct a detailed analysis of the Risk Management program. Management must identify the resources to be protected and analyze the actual or potential risk of espionage, sabotage, damage, and theft to determine the minimum level of protection needed. Risk Analysis is used to justify the expenditure of resources as well as to determine the most cost effective safeguards.

2. OBJECTIVES. The objective of risk management is to achieve the most effective safeguards against deliberate or inadvertent--

- a. Unauthorized disclosure of information.
- b. Denial of service or use.
- c. Unauthorized manipulation of information.
- d. Unauthorized use.

3. METHODOLOGY.

a. Four steps are utilized to conduct a Risk Management Review. They are:

(1) Risk Assessment, as derived from an analysis of threats and vulnerabilities.

(2) Management Decision, to implement security countermeasures and to accept residual risk.

(3) Implementation of Countermeasures.

(4) Effectiveness Review.

b. Each phase should be applied to the areas of software, hardware, procedures, communications, emanations, personnel (the highest risk), information, and physical security. In addition, relative risks within each area should be analyzed.

c. Risk assessment involves estimating loss potential that exist as the result of threats and vulnerabilities.

4. Threat agents are identified as:

a. Man-made/natural Disasters:

- (1) Fire
- (2) Water
- (3) Tornado
- (4) Earthquake
- (5) Flood
- (6) Lightning
- (7) Windstorm
- (8) Dirty Power

b. External Threats:

- (1) Theft of equipment
- (2) Unauthorized use of data
- (3) Fraud
- (4) Theft of data
- (5) Destruction of equipment
- (6) Dirty data
- (7) Foreign intelligence services

c. Internal Threats:

- (1) Theft of equipment
- (2) Unauthorized use of data
- (3) Fraud, waste, and abuse
- (4) Theft of data
- (5) Destruction of equipment
- (6) Dirty data

d. An overt or covert realization of a threat could result in:

- (1) Unauthorized disclosure of information.
- (2) Denial of service or use.
- (3) Unauthorized manipulation of information.
- (4) Unauthorized use.

5. Vulnerability. System vulnerability is defined as the total range of susceptibilities to all threats. General factors to be considered include-- geographical location, classification of data in the AIS versus security clearance of users, sensitivity and amount of material being handled, and overall criticality of the mission or operation.

a. Fire. Information systems are vulnerable to fire and could result in loss of service or use.

b. Water. Information systems are vulnerable to water damage and could result in loss of service or use.

c. Tornado. Information systems are vulnerable to tornados and could result in loss of service or use by destruction of equipment.

d. Earthquake. Information systems are vulnerable to earthquakes and could result in loss of service or use by destruction of equipment.

e. Flood. Information systems are vulnerable to flooding and could result in loss of service or use.

f. Lightning. Information systems are vulnerable to lightning and could result in loss of service or use by destruction of equipment and loss of information.

g. Windstorm. Information systems are vulnerable to windstorms and could result in loss of service or use by destruction of equipment.

h. Dirty Power. Information systems are vulnerable to dirty power and could result in loss of service or use by destruction of equipment and loss of information.

i. Theft of Equipment/Data. Information systems are vulnerable to theft of equipment and data and could result in loss of service or use, unauthorized use of data, fraud, and theft.

6. The following matrix is included as an example format of a risk management review.

a. VULNERABILITY RISK

<u>Threat</u>	<u>Analysis</u>	<u>Assessment</u>	<u>Countermeasure</u>
Fluctuation of voltage	Probability of power surge is likely.	This could cause damage to equipment and loss of data.	The system is protected by a UPS.
Loss of commercial electrical power	Probability is likely	This could cause loss of data being edited when loss of power occurs.	Periodical backing up of files.

<u>Threat</u>	<u>Analysis</u>	<u>Assessment</u>	<u>Countermeasure</u>
Flooding of the facility	Probability of flooding is unlikely.	Flooding would cause damage to equipment and disruption of	System is in a building near crest of a hill and on the second floor.
Intruder on site with intent to gain access to classified information/destroy equipment.	(As appropriate)	(As appropriate)	(As appropriate)
Terrorist attack	(As appropriate)	(As appropriate)	(As appropriate)
Fire	(As appropriate)	(As appropriate)	(As appropriate)
Tornado	(As appropriate)	(As appropriate)	(As appropriate)

LIST ANY OTHER THREATS

b. PERSONNEL SECURITY: All personnel having access to the computer system have a favorably adjudicated security clearance at the appropriate level. All personnel have received automation security training. (List other appropriate measures).

c. HARDWARE SECURITY: System is kept under key lock during nonduty hours. (List other appropriate measures).

d. SOFTWARE SECURITY: Only approved and legal software will be used. (List other appropriate measures).

e. EMANATION SECURITY: (If required list appropriate measures).

f. COMMUNICATIONS SECURITY: (List appropriate measures).

g. PROCEDURAL SECURITY: (List appropriate measures).

h. INFORMATION SECURITY: (List appropriate measures).