Department of the Army Pamphlet 25–1–2

Information Management:

Information Technology Contingency Planning

Headquarters
Department of the Army
Washington, DC
6 June 2012

UNCLASSIFIED

SUMMARY of CHANGE

DA PAM 25–1–2
Information Technology Contingency Planning

This major revision, dated 6 June 2012--

- Establishes and addresses information relating to systems requiring an information technology contingency plan and identifies information technology contingency plan baseline requirements as defined by either the Department of Defense or by Federal statute (para 1-6).

- Identifies the information technology contingency plan coordinator as the suggested ultimate responsible party for planning, creating, maintaining, and training of the information technology contingency plan (para 1-7).

- Creates a Roles chapter to help delineate possible roles for information technology contingency planning (chap 2).

- Assigns responsibilities and gives authority to the information technology contingency plan coordinator to take necessary actions for maintaining operational information systems (para 2-4).

- Consolidates multiple chapters from the previous version to create a consolidated chapter 3 that better defines the information technology contingency plan planning process (chap 3).

- Utilizes the format of the Army five-paragraph operations order and operations plan to redefine information technology contingency plan (para 4-1).

- Establishes the reference and suggested use of FM 5-0, FM 5-19, and AR 525-26 (app A).

- Utilizes only the terms information technology contingency plan and information technology contingency plan coordinator for information technology contingency plans (throughout).

- Updates the information technology contingency plan and explains its relationship to the continuity of operations plan (throughout).

- Makes administrative changes (throughout).

Headquarters
Department of the Army
Washington, DC
6 June 2012

***Department of the Army Pamphlet 25–1–2**

Information Management:

Information Technology Contingency Planning

By Order of the Secretary of the Army:

RAYMOND T. ODIERNO
General, United States Army
Chief of Staff

Official:

JOYCE E. MORROW
Administrative Assistant to the Secretary of the Army

History. This publication is a major revision.

Summary. This pamphlet provides procedures for developing and exercising Information Technology Contingency Plans. This pamphlet supports AR 25–1 in implementing Title 10, United States Code, and Section 1401, Title 40, United States Code (Public Law 104–106, the Clinger-Cohen Act, formerly Division E, Technology Management Reform Act). Procedures for operational security and the development of emergency relocation groups are covered in other publications and are not included in this publication.

Applicability. This pamphlet applies to the active Army, the Army National Guard/Army National Guard of the United States, and the U.S. Army Reserve, unless otherwise stated. This pamphlet also applies to non-tactical command, control, communications, and computers/information technology at all Army installations, activities, and communities.

Proponent and exception authority. The proponent of this pamphlet is the Chief Information Officer/G–6. The proponent has the authority to approve exceptions or waivers to this pamphlet that are consistent with controlling law and regulations. The proponent may delegate this approval authority, in writing, to a division chief within the proponent agency or its direct reporting unit or field operating agency, in the grade of colonel or the civilian equivalent. Activities may request a waiver to this pamphlet by providing justification that includes a full analysis of the expected benefits and must include formal review by the activity's senior legal officer. All waiver requests will be endorsed by the commander or senior leader of the requesting activity and forwarded through their higher headquarters to the policy proponent. Refer to AR 25–30 for specific guidance.

Suggested improvements. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to Chief Information Officer/G–6, Chief Information Officer Policy Division (SAIS–GKP), 107 Army Pentagon, Washington, DC 20310–0107.

Distribution. This pamphlet is available in electronic media only and is intended for command levels C, D, and E for the active Army, the Army National Guard/ Army National Guard of the United States, and the U.S. Army Reserve.

Contents (Listed by paragraph and page number)

*This pamphlet supersedes DA Pam 25–1–2, dated 16 November 2006.

UNCLASSIFIED

Contents—Continued

Table List

Contents—Continued

Figure List

Glossary

Chapter 1
Information Technology Contingency Planning

1–1. Purpose

This pamphlet provides operational procedures and practical guidance for information technology (IT) contingency planning to support Army organizations developing, using, or maintaining non-tactical IT services, products, and support. IT contingency planning includes general support systems and information technology contingency plans (ITCPs) for major applications and support systems. Strategy plans for the Land Warrior Network (LandWarNet) will have a major impact on the development of IT contingency planning as Armywide strategy transitions from many loosely affiliated independent networks into a truly global capability that is designed, deployed, and managed as a single integrated enterprise. The primary focus of this document is the implementation of policies mandated by AR 25–1, AR 25–2, AR 500–3, AR 70–1, Department of Defense Instruction (DODI) 8500.2, Department of Defense Directive (DODD) 3020.26, and Department of Defense (DOD) Memorandum dated 2 May 2009, LandWarNet - Global Network Enterprise Construct Strategy Implementation. This document follows the guidelines in DODI 3020.42; DOD Memorandum - Federal Information Security Management Act (FISMA) Guidance - Fiscal Year (FY) 08; National Institute for Standards and Technology (NIST) Special Publication (SP) 800–34; NIST SP 800–53; NIST 800–18; and Federal Information Processing Standards (FIPS) Publication 199. Its emphasis is on identifying and describing implementing procedures, explicit and implied, stemming from DOD policies and Federal authorities, to include the Clinger-Cohen Act; Title 40, United States Code, Chapter 111 (40 USC 111); 40 USC 3; the FISMA - 2002 (Title III of Public Law 107–347, the E–Government Act of 2002); Federal Continuity Directive 1; the National Defense Authorization Act for FY 2000: Information Assurance (IA) Initiative; 10 USC 2224; and Office of Management and Budget Circular A–130.

1–2. References

Required and related publications are listed in appendix A.

1–3. Explanation of abbreviations and terms

Abbreviations and special terms used in this publication are explained in the glossary.

1–4. Exceptions

This pamphlet does not address operations security, the development of emergency relocation groups, or continuity of operations (COOP), which are covered by AR 500–3.

1–5. Continuity of Operations Plan

An ITCP provides procedures and capabilities for recovering and sustaining an IT system, capability or application. An ITCP is a critical part of a COOP plan, but it is not a COOP plan. An ITCP can be enacted without enacting a COOP plan. A COOP, as stated in AR 500–3, is the degree or level in which there is a continuous commitment in the conduct of functions, tasks, or duties that are necessary to accomplish a military action or mission in carrying out national military strategy. A COOP plan is a set of policies, plans, procedures, and capabilities that addresses the subset of an organization's missions that are deemed most critical, it is usually written at the headquarters level, and it is not IT-focused. The requirements for an ITCP are regulated by one of three mission assurance category (MAC) levels (see DODI 8500.2 for MAC level details) and one of three confidentiality levels as set forth by AR 25–2 and AR 25–1 on Army Portfolio Management Solution - Army IT Registry (APMS–AITR) registration requirements. The MAC level is used to determine the IA controls for integrity and availability in accordance with DODI 8500.2. The confidentiality level identifies the classification or sensitivity of the information associated with the system. The confidentiality level is used to establish acceptable access factors and to determine the DODI 8500.2 IA controls applicable to the information system (IS). Additional information on ISs can be found in FIPS Publication 199. In this document, IT platforms or IT systems are considered to be any major application or general support system; the term IT will be used for both within this publication.

1–6. Support

The ITCP program supports the President, the Secretary of Defense, the Chairman of the Joint Chiefs of Staff, Department of the Army organizations, and other DOD components. This pamphlet also supports managers and those individuals responsible for IT system continuity at the system and operational levels. This description includes the following personnel:

a. The designated ITCP coordinator as defined in the AR 25–2 and ITCP coordinators designated by the commander.

b. Managers responsible for overseeing IT operations or business processes that rely on specified IT systems.

c. System administrators responsible for maintaining daily IT operations.

d. IA managers, IA security officers and other staff responsible for developing, implementing, and maintaining an organization's IT security activities.

e. System engineers and architects responsible for designing, implementing, or modifying ISs.

f. Users who employ ISs, such as desktop and portable systems, to perform their assigned job functions.

g. Other personnel responsible for designing, managing, operating, maintaining, or using ISs.

1–7. Required information systems

a. Any IS capability or application assigned a MAC level, in accordance with AR 25–2, requires an ITCP. Program managers (PMs) and program executive officers (PEOs) should use the security categorizations described in FIPS Publication 199 whenever there is a Federal requirement to provide such a categorization of information or IS.

b. DOD MAC level I is the most stringent of all requirements. If your system is compliant with DOD MAC level I, then it is compliant with Federal standards in accordance with DODI 8500.2. Refer to http://www.dtic.mil for more details on MAC levels.

c. Each category level establishes the baseline requirements for either the DOD or Federal IT contingency planning. The guidelines will serve as a baseline checklist for personnel tasked with IT contingency planning. The most important baseline requirement is the frequency of ITCP testing.

d. To be compliant with Federal law, system owners (SOs) are responsible for registering the system in APMS and ensuring a contingency plan is developed and tested at least once a year, with the exception of MAC level I, which must be tested twice a year. If the system is fielded to multiple locations, the SO must coordinate with the system administrators at each location and the system administrators must implement and extend the ITCP as appropriate for that location, whether it is at the organizational level or installation level. After the completion of the test, there are two fields listed below that are mandatory for the SOs to complete and record in the APMS–AITR. For more information regarding APMS–AITR refer to DA Pam 25–1–1; and Army IT Portfolio Management Guidance, March 2008; or APMS Fundamentals, located on Army Knowledge Online (AKO) https://www.us.army.mil. Completion of the two data fields below shall comply with DOD IT Portfolio Repository reporting standards.

(1) *Contingency plan.* This field indicates if a contingency plan is in place to account for disruptions in the operation of this system. It is a mandatory DOD IT portfolio repository data element for all systems.

(2) *Contingency test date.* This field indicates the last date the ITCP was exercised. It is a mandatory DOD IT portfolio repository data element for all systems with an ITCP.

1–8. General information technology contingency planning and requirements

a. An ITCP is a living document and also requires a long-term planning strategy and program management plan. The planning process is to outline how the organization will designate resources, define short and long term ITCP goals and objectives, forecast budgetary requirements, anticipate and address issues and potential obstacles, discuss mission essential functions (MEFs) and establish planning milestones. A well defined IT portfolio management and evaluation methodology is essential for assessing ITCP as related to the existing baseline enterprise architecture. A lack of understanding of how the ITCP relates to the enterprise architecture will result in a lack of funding and effort needed to implement effective and efficient approaches of crisis restoration across the IT enterprise and the inability of the Army to provide and plan for ITCP funding, IA, hardware and software applications and for staffing during crisis management scenario operations.

b. IT contingency planning is a command responsibility. Commanders are integral in the establishment of a fully incorporated ITCP. A commander's lack of attention to planning would bring about a loss of funding or inability to operate. Commanders must set policies that are clear and designate a single ITCP point of contact (POC) who will then be the ITCP coordinator (see para 2–4).

c. IT contingency planning should:

(1) Be addressed throughout the system development life cycle (see para 3–1).

(2) Establish a sole ITCP coordinator with the responsibility for planning and ITCP (see para 2–4).

(3) Identify and prioritize MEFs (see paras 3–8, 3–9, and 3–10).

(4) Establish baseline category requirements (see para 1–6).

(5) Address risk management and mitigation (see para 3–4).

(6) Establish system backup procedures (see para 3–8).

(7) Create a Federally compliant ITCP (see chap 4).

(8) Address plan testing, training and reporting (see para 3–13).

(9) Address how ITCP requirements will be incorporated into daily operations (see paras 3–6*j* and 3–8).

(10) Address how the ITCP relates to other disaster and emergency plans (see chaps 3 and 4).

(11) Evaluate the system to link these critical services to system resources (see para 2–4).

d. All mission critical (MC), mission essential (ME), and mission support IT systems that are fielded, as well as all the MC/ME IT systems in development, that is, all acquisition category I through III programs, must be recorded in APMS, per AR 25–1, and must be registered with the Army Chief Information Officer (CIO)/G–6 and the DOD CIO

per AR 70–1. Any IS supporting a MEF should, by definition, be one of the above. Information on the requirements for survivability of MC/ME systems can be obtained in AR 70–75.

Chapter 2
Roles in Planning for Information Contingencies

2–1. Commanders
ITCP is a command responsibility. Commanders are integral in the establishment of a fully incorporated ITCP. If a commander does not set a clear policy statement granting a singular POC the responsibility of ITCP development, testing of the ITCP, and IT contingency planning, then the ability to establish a functional and authoritative ITCP is hindered.

2–2. Program executive officers and program managers
The PEOs and PMs have the same role as stated in AR 25–1. IT contingency planning is a life cycle development process that is most effective when implemented in the development and configuration management stages. If PEOs and PMs take the necessary steps to develop and maintain the baseline for the system and routinely validate with stakeholders that the system is meeting all critical requirements.

2–3. System owner
The SO is the Government civilian, military person, or organization responsible for introduction or operation of any IT used by or in support of the Army. The SO is responsible for ensuring the security of the IT system as long as it remains in Army inventory, or until transferred (temporarily or permanently) to another Government person or organization and such transfer is appropriately documented and provided as an artifact to the accreditation package. If a contractor provides IA services to a system with the intent of meeting some or all of the SOs IA responsibilities, the IA responsibilities do not shift from the Government SO to the contractor. The Government SO remains responsible for ensuring that the IA services are provided. The Government SO may charge the IA manager with authority to perform many of the SO IA duties, if appropriate; however, final responsibility will remain with the SO. The SO could be a product, program or project manager, a staff or command element that purchases or develops IT equipment and systems, a network enterprise center (NEC), or any other entity that is responsible for an IT system. The SO is responsible for ensuring that all IA requirements are identified and included in the design, acquisition, installation, operation, maintenance, upgrade or replacement of all Department of the Army IT system in accordance with DODD 8500.1.

2–4. Network enterprise center and information technology contingency plan coordinators
Designated by the commander as the primary ITCP POC, the ITCP coordinator, who may be located at the NEC, is responsible for overseeing all aspects of IT contingency planning. However, if another individual is appointed the POC outside the NEC, then he or she may hold authority over the NEC and is then responsible for the installation's ITCPs. Regardless of whether the ITCP coordinator is located within the NEC, the ITCP coordinator has the authority to take independent action when necessary to maintain operational information systems and should—

a. Operate as the ITCP POC as coordinated and managed under the Army COOP program.

b. With the involvement of functional users and tenets, identify all organizational functions.

c. Maintain a copy of all of the installation's current service agreements and contract numbers with their vital records.

d. Support or conduct a business impact analysis (BIA) (see para 3–5). Although in general the ITCP coordinator should:

(1) Identify and coordinate with internal and external POCs associated with the system to characterize the ways they depend on or support the IT system. When identifying contacts, it is important to include organizations that provide or receive data from the system as well as contacts supporting interconnected systems. This coordination should enable the system manager to characterize the full range of support provided by the system, including security, managerial, technical, and operational requirements.

(2) Evaluate the system to link these critical services to system resources. This analysis will usually identify infrastructure requirements such as electric power, telecommunications connections, and environmental controls. Specific IT equipment, such as routers, application servers, and authentication servers are usually considered critical. However, the analysis may determine that certain IT components, such as a printer or print server, are not needed to support critical services.

(3) Determine the optimal point to recover IT systems.

(4) Develop and prioritize recovery strategies to be implemented during ITCP activation.

e. In coordination with the COOP site manager, develop a plan to test the ITCPs. Refer to paragraph 3–12 for guidance on ITCP testing and training.

f. Coordinate with Network Enterprise Technology Command or other IT support providers as required and engage in quarterly communications exercises with supported tenants and IT support elements.

g. Maintain a copy of the ITCPs associated systems and a list of those to whom the plan was distributed.

h. Communicate changes in the ITCP to representatives of associated plans or programs, as necessary, and record plan modifications.

i. Coordinate frequently with associated internal and external organizations and system POCs to stay aware of necessary changes to the ITCP based on changes to systems and requirements.

j. Refer to AR 380–5 for information pertaining to the protection of information stored at the site of a contingency situation.

k. Evaluate supporting information to ensure the information is current and meets system requirements.

l. Make and publish changes to the plan in a format that will prevent unofficial or unapproved changes to the plan.

m. Activate the ITCP if any activation criterion is met.

n. Select an appropriate recovery strategy upon activation of the plan.

o. Determine how often media should be backed up.

p. Select appropriate disk replication techniques and products.

q. Assess the robustness and reliability within their core networks.

2–5. System users

System users are those organizations or personnel which utilize a portion of an information system, capability, or application.

2–6. Continuity of operations site managers

COOP site managers are those personnel prescribed to such duties as defined in AR 500–3. These site managers are a wealth of resources for anyone planning to write or revise an ITCP or COOP and they can provide the ITCP coordinator the contact information and contract lists necessary to complete a fully functioning ITCP. This is because a COOP plan will incorporate its own ITCP and much of the information contained within that plan can be utilized by any ITCP coordinator. They can specifically help with:

a. Discussing emergency internet connectivity with the local data service center and developing procedures for Tier 1 and 2 help desk support to ensure the required level of quality of service will be met. Refer to paragraph 3–14 for more information on IT contingency planning at the installation level.

b. Determining testing requirements and, if necessary, scheduling a test in coordination with the ITCP coordinator.

c. Coordinating with the ITCP coordinator to develop a test plan designed to test the selected element(s) of the ITCP against explicit test objectives and success criteria.

2–7. Contingency response team

In general a contingency response team is comprised of personnel who have been trained and are proficient at the assigned task or are subject matter experts for specific plan operations within the organization. The response team can evaluate effects of changes to ITCPs and should always be prepared to perform contingency measures to restore system functions. Army users can also coordinate with a regional computer emergency response team, which serves as the Army Computer Emergency Response Team's regional focal point for conducting computer network defense in support of Army information assurance to ensure the availability, integrity, and confidentiality of the information and information systems used by theater commanders. Refer to https://www.rcert-s.army.mil for more information.

2–8. Risk management team

The risk management team includes representatives of management, user departments, and the IA department. They carry out the tenets of the risk management program as prescribed in FM 5–19.

2–9. Other possible information technology contingency plan teams

Other possible teams who will help carry out the duties of the ITCP coordinator to successfully plan and activate an ITCP are listed below. These are not required and are only suggested to help the ITCP coordinator accomplish his or her task. Furthermore, this list is not meant to be comprehensive. If the ITCP coordinator needs other teams, he or she should create them as needed.

a. Management team.

b. Damage assessment team.

c. Operating system administration team.

d. Systems software team.

e. Server recovery team (for example, client server, Web server).

f. Local area network (LAN)/wide area network (WAN) recovery team.

g. Database recovery team.

h. Network operations recovery team.
i. Application recovery team(s).
j. Telecommunications team.
k. Hardware salvage team.
l. Alternate site recovery coordination team.
m. Original site restoration/salvage coordination team.
n. Test team.
o. Administrative support team.
p. Transportation and relocation team.
q. Media relations team.
r. Legal affairs team.
s. Physical or personnel security team.
t. Procurement team.
u. Risk management team.

Chapter 3
Information Technology Contingency Planning Guidance

The Army ITCP program assures that the capability exists to continue MEFs across the full spectrum of emergencies and prepares Army organizations for any contingency that potentially interrupts normal operations. Developing flexible ITCPs and procedures for as many events as possible has become the new norm for the Army. Coinciding with Army COOP, Army ITCPs should be event-neutral and consider capabilities, connectivity, and procedures that would provide Army organizations and leadership with the ability to ensure their MEFs continue to operate in all-hazards environments with minimum disruption through and during the event, until normal operations are restored. Further help in the Army planning process can be found in FM 5–0.

3–1. Guidance for the system life cycle

IT contingency planning is similar to all Army planning. The process starts with PEOs and PMs and carries on to the system owner and users. The ITCP is an organic document, meaning it can and must change whenever necessary. The system development life cycle is depicted in figure 3–1.

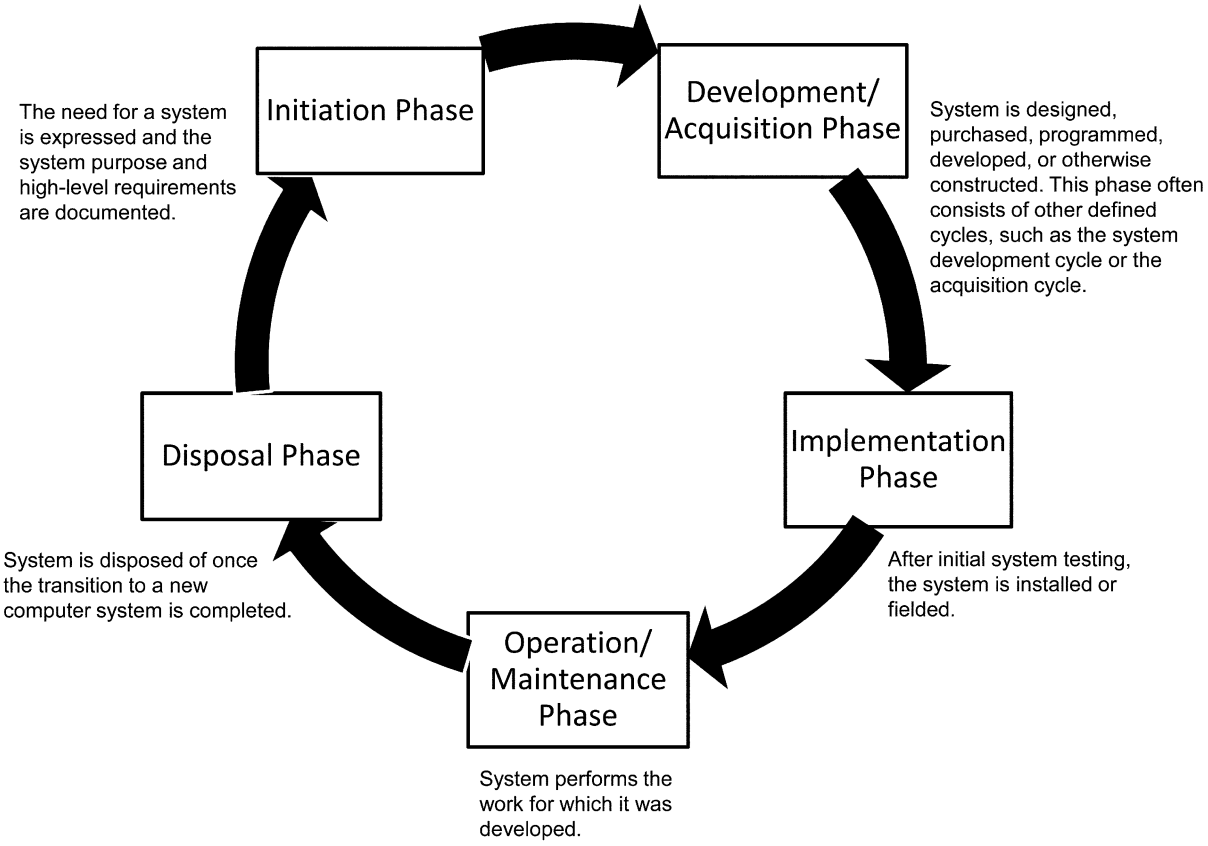


Figure 3–1. System development life cycle

a. Iniation phase. An ITCP should be comprehensive and should receive support and funding. If the ITCP is not incorporated into this phase it is unlikely that the ITCP will overcome the initial lack of requirements.

(1) In this phase, systems requirements are identified and matched to their related operational processes, and initial contingency requirements. This would include classifying systems within their MAC or potential impact level.

(2) During this phase, the new IT systems should be evaluated against all other existing and planned IT systems to determine appropriate recovery priority.

(3) The deliverable for this phase would be a general system ITCP which would address all pertinent issues except site-specific requirements. Below are the elements this should include:

(a) Completing data backup procedures.

(b) Performing disaster and recovery planning.

(c) Identifying essential system functions.

b. Development and acquisition phase. As initial concepts develop into system designs, specific contingency solutions may be incorporated. As in the initiation phase, contingency measures included in this phase should reflect system and operational requirements. In cases where applications and systems are developed by a PM, a standard method for IT contingency planning should be provided to customers. AR 70–1 requires that MC/ME IT systems be registered with the Army CIO/G–6 and the DOD CIO. AR 25–1 requires that MC/ME IT systems be registered in APMS-AITR. AR 70–75 details the requirements for survivability of MC/ME systems. It is also recommended that the MAC level or potential impact level be established according to DOD or Federal regulation as referenced in paragraph 1–6*a*.

(1) The design should incorporate redundancy and robustness directly into the system architecture to optimize reliability, maintainability, and availability during the operation/maintenance phase.

(2) If multiple applications are hosted within the new general support system, individual priorities for those applications should be set to assist with selecting the appropriate contingency measures and sequencing for the recovery execution.

(3) Examples of contingency measures considered in this phase include:

(a) Redundant communication paths.

(b) Single points of failure.

(c) Enhanced fault tolerance of network components and interfaces.

(d) Power management systems with appropriately sized backup power source.

(e) Load balancing.

(f) Data mirroring and replications.

(4) During this phase set up the requirements for service level agreements (SLAs) with the area processing centers (APCs).

c. Implementation phase. As the system undergoes initial testing, contingency strategies also should be tested to ensure technical features and recovery procedures are accurate and effective.

(1) Testing contingency strategies requires a test plan.

(2) Verify contingency measures will be documented in the ITCP.

d. Operation and maintenance phase. Users, administrators, and managers will maintain a training and awareness program which addresses ITCP procedures in accordance with AR 25–2 and FISMA guidelines as established in the MAC level or potential impact level incorporating them into everyday activities.

(1) Exercises and tests should be conducted to ensure procedures remain current and effective.

(2) System backups should be created and stored offsite.

(3) The ITCP should be updated to reflect changes to procedures based on lessons learned through after action reviews conducted at the end of each test or event.

(4) Modifications should be reflected in the ITCP when IT systems are upgraded or modified.

(5) Documented changes should be incorporated in a timely manner to maintain an effective ITCP.

e. Disposal phase. Contingency considerations for an existing system remain in effect during transition to a replacement capability.

(1) Until the new system is fully tested, accredited, and operational (including its contingency capabilities), the original systems ITCP applies. As legacy systems are replaced, they may provide a valuable backup capability if a loss or failure of the new system should occur.

(2) Legacy systems can be used as test systems for new applications, allowing potentially disruptive system flaws to be identified and corrected on non-operational systems.

3–2. Develop the information technology contingency policy

a. The IT contingency policy is consistent with applicable Federal laws, directives, policies, regulations, standards, and guidance. The IT contingency policy can be included as part of a general information security policy for the organization. This will include the special requirements for heath data as required by the Health Insurance Portability and Accountability Act.

b. The IT contingency policy is developed and signed by the commander. This will ensure the ITCP is supported by senior management. These officials can be included in the process to develop the program policy, structure, objectives, and roles and responsibilities. An example of an organizational IT contingency policy is located at Annex C as referenced in paragraph 4–1*e*(5)(*c*) of this publication.

c. At a minimum, the IT contingency policy should comply with the FISMA as outlined in NIST SP 800–53 and AR 500–3. These COOP requirements provide a good guide for ITCP requirements, as an ITCP is often part of a COOP plan.

d. Agencies should evaluate their IT systems, operations, and requirements to determine if additional IT contingency planning requirements are necessary. Key policy elements for consideration include:

(1) Scope, as it applies to the type(s) of platform(s) and organization functions subject to IT contingency planning.

(2) Responsibilities.

(3) Resource requirements.

(4) Plan maintenance schedule.

(5) Frequency of backups and storage of backup media.

(6) Non-compliance punishments.

(7) ITCP POC information.

(8) APC support.

e. As the IT contingency policy and plan are developed, they should be coordinated with related and relevant organization activities, including:

(1) IT and physical security.

(2) Human resources.

(3) IT operations.

(4) Emergency preparedness functions. ITCP activities should be compatible with program requirements for these

areas and contingency personnel should coordinate with representatives from each area to remain aware of new or evolving policies, programs, or capabilities.

3–3. Establish roles and responsibilities

a. The responsibility and authority will come from the IT contingency policy developed and signed by the commander. This will enhance the ITCP coordinator's ability to execute his or her responsibilities through a funded ITCP.

b. It is essential among selected ITCP teams (see paras 2–7 through 2–9) in support of the ITCP coordinator to ensure a comprehensive and thoroughly tested ITCP to delegate work responsibilities. It is still important to have a single authority appointed as he or she will consolidate all information into a comprehensive plan and will continually update, register, and test the plan, as needed or required, by DOD or Federal regulations.

c. ITCP teams are not required but are recommended to provide support to the ITCP coordinator.

d. The results of the BIA described in paragraph 3–5 should be incorporated into the analysis and strategy development efforts, and will help identify which ITCP teams are needed.

3–4. Conduct composite risk management

a. Army risk management regarding IT contingency planning is regulated by two administrative publications; FM 5–19 and AR 525–26. These publications provide a general outline on the process for creating a risk management plan. This section will first highlight general process steps prescribed in the other publications, and then give more specific help for IT contingency planning. Composite risk management (CRM) is a five-step process:

(1) Identify hazards.

(2) Assess hazards to determine risk.

(3) Develop controls and make risk decisions.

(4) Implement controls.

(5) Supervise and evaluate.

b. Steps 1 and 2 are assessment steps, steps 3 through 5 are managerial. For a thorough explanation of each step refer to FM 5–19.

c. To help a planner in this process the Army has developed DA Form 7566, Composite Risk Management Worksheet.

(1) The ITCP coordinator can utilize this form in the planning process.

(2) This form would be a helpful addition to any ITCP documentation.

(3) If used, this form should be updated as often as necessary. The more it is updated, the better chance an ITCP has to be fully comprehensive.

d. Composite risk management is a process. Effective CRM requires that the process be integrated into all phases of mission or operational planning, preparation, execution, and recovery.

e. IT contingency planning risk management transcends traditional protection programs by focusing on the continuation of essential functions regardless of threats from or vulnerabilities to unplanned natural, technological, or manmade (deliberate attacks or accidents with unintended consequences) events. Policy and procedures consider cyber and physical infrastructure as supporting elements of essential functions.

f. It is important to implement risk mitigation operations to minimize the possibility of executing the ITCP.

g. Risk management is a team activity and should begin by forming a risk management team. Refer to paragraph 2–7 for guidance on the roles of the risk management team.

h. Risk mitigation strategies include, but are not limited to:

(1) Appropriately sized uninterruptible power supplies (UPSs) to provide short-term backup power to all system components (including environmental and safety controls).

(2) IT design changes or technical controls useful in precluding or reducing continuity issues.

(3) Gasoline-powered or diesel-powered generators to provide long-term backup power.

(4) Air-conditioning systems with adequate excess capacity to accommodate failure of certain components, such as a compressor.

(5) Fire detection and suppression systems.

(6) Water sensors in the computer room ceiling and floor.

(7) Plastic tarps that may protect IT equipment from water damage.

(8) Heat-resistant and waterproof containers for backup media and vital nonelectronic records.

(9) Emergency master system shutdown switch.

(10) Offsite storage of backup media, nonelectronic records, and system documentation.

(11) Technical security controls, such as cryptographic key management and least-privilege access controls.

(12) Frequent, scheduled backups.

(13) Environmental control monitoring systems.

3–5. Conduct a business impact analysis

a. The BIA enables the ITCP coordinator to fully characterize system requirements, processes, and interdependencies and use this information to determine contingency requirements and priorities. The BIA process helps ITCP coordinators streamline and focus their ITCP development activities to achieve a more effective plan by identifying recovery priorities. A general flow chart for identifying recovery priorities for a singular critical business process is located in figure 3–2.

b. The purpose of the BIA is to show the relationship of specific system components with the critical services they provide and characterize the consequences of a disruption to the system components.

(1) The effects of the outage may be tracked over time. This enables the ITCP coordinators to identify the maximum allowable time a resource may be denied before it prevents or inhibits the performance of an essential function.

(2) The effects of the outage may be tracked across related resources and dependent systems, identifying any cascading effects that may occur as a disrupted system affects other processes that rely on it.

c. The BIA identifies critical IT resources. IT systems can be very complex, with numerous components, interfaces, and processes. A system often has multiple missions resulting in different perspectives on the importance of system services or capabilities. This first BIA step evaluates IT systems to determine the critical functions performed by the system and to identify the specific system resources required to perform them.

(1) Identify disruption allowable outage times.

(a) The optimal point to recover the IT system is found by balancing the cost of system inoperability against the cost of resources required for restoring the system.

(b) This will define how long the organization can afford to allow the system to be disrupted.

(2) Develop recovery priorities.

(a) The outage impact(s) and allowable outage times characterized in the previous step enable the development and prioritization of recovery strategies that personnel will implement during ITCP activation.

1. For example, if the outage impact step determines that the system should be recovered within 4 hours, the ITCP coordinators would need to adopt measures to meet that requirement.

2. Similarly, if most system components could tolerate a 24–hour outage, but a critical component could be unavailable for only 8 hours, the ITCP coordinators would prioritize the necessary resources for the critical component.

(b) By prioritizing these recovery strategies, the ITCP coordinators will make more informed, tailored decisions regarding contingency resource allocations and expenditures, saving time, effort, and costs.

d. For a complete guide on the BIA refer to NIST SP 800–34.

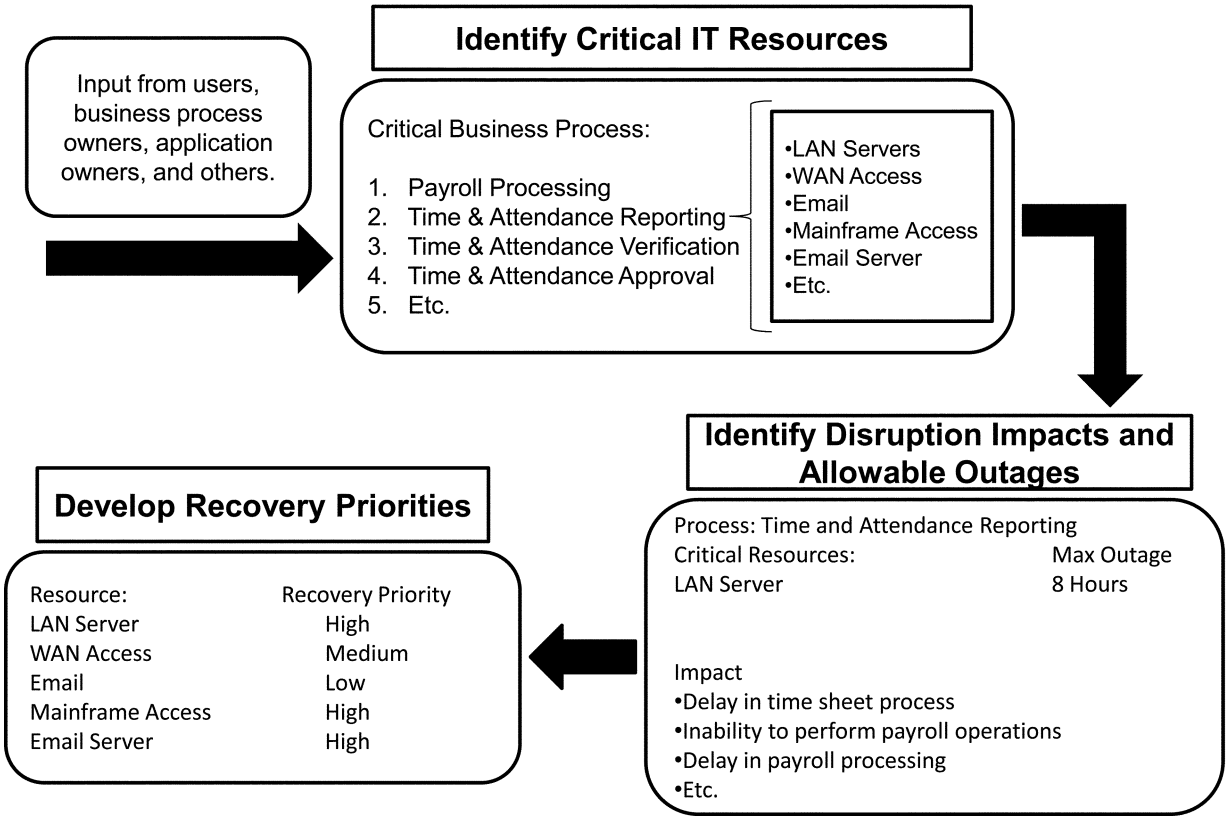


Figure 3–2. Identify critical information technology resources

3–6. Develop a data backup policy

a. Requirements. Backup is required by both DOD and Federal statute. To what extent and how often depends on the category of the system. Utilize the MAC level or the potential impact level requirements as the base-line for backup strategies.

b. Backup policy. The most effective data backup policy designates the location of stored data, file-naming conventions, frequency of backups (for example, daily or weekly, incremental or full), and methods for transporting data offsite. The protection and ready availability of electronic and hardcopy emergency operating records, documents, references, records, and information systems needed to support MEFs at an alternate site under the full spectrum of emergencies is a critical element of a successful ITCP. Personnel should have access to and be able to use these records and systems in conducting their essential functions. Refer to DA Pam 25–403 for more information.

c. Data storage media. Data may be backed up on magnetic disk, tape, or optical disks (such as compact disks [CDs]). The specific method chosen for conducting backups should be based on system and data availability and integrity requirements refer to AR 380–5 for specific guidelines on security of this material.

d. Off-site storage. It is a good business practice to store backed up data offsite. If your system is supported in everyday operations in an APC, there is an option to have your system backup to alternate APCs. This would be part of the SLA as described in paragraph 3–7*c*.

e. Vital records and databases. The protection and ready availability of electronic and hard copy emergency operating records, documents, references, records, and information systems needed to support MEFs at an alternate site under the full spectrum of emergencies is a critical element of a successful ITCP. Personnel with need-to-know access should have access to and be able to use these records and systems in conducting their essential functions. Refer to DA Pam 25–403 for more information.

f. Equipment replacement. If the IT system is damaged or destroyed, or the primary site is unavailable, necessary hardware and software will need to be activated or procured quickly and delivered to the alternate location. When selecting the most appropriate strategy, note that the availability of transportation may be limited or temporarily halted in the event of a catastrophic disaster.

g. Vendor agreements. Agreements with hardware, software, and support vendors may be made for emergency maintenance service. The agreements should specify the requirements in paragraph 3–7*c*.

h. Equipment inventory. Required equipment may be purchased in advance and stored at a secure off-site location, such as an alternate site where recovery operations will take place (warm or mobile site) or at another location where they will be stored and then shipped to the alternate site. This solution has certain drawbacks, however. An organization must commit financial resources to purchase this equipment in advance and the equipment could become obsolete or unsuitable for use over time because system technologies and requirements change.

i. Existing compatible equipment. Equipment currently housed and used by the contracted hot site or by another organization within the agency may be used by the organization. Agreements made with hot sites and reciprocal internal sites stipulate that similar and compatible equipment will be available for contingency use by the organization.

j. Procedures. Most importantly, backup procedures should be implemented into the daily routine of an office. This will ensure all parties involved know where the information is going and also ensure their information has a backup.

k. Access. Having a backup policy for the system does not alone ensure continuity of operations. Access to the information is also needed. For more information, refer to paragraphs 3–7 and 3–8, of this publication.

3–7. Establish alternate sites

a. Although major disruptions with long-term effects may be rare, they should be accounted for in the ITCP. As such, the plan should include a strategy to recover and perform system operations at an alternate facility for an extended period. The selection of the type of site should be based on the organizations BIA, cost, and requirements of the system. Table 3–1 summarizes the criteria which can be employed to determine which type of alternate site meets the organization's requirements. Table 3–2 gives a basic outline of costs associated with ITCP.

b. Alternate sites can contain the system backup hardware or could be a remote site that is, in essence, teleworking from an off-site location, also known as a teleworking site. In general, three types of alternate sites are available:

(1) Dedicated site-owned or site-operated by the organization.

(2) Reciprocal agreement or memorandum of agreement with an internal or external entity.

(3) Commercially-leased facility.

c. Once selected, the above three site types can be further categorized into one of the five below categories.

(1) *Cold site.* Typically consists of a facility with adequate space and infrastructure (electric power, telecommunications connections, and environmental controls) to support the IT system.

(2) *Warm site.* Partially equipped office spaces that contain some or all of the system hardware, software, telecommunications, and power sources. The warm site is maintained in an operational status, ready to receive the relocated system. In many cases, a warm site may serve as a normal operational facility for another system or function, and in the event of ITCP activation, the normal activities are displaced temporarily to accommodate the disrupted system.

(3) *Hot site.* Office spaces appropriately sized to support system requirements and configured with the necessary system hardware, supporting infrastructure, and support personnel. Hot sites are typically staffed 24 hours a day, 7 days a week.

(4) *Mobile site.* Self-contained, transportable shells custom-fitted with specific telecommunications and IT equipment necessary to meet system requirements.

(5) *Mirrored site.* Fully redundant facilities with full, real-time information mirroring. Mirrored sites are identical to the primary site in all technical respects.

Table 3–1
Alternate site criteria selection

Site	Cost	Hardware Equipment	Telecommunications	Setup Time	Location
Cold Site	Low	None	None	Long	Fixed
Warm Site	Medium	Partial	Partial/Full	Medium	Fixed
Hot Site	Medium/High	Full	Full	Short	Fixed
Mobile Site	High	Dependent	Dependent	Dependent	Not Fixed
Mirrored site	High	Full	Full	None	Fixed

d. Service level agreements.

(1) A memorandum of understanding, memorandum of agreement, operational level agreement, or an SLA for an alternate site or backup processing should be developed specific to the organization's needs and the partner organization's capabilities. It is up to the ITCP coordinator to decide which agreement is most relevant. The legal department of each party must review and approve the agreement. In general, the agreement can address each of the following elements:

(a) Contract/agreement duration.

(b) Cost/fee structure for disaster declaration and occupancy (daily usage), administration, maintenance, testing, annual cost/fee increases, transportation support cost (receipt and return of offsite data and supplies, as applicable), cost/expense allocation (as applicable), and billing and payment schedules.

(c) Disaster declaration (for example, circumstances constituting a disaster and notification procedures).

(d) Site/facility priority access and/or use in the event of a catastrophic disaster involving multiple clients.

(e) How quickly the vendor must respond after being notified.

(f) Site availability.

(g) Site guarantee.

(h) Other clients subscribing to same resources and site, and the total number of site subscribers, as applicable.

(i) Contract/agreement change or modification process.

(j) Contract/agreement termination conditions.

(k) Process to negotiate extension of service.

(l) Guarantee of compatibility.

(m) IT system requirements (including data and telecommunication requirements) for hardware, software, and any special system needs (hardware and software).

(n) Change management and notification requirements, including infrastructure.

(o) Security requirements, including special security needs.

(p) Staff support provided/not provided.

(q) Facility services provided/not provided (for example, use of on-site office equipment, and cafeteria).

(r) Testing, including scheduling, availability, test time duration, and additional testing, if required.

(s) Records management (on-site and off-site), including electronic media and hard copy.

(t) Service level management (performance measures and management of quality of IT services provided).

(u) Workspace requirements (for example, chairs, desks, telephone, personal computers).

(v) Supplies provided or not provided (for example, office supplies).

(w) Additional costs not covered elsewhere.

(x) Other contractual issues, as applicable.

(y) Other technical requirements, as applicable.

(2) Be aware that multiple organizations may contract with a vendor for the same alternate site; as a result, the site may be unable to accommodate all of the customers if a disaster affects enough of those customers simultaneously. The vendor's policy on how this situation should be addressed and how priority status is determined should be negotiated.

(3) Two or more organizations with similar or identical IT configurations and backup technologies may enter a formal agreement to serve as alternate sites for each other or enter into a joint contract for an alternate site. This type of site is set up via a reciprocal agreement or memorandum of understanding. A reciprocal agreement should be entered into carefully because each site must be able to support the other in addition to its own workload in the event of a disaster. This type of agreement requires the recovery sequence for the applications from both organizations to be prioritized from a Joint perspective, favorable to both parties.

(4) Alternate site and emergency communications: the success of organizational operations at an alternate facility is dependent on the availability and redundancy of critical communications systems to support connectivity to internal organizations, other agencies, critical customers, and the public. When identifying communications requirements, agencies should take maximum advantage of the entire spectrum of communications media likely to be available in any emergency situation. These services may include, but are not limited to: secure and/or non-secure voice, fax, and data, connectivity; Internet access; and e-mail. Interoperable communications should provide:

(a) Capability commensurate with an organization's MEFs and activities.

(b) Ability to communicate with the ITCP staff, management, and other organizational components.

(c) Ability to communicate with other agencies and emergency personnel.

(d) Access to other data and systems necessary to conduct essential activities and functions.

(e) It is essential that emergency communications planning prepares for the loss of e-mail capability. In the event that a WAN or LAN is lost, so is any e-mail capability. Other methods such as cellular/wireless, including secure voice phones, Iridium, and International Maritime Satellite/Enhanced Mobile Satellite Services may be helpful for ITCP coordinators. It is recommended that at least some of the personnel responsible for carrying out the ITCP have access to cellular phones and wireless devices that have had wireless priority service added to them. Similarly, those personnel

should have access to the Government emergency telephone service. In previous contingency scenarios, landline service was non-existent and cellular and wireless networks soon became congested. Wireless priority service and Government emergency telephone service both assist essential and first responder personnel in getting calls through.

3–8. Creating telework policies

a. Plans should be in place that will allow Government business to continue during emergency situations. Telework is a virtual resource solution and provides access to resources that may not be available otherwise. Agencies have the flexibility to use teleworkers in emergency situations, but it will not happen spontaneously. A viable ongoing telework program is the foundation that should be utilized to help facilitate preparedness.

b. Telework provides flexibility in the locations where employees may perform their jobs. Telework lets employees work at home, at an alternate office closer to home, or at other defined telework locations as established during an alternate site designation. Telework may be performed on a fixed schedule or at random. For the Army, perhaps the most important aspect of telework is that it can greatly facilitate the ITCP in times of crisis. See AR 25–1 and DA Pam 25–1–1 for additional telework policy and procedures.

c. Designated contingency facilities may not have all the staff needed to support MEFs and may not be able to accommodate enough key staff to facilitate maximum Government operations. Organizations should make sure that key members of the staff are designated to report to alternate sites, including their home, if they telework.

d. Telework is particularly appropriate in times of a pandemic health crisis in which direct contact is discouraged. Although this is not an IT crisis on the surface, losing access to the workforce that supports command, control, communications, and computers/IT would be.

3–9. Develop activation criteria

Activation criteria should give a baseline state of degraded services provided by the IT system in which case the ITCP will be activated. This can be developed in conjunction with the CRM plan and can give different scenarios which would cause the IT system to be disrupted. The ITCP can develop activation criteria focused on what MAC or potential impact level the system is at. The ITCP coordinator must create activation criteria in accordance with those levels. It would be most beneficial to create a checklist that describes minimum system functions if degraded or inoperable, would activate the ITCP.

3–10. Establish recovery strategies

a. Recovery strategies provide a way to restore IT operations quickly and effectively following a service disruption. The strategies should address disruption impacts and allowable outage times identified in the BIA. Several alternatives should be considered when developing the recovery strategy including:

(1) Cost.

(2) Allowable outage time.

(3) Security.

(4) Integration with larger, organization-level ITCPs and COOP plans.

b. A wide variety of recovery approaches may be considered; the appropriate choice depends on the incident, type of system, and its operational requirements. It is important to balance the costs of the recovery with the length of time planned for recovery. To do this, a recovery strategy budget planning guide is provided in table 3–2. More technical information on specific systems can be found in chapter 5, but a good general recovery strategy:

(1) Addresses potential impacts identified in the BIA.

(2) Integrates the system architecture during the design and implementation phases of the system lifecycle.

(3) Includes a combination of methods to provide recovery capability over the full spectrum of incidents.

c. The most effective recovery strategies use established backup methods and alternate sites to connect to the backup, if the backup does not have a front end physical connection site for employees.

(1) Backup methods (see para 3–6).

(2) Alternate sites or telework policies (see paras 3–7 and 3–8 and table 3–2).

Table 3–2
Recovery strategy budget planning example (in dollars)

		Vendor Costs	Hardware Costs	Software Costs	Travel/ Shipping Costs	Labor/ Contractor Costs	Testing Costs	Supply Costs	Totals
Alternate Site	Cold Site	25,000	30,000	3,000	15,000	20,000	2,000	10,000	105,000
	Warm Site	50,000	40,000	4,000	10,000	15,000	3,000	8,000	130,000
	Hot Site	75,000	45,000	4,500	5,000	10,000	4,000	5,000	148,500
	Mobile Site	75,000	45,000	4,500	8,000	15,000	4,000	5,000	156,500
	Mirrored Site	50,000	40,000	4,000	5,000	10,000	3,000	3,000	115,000
Offsite Storage	Commercial	100,000	0	0	5,000	10,000	4,000	3,000	122,000
	Internal	25,000	30,000	3,000	0	0	2,000	2,000	62,000
Equipment Replacement	SLAs	25,000	30,000	15,000	0	10,000	3,000	0	83,000
	Storage	20,000	20,000	5,000	0	0	0	0	45,000
	Existing Use	0	50,000	3,000	3,000	0	2,000	2,000	60,000

3–11. Establish service priorities

a. During stressed situations, the reduction or denial of information services to some users may be necessary to support MEFs. The stressed situation may be due to a mobilization effort, wartime operation, terrorist activity, civil disturbance, or natural disaster and may result from increased system use or service degradation due to equipment, software, or transmission failure. The direct impact will be that provisions of quality information service will not be possible. User access to some systems should be restricted or denied to ensure essential operational users are supported.

b. Guidelines are provided by the National Communications System (NCS) for reduction of information transfer traffic in an emergency (Minimize) and communications circuit restoration priority system procedures. However, these do not apply to most installation information service users for ITCP, telephone service, or data processing support. For more information on the NCS, see the Minimize policy in AR 25–1.

c. The following prioritization scheme criteria are used for the prioritization of information services provided to users not assigned an NCS priority:

(1) *Priority 1.* Systems use associated with essential command and control operations.

(2) *Priority 2.* Systems use associated with essential security, safety, and fire operations.

(3) *Priority 3.* Systems use essential for national emergency, mobilization, or natural disaster operations.

(4) *Priority 4.* Systems use very useful in meeting national emergency, mobilization, or natural disaster operations.

(5) *Priority 5.* Systems use not essential to support national emergency, mobilization, or natural disaster operations, but essential to satisfy other mission/installation support requirements.

(6) *Priority 6.* Systems use not essential and could be discontinued or eliminated during the stressed situation.

d. Prioritization schemes are developed as a coordinated effort with users and installation contingency/mobilization planners. Completed prioritization schemes are approved by the installation commander.

e. Denial of services and/or restoration of communications circuits and associated terminal equipment that are assigned NCS restoration priorities is made under policies and procedures established by NCS.

3–12. Plan testing, training, and exercise

a. The organization should test the contingency plan for the information system at least annually, using one of the two defined testing procedures in accordance with the appropriate MAC level requirement. This will determine the plan's effectiveness and the organization's readiness to execute the plan. Appropriate officials review the contingency plan test results and initiate corrective actions. Additionally the organization can coordinate contingency plan testing with organizational elements responsible for related plans (for example, business continuity plan, disaster recovery plan, continuity of operations plan, business recovery plan, and incident response plan). Another good business practice, if applicable, is testing the contingency plan at the alternate processing site to familiarize contingency personnel with the facility and available resources and to evaluate the site's capabilities to support contingency operations.

b. Planned testing is a critical element of a viable ITCP and will be conducted at least annually. For MAC level I systems, testing will be conducted semi-annually per DOD guidance. Testing enables plan deficiencies to be identified and addressed. Testing also helps evaluate the ability of the recovery staff to implement the plan quickly and

effectively. Each ITCP element should be tested to confirm the accuracy of individual recovery procedures and the overall effectiveness of the plan. This will be confirmed or denied by an after action review and report.

c. To derive the most value from the test, a test plan will be developed to test the selected element(s) against explicit test objectives and success criteria.

d. Management support and buy-in is essential. Poorly conducted and planned testing is a waste of time and money. Poor use of personnel time in testing will erode the ability of the official responsible for testing to accomplish planning and training tasks in the future.

e. The most effective ITCP test will include, at a minimum:

(1) Notification procedures.

(2) Coordination among recovery teams.

(3) Systems recovery on an alternate platform from backup media.

(4) Internal and external connectivity.

(5) Systems performance using alternate equipment.

(6) Restoration of normal operations.

(7) After action review and report.

f. The following list contains the types of acceptable testing:

(1) *Tabletop.* Contingency response team members are alerted or assembled to a location and allowed a certain quantity of time to work through a contingency scenario. This type of training is the easiest and least expensive method in which to test emergency preparedness.

(2) *Functional testing and system testing.* System testing entails utilizing only a portion of the contingency response team and is limited to a specific system or process. This type of testing is excellent for instituting new systems, or new procedures for old systems, into the continuity plan. System testing can also be used to test and train on failover hardware and procedures. For example, a failover test can be conducted on redundant firewall modules in a router.

g. A thorough after action review should be conducted with all individuals involved in the testing and training event.

(1) ITCP documentation should be updated and a full report filed, to include lessons learned.

(2) Action items should be assigned to team members and all deliverables tracked.

(3) Procedures found to be inadequate should be documented, changed and retested as soon as feasible.

(4) Information collected during the test and post-test reviews that improve plan effectiveness should be incorporated into the ITCP.

(5) The ITCP coordinator should record plan modifications using a record of changes, which lists the page number, change comment, and date of change.

h. Announcing the test in advance is a benefit to team members so they can prepare for it mentally and have time to prioritize their workload. It is likely that some team members will not be available because of absence or because the test may be disruptive to their workload. Personnel availability issues are beneficial to the plan to capture how a real response may play out, thus providing critical input to plan modifications. It is important that an exercise should never disrupt normal operations. If testing at the alternate facility, the ITCP coordinator should coordinate test dates and operations with the facility.

i. Training for personnel with ITCP responsibilities should complement testing. Training should be provided at least annually; new hires who will have plan responsibilities should receive training shortly after they are hired. Ultimately, ITCP personnel should be trained to the extent that they are able to execute their respective recovery procedures without aid of the actual document. This is an important goal in the event that paper or electronic versions of the plan are unavailable for the first few hours resulting from the extent of the disaster. Recovery personnel should be trained on the following plan elements:

(1) Purpose of the plan.

(2) Cross-team coordination and communication.

(3) Reporting procedures.

(4) Security requirements.

(5) Team-specific processes (notification/activation, recovery, and reconstitution phases).

(6) Individual responsibilities (notification/activation, recovery, and reconstitution phases).

(7) Tape archiving.

3–13. Information technology contingency plan maintenance

a. Because the ITCP contains potentially sensitive operational and personnel information, its distribution should be marked accordingly and controlled according to AR 380–5.

b. Typically, copies of the plan are provided to recovery personnel for storage at home and the office. A copy should also be stored at the alternate site and with the backup media. Storing a copy of the plan at the alternate site ensures its availability and good condition in the event local plan copies cannot be accessed because of the disruption. The ITCP coordinator along with the NEC should maintain a record of copies of the plan and to whom the plan was distributed.

c. To be effective, the plan must be maintained in a state of readiness that accurately reflects system requirements, procedures, organizational structure, and policies. IT systems undergo frequent changes because of shifting business needs, technology upgrades, or new internal or external policies. As a general rule, the plan should be reviewed for accuracy and completeness at least annually prior to testing or whenever significant changes occur to any element of the system, capability or plan. Certain elements will require more frequent reviews, such as contact lists and hardware. Evaluate supporting information to ensure the information is current and continues to meet system requirements adequately. This information includes the following:

(1) Names and contact information of team members.
(2) Alternate site contract, including testing times.
(3) Off-site storage contract.
(4) Software licenses.
(5) Memorandums of understandings or vendor SLAs and POC information related to them.
(6) Hardware and software requirements.
(7) System interface agreements.
(8) Security requirements.
(9) Recovery strategy.

d. Based on the system type and criticality, it may be reasonable to evaluate plan contents and procedures more frequently. At a minimum, plan reviews should focus on the following elements:

(1) Operational requirements.
(2) Security requirements.
(3) Technical procedures.
(4) Vital records (electronic and hardcopy).
(5) Alternate and offsite facility requirements.

e. The ITCP coordinator should record plan modifications using a record of changes, which lists the page number, change comment, and date of change. Changes to the ITCP should be communicated to representatives of associated plans or programs, as necessary.

f. Although some changes may be quite visible, others will require additional analysis. The BIA should be reviewed periodically and updated with new information to identify new contingency requirements or priorities. As new technologies become available, preventive controls may be enhanced and recovery strategies may be modified. Table 3–3 is a checklist to assist the planner in determining the viability of IT contingency planning elements.

g. The ITCP coordinator should coordinate frequently with associated internal and external organizations and system POCs to ensure that impacts caused by changes within either organization will be reflected in the contingency plan. Strict version control should be maintained by requesting old plans or plan pages to be returned to the ITCP coordinator in exchange for the new plan or plan pages.

h. The ITCP coordinator should refer to AR 380–5 for information pertaining to the protection of information stored at the site of a contingency situation. More specifically, plans should be in place to monitor emergency personnel so classified material is accounted for as part of the damage assessment phase.

Table 3–3
Questions to determine information technology contingency plan viability

Specific control objectives and techniques
The ITCP coordinator should ensure that policies and procedures for the following checklist questions are implemented, tested, and integrated to assess the viability of IT contingency planning elements.
Contingency Planning Critical Element: Are resources supporting critical operations identified?
Have processing priorities been established and approved by management?
Critical Element: Has a comprehensive contingency plan been developed and documented?
Are critical data files and operations identified and the frequency of file backup documented?
Is there an alternate processing site; if so, is there a contract or interagency agreement in place?
Critical Element: Are tested contingency and/or disaster recovery plans in place?
Is an up-to-date copy of the plan stored securely off-site?
Are employees trained in their roles and responsibilities?
Critical Element: Is the plan periodically tested and readjusted as appropriate?
Is the location of stored backups identified?
Have the most critical and sensitive operations and their supporting computer resources been identified?
Are backup files (tape archives, data replications) created on a prescribed basis and rotated off-site often enough to avoid disruption if current files are damaged?
Is system and application documentation maintained at the off-site location?
Are all system defaults reset after being restored from a backup?
Are the backup storage site and alternate site geographically removed from the primary site and physically protected?
Has the contingency plan been distributed to all appropriate personnel?
Is the plan approved by key affected parties?

Table 3–3
Questions to determine information technology contingency plan viability—Continued

Are there detailed instructions for restoring operations?
Are responsibilities for recovery assigned?

3–14. Information technology contingency planning at the installation level

The ITCP should be fully aligned with the ITCPs of agencies such as Defense Information Systems Agency and the Network Enterprise Technology Command as required in AR 500–3 and AR 525–26. For a list of roles in planning for ITCPs see chapter 2 of this pamphlet. The installation networks and mission are part of the overall infrastructure designed to provide IT support to the Army in both peacetime and war. Local installations should also be prepared to support other garrison and military units in time of crisis by utilizing their own emergency plans. Armywide and installation-level planning is different in two key factors. Armywide ITCPs and operations are usually funded and mandated by regulation. IT contingency operations at the installation level are often poorly funded and based on doctrine from a variety of non-regulated sources. ITCPs at the installation level are generally similar in all phases of any other ITCP with the following exception: multi-year long-term planning focused on near term needs. Long-term planning is needed and warranted in the areas of backbone infrastructure and contingency site location. True multi-year long-term ITCPs at the installation level can be unrealistic and difficult to manage. Technology infrastructure business processes are often in flux and usually mandated from higher headquarters, as are funding and future technologies. Consequently, it is almost impossible to plan for what type of technology will be available in the long term. These limitations mean that ITCPs should be applied when business practices and technology changes are being planned for and implemented at the installation level. Examples of this type of planning include:

a. Purchasing. When purchasing servers for a new business software initiative, plan on purchasing one additional server of the same type, or coordinate with another project(s) to share a redundant server. The additional server can be used for contingency as well as testing purposes. The additional server could be loaded with appropriate software and placed in an alternate location, such as a hot or cold contingency site.

b. Implementation. When implementing a new technology service, create as-built documentation. Add all vendor information as well as system documentation to your ITCP documentation. This will ensure a ready reference is available for rebuilding the service in an emergency.

c. Services. Minimum acceptable services required to support the installation IT infrastructure must be determined. Required functions will vary depending on the installation's IT infrastructure and mission. Any support agreements between a NEC/ITCP coordinator and tenant/user should clearly state the responsibilities of the NEC/ITCP coordinator and tenant/user during a contingency situation.

d. Installation. The installation ITCP is integrated into daily operations. Few if any installation-level activities have a dedicated ITCP coordinator. Therefore, the use of smart books, as-built documents, troubleshooting checklists, and lessons learned should be maximized. Examples of this type of planning include:

(1) When replacing an out-of-date router with a newer model, develop a plan to ensure connectivity remains during the hardware changeover. Configuration changes and actions taken to maintain connectivity should be documented and placed in the installation ITCP. This type of operation simulates and verifies the actions that would be taken during a contingency operation.

(2) Instead of taking mail servers off-line for maintenance, develop a method to transfer users to a different server during the maintenance time period. This type of operation would be useful in documenting a method to move users to an off-site mail server during or after an emergency.

e. Recovery strategies. Recovery strategies are specific, with regard to restoring affected system(s) or business processes to 100 percent of their full capacity before, during, or after an emergency. The first step in this process is to identify what will need to be recovered given the installations worst case scenario. For example, a catastrophic event that occurs at a critical communications center could cause the loss of off-post network connectivity for both the secure internet protocol network (SIPRNET) and non-secure internet protocol router network (NIPRNET). This would cause the loss of off-post email services and internet connectivity. Strategies should be created to meet each individual issue independently as well as the major issue surrounding the loss of the communications center. A good plan will see services and processes that depend on the critical communications center partially restored even though the critical communications center is down. An agreement should be in place with the locally assigned tactical unit to support SIPRNET connectivity in an emergency. The location for the connection should already be identified in the ITCP. All associated documentation and paperwork necessary to execute the recovery strategies should be included in the ITCP.

f. Installation information technology contingency plans. The ITCP is often worked in concert with installation recovery strategies. As recovery strategies combine to restore connectivity following a catastrophic event, ITCPs are combined to restore individual systems that are necessary for the recovery strategy to work. ITCPs are checklists and

procedures for building and recovering a particular system or service from the ground up. For example, a fire destroys the room that houses the installation mail servers and switches that connect the servers to the network.

Chapter 4
The Information Technology Contingency Plan

In general, each organization develops and implements a contingency plan for their information system(s) addressing contingency roles, responsibilities, assigned individuals with contact information, and activities associated with restoring the system after a disruption or failure. To do this the ITCP should be in accordance with NIST SP 800–34 and the general checklist found in NIST SP 800–53, with explanations of each list element further in the document. Another checklist with requirements for DOD systems is located in DODI 8500.2. This publication establishes baseline IA levels for continuity of MAC systems. There are a total of 12 base-line controls for continuity of MAC systems. To be DOD and Federally compliant an ITCP must include these baseline requirements. The following plan format and description will help the ITCP coordinator be compliant with the regulations mentioned above.

4–1. Plan format and required key elements

a. Army organization ITCPs can be designated as an operations plan (OPLAN). Upon ITCP activation, an ITCP OPLAN would automatically become an operation order (OPORD). The planning format and rules are a combination of FM 5–0, Chairman of the Joint Chiefs of Staff Memorandums (CJCSM) 3122.05, Army writing requirements in AR 25–50, and the general requirements contained in Federal Preparedness Circular 65. The ITCP coordinator can adjust the OPLAN to fit mission requirements. ITCP concept of operations (CONOPS) may be incorporated into the OPLAN or published as a separate document as directed by the ITCP coordinator. Security classification will be commensurate with the overall content of the document.

b. It is recommended that an ITCP coordinator use the FM 5–0 five–paragraph format for the basic ITCP OPLAN and annexes, to include paragraphs (1) through (5) listed below:

(1) Situation.
(2) Mission.
(3) Execution.
(4) Service support.
(5) Command and signal.

c. Formatting rules in FM 5–0 and CJCSM 3122.05 will serve as a guide. The general information in Federal Preparedness Circular 65 is a good subject matter outline that will assist planners and writers of ITCP procedures.

d. Paragraph *e,* below provides a suggested ITCP OPLAN outline. ITCP coordinators may adjust the plan as their mission needs dictate and should be able to decide who completes each subtask. Normally, very detailed procedures and/or checklists are included in lower echelon documents while the higher-echelon plans contain big-picture concepts and directions.

e. The following highlights the Federal or organizational requirements for contingency planning that are absolutely mandatory to be Federally or DOD compliant.

(1) Table of Contents:
(2) Tab A: ITCP Policy Statement.
(3) Tab B: Record of Changes and References.
(4) Tab C: Summary of Changes from Previous ITCP OPLAN.
(5) Tab D: Basic ITCP OPLAN.
(a) Annex A: Task organization.
1. Appendix 1 Contact tree.
2. Appendix 3 Team description with roles and responsibilities.
(b) Annex B: Intelligence.
1. Appendix 1 Intelligence estimate/human threats to the system.
2. Appendix 2 Counterintelligence.
3. Appendix 3 Other threats to the system/natural threats to the system.
(c) Annex C: Decision trees, decision tree to activate the ITCP OPLAN, during an ITCP event actions.
(d) Annex D: Command, control, communication, and computer operations:
1. Appendix 1 System description with MEF.
2. Appendix 2 IT architecture related to system.
3. Appendix 3 Location(s) of system hardware.
4. Appendix 4 Other important technical considerations.
(e) Annex H: Service support.
1. Appendix 1 Backup information.

2. Appendix 2 Alternate site documentation and description.
3. Appendix 3 Strip map and directions to alternate site.
4. Appendix 4 Personnel and administration.
a. Rosters Alert and access.
b. Key personnel listings ITCP coordinator, NEC, COOP POCs.
c. Manning/TDA listings.
d. Legal requirements and considerations.
5. Appendix 5 Contracting support.
a. Vendor contact list and contracts.
b. Acquisition.
6. Appendix 6 Reports.
7. Appendix 7 LandWarNet strategy/APC support information.
(f) Annex I: Security measures.
1. Appendix 1 Personnel security and force protection.
2. Appendix 2 Security of backup data.
3. Appendix 3 Health Insurance Portability and Accountability Act requirements.
(g) Annex J: Operations security.
(h) Annex K: Training and testing.
1. Appendix 1 Testing type authorized with process.
2. Appendix 2 After action reports of previous tests.
3. Appendix 3 Business impact statement.
(i) Annex Y: Glossary and terms.
(j) Annex Z: Distribution.

4–2. Information technology contingency plan-specific information for the five-paragraph Information technology contingency operations plan

a. Using the five-paragraph OPLAN format will help in the execution of a functional and successful ITCP. The five-paragraph OPLAN will help the ITCP coordinator with planning for and creating a Federal- and DOD-compliant ITCP. Contained within this section is information which supplements the description and explanation of the OPLAN format found in FM 5–0. Another helpful OPLAN to review is the Headquarters of the Department of Army COOP OPLAN available for view on the Army COOP office Web site.

b. Below is ITCP specific information that should be contained within a five-paragraph ITCP OPLAN that may not generally be found in other OPLANs:

(1) List the assumptions of the ITCP OPLAN.
(a) Describe the scope of the ITCP OPLAN.
(b) Give a general system description and architecture.
(c) List the mission essential functions of the system along with priorities.
(2) Mission.
(a) Explain the mission of the ITCP in very general terms, to include which organization(s) is involved, what it will be doing, when it will be doing that, where it will take place and why they will be taking these actions.
(b) A plan without a mission will lack direction.
(3) Execution.
(a) The intent should come from the IT contingency policy statement.
(b) The concept of operations is located in paragraph 4–3.
(c) Coordinating instructions.
1. General conditions that require the plan to be implemented.
2. Commanders critical information requirements (This will come from the IT contingency policy statement).
3. Risk reduction control measures that have been identified in the planning stage.
(4) Service and support:
(a) Name and location of alternate site.
(b) Name and location of backup system(s).
(c) Standing operating procedure process in place for backing up information and data.
(5) Command and signal:
(a) Succession of command will be located in Annex A in the form of a contact tree.
(b) Explain the priority of communication; phone call, radios, email, and so forth.

4–3. Concept of operation

The concept of operations should follow the guideline listed above. All ITCPs can benefit from using this as the CONOPS. There will be three distinct phases to all ITCP CONOPS—

a. Notification and activation phase. This phase addresses the initial actions taken to detect and assess damage inflicted by a disruption to the system. Based on the assessment of the event, the plan may be activated by the ITCP coordinator. This phase should include sections on:

(1) System priorities.

(2) Contact information.

(3) Damage assessment procedures.

(4) Alternate assessment procedures.

(5) Upon completion of the damage assessment.

(6) Conditions that require the plan to be implemented.

b. Recovery phase. This section provides procedures for recovering the application at the alternate site, whereas other efforts are directed to repair damage to the original system and capabilities.

(1) An example of a sub-mission statement for this phase is: "The following procedures are for recovering the system at the alternate site. Procedures are outlined per team required. Each procedure should be executed in the sequence it is presented to maintain efficient operations."

(2) This phase should be broken down by sub-sections on recovery goals by priority as identified in the BIA. Each goal should include sub-sections with general explanations of what each team as identified in the BIA should be doing.

c. Return to normal operations phase. This section discusses activities necessary for restoring your system's operations at your organization's original or new site. When the computer center at the original or new site has been restored, your system's operations at the alternate site must be transitioned to the original or new site. The goal is to provide a seamless transition of operations from the alternate site to the computer center. This phase should include the following sub-sections:

(1) *Original or new site restoration.* Procedures should be outlined, per necessary team, to restore or replace the original site so that normal operations may be transferred. IT equipment and telecommunications connections should be tested.

(2) *Concurrent processing.* Procedures should be outlined, per necessary team, to operate the system in coordination with the system at the original or new site. These procedures should include testing the original or new system until it is functioning properly and the contingency system is shut down gracefully.

(3) *Plan deactivation.* Procedures should be outlined, per necessary team, to clean the alternate site of any equipment or other materials belonging to the organization, with a focus on handling sensitive information. Materials, equipment, and backup media should be properly packaged, labeled, and shipped to the appropriate location(s). Team members should be instructed to return to the original or new site.

4–4. Plan annexes and appendixes

a. Contingency plan annexes. Contingency plan annexes and appendixes provide key details not contained in the main body of the plan. The appendixes should reflect the specific technical, operational, and management contingency requirements of the given system; however, some annexes and appendixes are frequently found within the ITCP. This section is meant to clarify the annexes and appendixes listed above in paragraph 4–1*e*.

b. Annex A: Task organization.

(1) This annex should contain at least a contact tree and a description of roles and responsibilities of any teams involved with the ITCP. This will ensure the plan is compliant with Federal and DOD statute. A call tree can look like figure 4–1. It should contain the following information for each individual involved in the ITCP.

(a) Team position.

(b) Name.

(c) Contact information.

1. Cell phone.

2. Home phone.

3. Work phone.

4. Pager numbers.

5. E-mail addresses.

6. Home addresses.

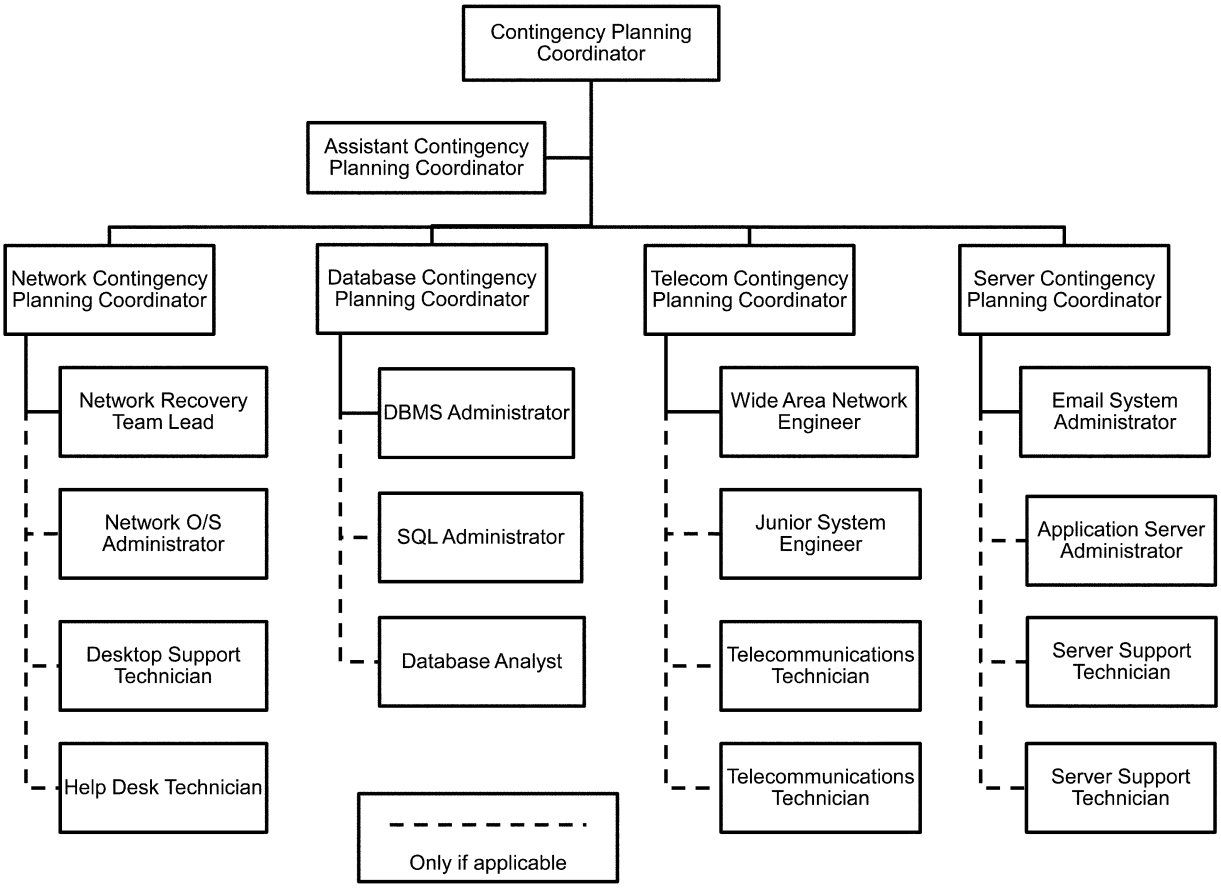


Figure 4–1. Sample call tree

(2) A description of the process should also be included along with the call tree. The type of information to be relayed to those being notified should be documented in the plan. When possible, ITCP response teams are the first teams notified of the incident. The amount and detail of information relayed may depend on the specific team being notified. As necessary, notification information should include the following:

(a) Nature of the emergency that has occurred or is impending

(b) Loss of life or injuries

(c) Any known damage estimates

(d) Response and recovery details

(e) Where and when to convene for briefing or further response instructions

(f) Instructions to prepare for relocation for estimated time period

(g) Instructions to complete notifications using the call tree (if applicable)

(h) When the damage assessment team will convene.

(3) A description of damage assessment team duties and responsibilities is explained below with a sample team checklist in table 4–1.

(a) Information technology contingency plan implementation following an emergency. To determine how the ITCP will be implemented following an emergency, it is essential to assess the nature and extent of the damage to the system. This damage assessment should be completed as quickly as the given conditions permit, with personnel safety remaining the highest priority. Types of information to be covered by the damage assessment team are as follows:

1. Cause of the emergency or disruption.

2. Potential for additional disruptions or damage.

3. Area affected by the emergency.

4. Status of physical infrastructure (for example, structural integrity of computer room, condition of electric power, telecommunications, and heating, ventilation, and air-conditioning).

5. Inventory and functional status of IT equipment (for example, fully functional, partially functional, and nonfunctional).

6. Type of damage to IT equipment or data (for example, water damage, fire and heat, physical impact, and electrical surge).

7. Items to be replaced (for example, hardware, software, firmware, and supporting materials).

8. Estimated time to restore normal services.

(b) Personnel with damage assessment responsibilities. Personnel with damage assessment responsibilities should understand and be able to perform these procedures in the event the paper plan is unavailable during the situation. Once the impact to the system has been determined, the appropriate teams should be notified of updated information and planned responses to the situation.

Table 4–1
Sample local area network recovery team process

Recovery process for the LAN recovery team: *These procedures are used for recovering a file from backup tapes. The LAN recovery team is responsible for reloading all critical files necessary to continue production. Note the time as each is completed.*
1. Identify file and date from which file is to be recovered.
2. Identify tape number using tape log book.
3. If the tape is not in the tape library, request the tape from the recovery facility; fill out with appropriate authorizing signature.
4. When tape is received, log date and time.
5. Place tape into drive and begin recovery process.
6. When file is recovered, notify LAN recovery team leader.

c. Annex B: Intelligence. This annex will assess the threats internally and externally to the system. Human threats can be both internal and external. Externally, the human threat can come in the form of such attacks as a distributed denial of service attack. Internally, such threats can come from an employee tampering with the system or downloading unauthorized material. Environmental threats include natural disasters as well as weather disabling the power infrastructure. Much of this information came from or can be used by the composite risk assessment for the system.

d. Annex C: Decision trees. This annex should contain a decision tree to activate the ITCP OPLAN and a decision tree that covers an ITCP during event actions. This will give a simple one line step-by-step process for anyone to easily follow how the ITCP will go into effect and what will happen once it does.

e. Annex D: Command, control, communications and computers operations. This annex and Annex H are the most important annexes as they give the system information and how to make the system and ITCP work.

(1) Appendix 1 (System description with MEF): This appendix should give a short description of the system with a list of the system's Mission Essential Functions as identified in the IT contingency planning process. This will ensure all MEFs are accounted for and are easily located and identified.

(2) Appendix 2 (IT architecture related to system): This appendix will give a general diagram of the architecture supporting the system and if applicable, of what the system supports.

(3) Appendix 3 (Location(s) of system hardware): This will give a site name and location identification in the form of a street address, building name, and location within the building. This will help multiple teams find, identify, and locate system hardware.

(4) Appendix 4 (Other important technical considerations): If there are any other technical considerations not discussed within the plan, compile them in this appendix. If there are none, leave the appendix out.

f. Annex H: Service and support.

(1) This is the most important annex. It will ensure the system has a backup process in place that will make the system Federally and DOD compliant.

(a) Appendix 1 (Backup information): This appendix will give the location, description, any SLAs, and the process that is in place for backup of system data or information. This is all regulated by either the DOD MAC level or the Potential Impact level.

(b) Appendix 2 (Alternate site documentation and description): This appendix will give the location, description and any SLAs for use of an alternate site. This is all regulated by either the DOD MAC level or the potential impact level.

(c) Appendix 3 (LandWarNet strategy/APC support information): This appendix will give any information regarding LandWarNet strategy support to the system, if any.

(2) *Annex I: Security measures.*

(a) Appendix 1 (Personnel security & force protection): This annex will explain the process in place to ensure only those personnel with need-to-know access will be able to gain access to the system or system remnants in the case of a natural disaster.

(b) Appendix 2 (Security of backup data): This annex will show that there are both electronic security measures in place and physical security measures in place to secure the data contained in the system backup process. This is regulated by the DOD MAC level.

g. Annex J: Operations security. This annex will give the general operations security plan in place for the system as well as its backup and alternate site.

h. Annex K: Training and testing. This annex is vitally important to maintaining the most effective and comprehensive plan possible. The appendices contained within are regulated by the DOD MAC level of the system and Federal statute. In general, a list of test types and completion dates completed is the most important information contained within this annex, but if the other appendixes are included it will give the ITCP coordinator another tool in effective planning that will garner support and funds from commanders in support of ITCP testing.

i. Tab B: Record of changes. The record of changes should be listed in the format as depicted in table 4–1.

Chapter 5
Contingency Planning for Information Technology Systems

This section complements the process and framework guidelines presented in earlier sections by discussing technical contingency planning considerations for specific types of IT systems. The information presented in this section will assist the reader in selecting, developing, and implementing specific technical contingency strategies based on the type of IT system. Because each system is unique, information is provided at a level that may be used by the widest audience. All of the information presented may not apply to a specific IT system; therefore, the ITCP coordinator should draw on the information as appropriate and modify it to meet the system's particular IT contingency requirements. For each IT platform type, technical measures, such as configuration management, are considered from two perspectives. First, the document discusses technical requirements or factors that the ITCP coordinator should consider when planning a system recovery strategy. Second, technology-based solutions are provided for each platform. The technical considerations and solutions addressed in this section include preventive and recovery measures. Several of these contingency measures are common to all IT systems.

5–1. Desktop computers and portable systems

A desktop computer or portable system (for example, laptop or handheld device) typically consists of a central processing unit, memory, disk storage, and various input and output devices. A personal computer (PC) is designed for use by one person at a time. PCs are ubiquitous in most organizations' IT infrastructures. Because the desktop and portable computers are the most common platform for routine automated processes, they are important elements in an ITCP. PCs can be physically connected to an organization's LAN, can dial into the organization's network from a remote location, or can act as a stand-alone system. Table 5–1 provides an overview of contingency strategies for desktop computers and portable systems.

a. Contingency considerations. Contingency considerations for desktop and portable systems should emphasize data availability, confidentiality, and integrity. To address these requirements, the systems manager should consider each of the following practices:

(1) *Store backups off-site.* Backup media should be stored off-site in a secure, environmentally controlled facility. If users back up data on a stand-alone system rather than saving data to the network, a means should be provided for storing the media at an alternate site. A copy of the ITCP, software licenses, vendor SLAs and contracts, and other important documents should be stored with the backup media. The BIA should help to ascertain how often to send backups off-site.

(2) *Encourage individuals to back up data.* If the PC backup process is not automated from the network, users should be encouraged to backup data on a regular basis. This task can be conducted through employee security training and awareness.

(3) *Provide guidance on saving data on personal computers.* Instructing users to save data to a particular network folder eases the IT department's desktop support requirements. If a machine should be rebuilt, the technician will know which folders to copy and preserve while the system is being reloaded.

(4) *Configuration management.* Good configuration management practices are a necessary driver for good IT contingency planning. Knowing what equipment, software loads, versions, patch status, and configuration parameters are in place is a key element of configuration management, which directs input into IT contingency planning. System recovery is faster if hardware, software, and peripherals are standardized throughout the organization. If standard configurations are not possible throughout the organization, then configurations should be standardized by department or by machine type or model if possible. Additionally, critical hardware components that would need to be recovered

immediately in the event of a disaster should be compatible with off-the-shelf computer components. This compatibility will avoid delays in ordering custom-built equipment from a vendor. For more information on configuration management, refer to DA Pam 25–1–1.

(5) *Document system configurations and vendor information.* Well-documented system configurations ease recovery. Similarly, vendor names and emergency contact information should be listed in the ITCP so that replacement equipment may be purchased quickly.

(6) *Coordinate with security policies and system security controls.* Desktop and portable computer contingency solutions described below should be coordinated with security policies and system security controls. Therefore, in choosing the appropriate technical contingency solution(s), similar security controls and security-related activities (for example, risk assessment or vulnerability scanning) in the production systems should be implemented in the contingency solution(s) to ensure that, during a system disruption or emergency, executing the technical contingency solution(s) does not compromise or disclose sensitive data.

(7) *Use results from the business impact analysis.* Impacts and priorities discovered through the BIA of associated major applications and general support systems should be reviewed to determine related requirement.

b. Contingency solutions. Wide ranges of technical contingency solutions are available for desktop computers. Several efficient practices are discussed here. Data from the BIA of major applications and general support systems should be used to determine the recovery requirements and priorities to implement. Backups are the most common means to ensure data availability on PCs. Certain factors should be considered when choosing the appropriate backup solution.

(1) *Equipment interoperability.* To facilitate recovery, the backup device should be compatible with platform operating system and applications and should be easy to install onto different models or types of PCs.

(2) *Storage volume.* To ensure adequate storage, the amount of data to be backed up should determine the appropriate backup solution.

(3) *Media life.* Each type of media has a different use and storage life, beyond which the media cannot be relied on for effective data recovery.

(4) *Backup software.* When choosing the appropriate backup solution, the software or method used to backup data should be considered. The encryption of backup media should be considered as a means of thwarting data theft. In some cases, the backup application can be as simple as a file copy using the operating system file manager; in cases involving larger data transfers, a third-party application may be needed to automate and schedule the file backup. PC data backups can be accomplished in various ways, including those listed below:

(a) Compact discs and digital video discs. CD and digital video disc (DVD) read-only memory drives come standard in most desktop computers; however, not all computers are equipped with writable CD drives. CDs are low-cost storage media and have a higher storage capacity than floppy diskettes. To read from a CD, the operating system's file manager is sufficient; however, to write to a CD or DVD, a rewritable CD/DVD drive and the appropriate software is required.

(b) Network storage. Data stored on networked PCs can be backed up to a networked disk or a networked storage device:

(c) Networked disk. A server with data storage capacity is a networked disk. The amount of data that can be backed up from a PC is limited by the network disk storage capacity or disk allocation to the particular user. However, if users are instructed to save files to a networked disk, the networked disk itself should be backed up through the network or server backup program.

(d) Networked storage device. A network backup system can be configured to back up the local drives on networked PCs. The backup can be started from either the networked backup system or the actual PC.

(e) Replication or synchronization. Data replication or synchronization is a common backup method for portable computers. Handheld computers or laptops may be connected to a PC to replicate the desired data from the portable system to the desktop computer.

(f) Internet backup. Internet backup, or online backup, is a commercial service that allows PC users to back up data to a remote location over the Internet for a fee. A utility is installed onto the PC that allows the user to schedule backups, select files and folders to be backed up, and establish an "archiving" scheme to prevent files from being overwritten. Data can be encrypted for transmission; however, this will impede the data transfer speed over a modem connection. The advantage of Internet backup is that the user is not required to purchase data backup hardware or media.

c. In addition to backing up data, organizations should also back up system drivers. Organizations should store software and software licenses in a secondary location. If the software is commercial off-the-shelf, it can be purchased through a vendor if the copy or license that was installed before the destruction is unavailable. However, at a minimum, custom-built applications installed on desktops should be saved and stored at an alternate location or backed up through one of the methods described above. Instructions on recovering custom-built applications at an alternate site should also be documented, particularly if the application has hard-coded drive mappings (for the PC or network server). Code that prevents the application from running on a different system should be discouraged. If driver

mappings are hard-coded, the application should be modified to enable the application to be restored on a system other than the original.

d. The popularity of encryption as a security tool used on portable computers is growing. With the increased use of digital signatures for non-repudiation and the use of encryption for confidentiality, organizations should consider including encryption key pairs in their backup strategy. If the encryption key pair and verification key are stored on the PC, data can become unrecoverable or unverifiable if the PC becomes corrupted.

e. Because portable computers are vulnerable to theft, encryption can be used to protect data from being disclosed on a stolen computer. Portable computer users can also be provided a second hard drive to be used while on travel. The second hard drive should contain only the minimum applications and data necessary. By using a second hard drive, the amount of data loss is minimized if the laptop is stolen.

f. Imaging represents another contingency solution. A standard desktop computer image can be stored, and the corrupted computer can be reloaded. Imaging will install the applications and setting stored in the image; however, all data currently on the disk will be lost. Therefore, PC users should be encouraged to back up their data files. Because disk images can be large, dedicated storage, such as a server or server partition, may need to be allocated for the disk images alone. Software may be needed to push the images across the network. To decrease the number of images necessary for recovery in the event that multiple PCs are corrupted, standardizing PC models and configurations across all organizations (configuration management) will save space and ease the process of rebuilding computers. If site relocation is necessary, PC configurations and basic applications needed for mission-critical processing should be documented in the ITCP.

Table 5–1
Contingency strategies for desktop computers and portable systems

Document system and application configurations
Standardize hardware, software, and peripherals
Provide guidance on backing up data
Ensure interoperability among components
Coordinate with security policies and controls
Back up data and store offsite
Back up applications and store offsite
Use alternate hard drives
Image disks
Implement redundancy in critical system components
Use uninterruptible power supplies

5–2. Servers

Servers support file sharing and storage, data processing, central application hosting (such as email or a central database), printing, access control, user authentication, remote access connectivity, and other shared network services. Local users log into the server through networked PCs to access resources the server provides. Table 5–2 provides an overview of contingency strategies for servers.

a. Contingency considerations. Because servers can support or host numerous critical applications, server loss could cause significant problems to business processes.

(1) *Store backup media and software off-site.* As described previously, backup media and software should be stored off-site in a secure, environmentally controlled facility. The storage facility should be located far enough away from the original site to reduce the likelihood that both sites would be affected by the same event.

(2) *Standardize hardware, software, and peripherals.* System recovery may be expedited if hardware, software, and peripherals are standardized throughout the organization or site. Standard configurations should be documented in the ITCP.

(3) *Document system configurations and vendors.* Maintaining detailed records of system configurations enhances system recovery capabilities. Additionally, vendors that supply essential hardware, software, and other components should be identified in the ITCP.

(4) *Coordinate with security policies and system security controls.* Server contingency solutions should be coordinated with security policies and system security controls. Thus, in choosing the appropriate technical contingency solution(s), similar security controls and security-related activities (for example, risk assessment, vulnerability scanning) in the production environment should be implemented to ensure that, during a system disruption or emergency, executing the technical contingency solution(s) does not compromise or disclose sensitive data.

(5) *Use results from the business impact analysis.* Impacts and priorities discovered through the BIA of associated major applications and general support systems should be reviewed to determine related requirements.

Table 5–2
Server contingency strategies

Document system and application configurations
Standardize hardware, software, and peripherals
Coordinate with security policies and controls
Ensure interoperability among components
Back up data and store offsite
Back up applications and store offsite
Use UPSs
Implement redundancy in critical system components
Implement fault tolerance in critical system components
Replicate data
Implement storage solutions

b. Contingency solutions. Several technical measures are available to enhance server recovery capabilities. The BIA of major applications and general support systems should provide information to assist in determining the recovery requirements and priorities. Server contingency planning should emphasize reliability and availability of the network services provided by the server. When selecting the appropriate technical contingency solution, data confidentiality and sensitivity requirements should also be considered. Additionally, when selecting the appropriate server contingency solution, the availability requirements for the server, its applications, and data should be assessed. If possible, as a preventive contingency measure critical functions should not be co-located on servers with non-critical functions. For example, a server hosting a critical application should be dedicated to that application and not provide other resources. As with PCs, servers should be backed up regularly. Servers can be backed up through a distributed system, in which each server has its own drive, or through a centralized system, where a centralized backup device is attached to one server. Three types of system backup methods are available to preserve server data:

(1) *Full.* A full backup captures all files on the disk or within the folder selected for backup. Because all backed up files were recorded to a single media or media set, locating a particular file or group of files is simple. However, the time required to perform a full backup can be lengthy. In addition, full backups of files that do not change frequently (such as system files) could lead to excessive, unnecessary media storage requirements.

(2) *Incremental.* An incremental backup captures files that were created or changed since the last backup, regardless of backup type. Incremental backups afford more efficient use of storage media, and backup times are reduced. However, to recover a system from an incremental backup, media from different backup operations may be required. For example, consider a case in which a directory needed to be recovered. If the last full backup was performed three days prior and one file had changed each day, then the media for the full backup and for each day's incremental backups would be needed to restore the entire directory.

(3) *Differential.* A differential backup stores files that were created or modified since the last full backup. Therefore, if a file is changed after the previous full backup, a differential backup will save the file each time until the next full backup is completed. The differential backup takes less time to complete than a full backup. Restoring from a differential backup may require less media than an incremental backup because only the full backup media and the last differential media would be needed. As a disadvantage, differential backups take longer to complete than incremental backups because the amount of data since the last full backup increases each day until the next full backup is executed.

c. A combination of backup operations can be used depending on the system configuration and recovery requirements. For example, a full backup can be conducted on the weekend with differential backups conducted each evening. In developing the server backup schedule, the following questions should be considered:

(1) Where will media be stored?

(2) What data should be backed up?

(3) How frequently are backups conducted?

(4) How quickly are the backups to be retrieved in the event of an emergency?

(5) Who is authorized to retrieve the media?

(6) How long will it take to retrieve the media?

(7) Where will the media be delivered?

(8) Who will restore the data from the media?

(9) What is the media-labeling scheme?

(10) How long will the backup media be retained?

(11) When the media are stored on-site, what environmental controls are provided to preserve the media?

(12) What is the appropriate backup media?

(13) What types of media readers are used at the alternate site?

d. Backup media should be stored off-site in a secure, environmentally controlled location. When selecting the off-site location, operating hours of the location, ease of accessibility to backup media, physical storage limitations, and the contract terms should be taken into account. It is important that media be retrieved on a regular basis from off-site storage and tested to ensure the backups are being performed correctly. The ITCP coordinator should refer to the BIA to assist in determining how often backup media should be tested. Each backup tape, cartridge, or disk should be uniquely labeled to ensure the required data can be identified quickly in an emergency. This requires the agency develop an effective marking and tracking strategy. One method might be to label the media by the month, day, and year that the backup was created. Other strategies can be more complex, involving multiple sets of media that are rotated as old data is either appended to or overwritten. The marking strategy should be consistent with the media retention guidelines that dictate how long the media should be stored before they are destroyed.

e. Though off-site storage of backup media enables the system to be recovered, data added or modified on the server since the previous backup could be lost during a disruption. To avoid this potential data loss, a backup strategy may need to be complemented by redundancy solutions, such as disk mirroring, redundant arrays of independent disks (RAIDs), and load balancing. These solutions are discussed below. Data from the BIA may assist the ITCP coordinator in determining the appropriate length of time for data rotation.

f. RAIDs provide disk redundancy and fault tolerance for data storage and decreases mean time between failures. A RAID is used to mask disk drive and disk controller failures. In addition, a RAID increases performance and reliability by spreading data storage across multiple disk drives, rather than a single disk. RAIDs can be implemented through hardware or software; in either case, the solution appears to the operating system as a single logical hard drive. With a RAID system, hot swappable drives can be used; that is, disk drives can be swapped without shutting down the system when a disk drive fails. RAID technology uses three data redundancy techniques:

(1) *Mirroring.* With this technique, the system writes the data simultaneously to separate hard drives or drive arrays. The advantages of mirroring are minimal downtime, simple data recovery, and increased performance in reading from the disk. If one hard drive or disk array fails, the system can operate from the working hard drive or disk array, or the system can use one disk to process a read request and another disk for a different processing request. The disadvantage of mirroring is that both drives and disk arrays are processing in the writing-to-disks function, which can hinder system performance. Mirroring has a high fault tolerance and can be implemented through a hardware RAID controller or through the operating system.

(2) *Parity.* Parity refers to a technique of determining whether data has been lost or overwritten. Parity has a lower fault tolerance than mirroring. The advantage of parity is that data can be protected without having to store a copy of the data, as is required with mirroring.

(3) *Striping.* Striping improves the performance of the hardware array controller by distributing data across all the drives. In striping, a data element is broken into multiple pieces, and a piece is distributed to each hard drive. Data transfer performance is increased using striping because the drives may access each data piece simultaneously. Striping can be implemented in bytes or blocks. Byte-level striping breaks the data into bytes and stores the bytes sequentially across the hard drives. Block-level striping breaks the data into a given-size block, and each block is distributed to a disk.

g. RAID solutions rely on mirroring, parity, and striping techniques. Currently, ten RAID levels are available, with each level providing a different configuration. RAID–1 and RAID–5 are the most popular levels for data redundancy.

(1) RAID–0 is the simplest RAID level, relying solely on striping. RAID–0 has a higher performance in read and write speeds than the other levels, but it does not provide data redundancy. Thus, RAID–0 is not recommended as a data recovery solution.

(2) RAID–1 uses mirroring to create and store identical copies on two or more drives. RAID–1 is simple and inexpensive to implement; however, 50 percent of storage space is lost because of data duplication.

(3) RAID–2 uses bit-level striping; however, the solution is not often employed because the RAID controller is expensive and difficult to implement.

(4) RAID–3 uses byte-level striping with dedicated parity. RAID–3 is an effective solution for applications handling large files; however, fault tolerance for the parity information is not provided because that parity data is stored on one drive.

(5) RAID–4 is similar to RAID–3, but it uses block-level rather than byte-level striping. The advantage of this technique is that the block size can be changed to meet the application's needs. With RAID–4, the storage space of one disk drive is lost.

(6) RAID–5 uses block-level striping and distributed parity. This solution removes the bottleneck caused by saving parity data to a single disk in RAID–3 and RAID–4. In RAID–5, parity is written across all drives along with the data. Separating the parity information block from the actual data block provides fault tolerance. If one drive fails, the data from the failed drive can be rebuilt from the data stored on the other drives in the array. Additionally, the stripe set can be changed to fit the application's needs. With RAID–5, the storage space of one disk drive is lost.

h. A RAID is an effective strategy for disk redundancy. However, redundancy for other critical server parts, such as the power supply, also should be provided. The server may be equipped with two power supplies, so that the second power supply may continue to support the server if the main power supply becomes overheated or unusable.

i. Although a second power supply can protect against hardware failure, it is not an effective preventive measure against power failure. To ensure short-term power and to protect against power fluctuations, a UPS should be installed. The UPS often provides enough backup power to enable the system to shut down gracefully. If high availability is required, consider the use of fuel cells or a gas/diesel-powered generator. The generator or fuel cell can be wired directly into the site's power system and can be configured to start automatically when a power interruption is detected.

j. Electronic vaulting and remote journaling are similar technologies that provide additional data backup capabilities, with backups made to remote tape drives over communication links. Remote journaling and electronic vaulting enable shorter recovery times and reduced data loss should the server be damaged between backups. With electronic vaulting, the system is connected to an electronic vaulting provider to allow backups to be created off-site automatically. The electronic vault could use optical disks, magnetic disks, mass storage devices, or an automated tape library as the storage devices. With this technology, data is transmitted to the electronic vault as changes occur on the servers between regular backups. These transmissions between backups are sometimes referred to as electronic journaling. With remote journaling, transaction logs or journals are transmitted to a remote location. If the server needed to be recovered, the logs or journals could be used to recover transactions, applications, or database changes that occurred after the last server backup. Remote journaling can either be conducted through batches or be communicated continuously using buffering software. Remote journaling and electronic vaulting require a dedicated off-site location to receive the transmissions. The site can be the system's hot site, off-site storage site, or another suitable location. Depending on the volume and frequency of the data transmissions, remote journaling or electronic vaulting could be conducted over a connection with limited bandwidth.

k. Server load balancing increases server and application availability. Through load balancing, traffic can be distributed dynamically across groups of servers running a common application so that no one server is overwhelmed. With this technique, a group of servers appears as a single server to the network. Load balancing systems monitor each server to determine the best path to route traffic to increase performance and availability so that one server is not overwhelmed with traffic. Load balancing can be implemented among servers within a site or among servers at different sites. Using load balancing among different sites can enable the application to continue to operate as long as one or more sites remain operational. Thus, load balancing could be a viable contingency measure depending on system availability requirements.

l. With disk replication, recovery windows are minimized because data is written to two different disks to ensure that two valid copies of the data are always available. The two disks are called the protected server (the main server) and the replicating server (the backup server). Disk replication can be implemented locally or between different locations. Two different data replication techniques are available, and each provides different capabilities at different costs to support recovery time objectives (RTOs) and recovery point objectives (RPOs). The RTO is the maximum acceptable length of time specified by the information owner that may elapse before the unavailability of the system severely affects the organization. The RPO is the point in time specified by the information owner to which data must be restored in order to resume processing. Disk replication techniques include:

(1) *Synchronous (mirroring).* This method uses a disk-to-disk copy and maintains a replica of the database or file system by applying changes to the replicating server at the same time changes are applied to the protected server. The synchronous mode can degrade performance on the protected server and should be implemented only over short physical distances where bandwidth will not restrict data transfers between servers. With synchronous mirroring, the RTO can be minutes to several hours, and the RPO may be reduced to the loss of uncommitted work. Mirroring should be used for critical applications that can accept little or no data loss.

(2) *Asynchronous (shadowing).* This technique maintains a replica of the database or file system by continuously

capturing changes to a log and applying the changes in the log to the replicating server. With asynchronous shadowing, the RTO can range from hours to a day, depending on the time that is required to implement the changes in the unapplied logs. An acceptable RPO is the last data transfer the shadowing server received. Asynchronous replication is useful over smaller bandwidth connections and longer distances where network latency could occur. As a result, shadowing helps to preserve the protected server's performance.

m. Replication solutions also can be operating system-dependent, called host-based replication, and can use both synchronous and asynchronous replication. To choose the appropriate disk replication technique and product, the ITCP coordinator should evaluate platform support, integration with other complementary products, cost, speed of deployment, performance impact, and product completeness and manageability.

n. Disk replication also can act as a load balancer, where traffic is directed to the server with the most resources available. With disk replication, the protected server sends status messages to the replicating server. If the protected server stops replicating or sends a "distress" call, the replicating machine automatically assumes the protected server's functions. If the replication ceases, a resynchronization will have to be conducted between the protected server and mirroring server before beginning the replication.

o. If the ITCP coordinator is considering implementing replication between two sites, the supporting infrastructure for the protected and replicating server also should be considered. Redundant communications paths should be provided if adequate resources are available. The ITCP coordinator should be aware of potential disadvantages of disk replication, including the possibility that a corrupted disk or data could be replicated, which could destroy the replicated copy.

p. The storage virtualization concept is the process of combining multiple physical storage devices into a logical, virtual storage device that can be centrally managed and is presented to the network applications, operating systems, and users as a single storage pool. Benefits of storage virtualization are that storage devices can be added without requiring network downtime, storage volumes from a downed server or a storage device can be reassigned, and the assigned storage for a server can be easily created, deleted, or expanded on to meet the server's requirements. Virtualization technologies can complement network-attached storage (NAS) environments. NAS environments are file-oriented and offer a common storage area for multiple servers. NAS environments are beneficial for file-server applications or storage, such as file sharing or Web and mail services. A NAS device, or server, runs from a minimal operating system and is designed to facilitate data movement. Using file-oriented protocols, any application or any client using virtually any operating system can send data to or receive data from a NAS device.

q. Virtualization technology can also complement a storage area network (SAN), which is a high-speed, high-performance network that enables computers with different operating systems to communicate with one storage device. As opposed to a NAS, a SAN provides data access in blocks and is built to handle storage and backup traffic as opposed to file-oriented traffic. A SAN can be local or remote (within a limited distance) and usually communicates with the server over a fiber channel. The SAN solution moves data storage off the LAN, thus enabling backup data to be streamed to high-speed tape drives, which does not affect network resources as distributed and centralized backup architecture does. Virtualization, NAS, and SAN all move away from client/server architecture and toward data-centric architecture. If the system manager is considering implementing a data-centric architecture, the advantages and disadvantages of the technologies and the system manager's needs of a data-centric network should be considered. The Internet Small Computer System Interface (iSCSI) is a Transmission Control Protocol/Internet Protocol (IP)-based storage networking specification that complements NAS and SAN technology. iSCSI transmits native Small Computer System Interfaces over a layer of the IP stack, which facilitates long-distance storage deployment, management, and data transfer over the IP network. iSCSI enables any storage connected to an IP network to be backed up from any point on that network. With iSCSI, storage and servers can be added at any location and not be restricted by distances, as with SAN. Figure 5–1 shows the level of server availability provided by various contingency solutions.

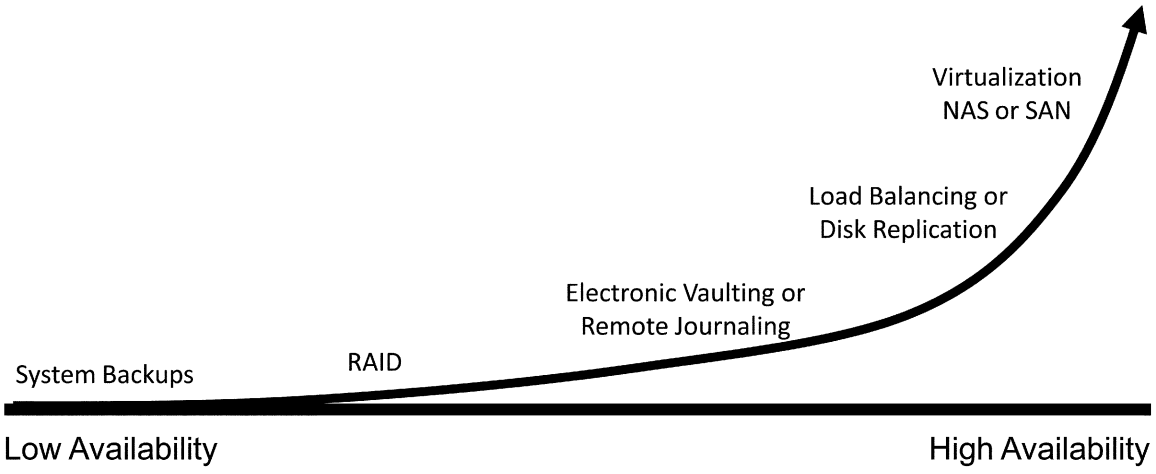


Figure 5–1. Server contingency solutions and availability

5–3. Web sites

Web sites present information to the public or authorized personnel via the World Wide Web or a private Intranet. An external Web site may also be an electronic commerce (e-commerce) portal, through which the organization may provide services over the Internet. A Web site may be used internally within an organization to provide information, such as corporate policies, human resources forms, or a phone directory to its employees. Table 5–3 provides an overview of contingency strategies for Web sites.

a. Additional Web site practices. In addition to the information presented in paragraph 5–2 several factors should be considered when determining the Web site recovery strategy. Practices for Web site contingency planning include the following measures:

(1) *Document Web site.* Document the hardware, software, and their configurations used to create and host the Web site.

(2) *Web site programming.* As with other applications, Web sites should undergo thorough testing on test servers before production. A configuration management program should be maintained, and changes should be documented appropriately. Approved versions should be recorded on CDs for easy storage.

(3) *Web site coding.* A Web site is hosted on a server that is assigned an IP address. That IP address maps to a domain name, or uniform resource locator (URL), by a domain name service (DNS). The Web site should not have IP addresses or domain names programmed into the code. If the Web site were recovered at an alternate site, the server could be assigned a different IP address. If the Web site contained hard-coded IP addresses, domain names, or drive letters, the system recovery could be delayed.

(4) *Contingency solutions coordination.* Coordinate contingency solutions with appropriate security policies and security controls. A Web site often is the entry point for a hacker getting into an organization's network. Thus, the Web server and supporting infrastructure should be protected through strong security controls. Contingency planning measures should be coordinated with these controls to ensure that security is not compromised during system recovery. Thus, the appropriate security controls and patches should be implemented on the Web sites that are rebuilt after being compromised.

(5) *Incident response procedures.* Coordinate contingency solutions with incident response procedures. Because an external Web site provides an image of the organization to the public, the organization's public image could be damaged if the Web site were defaced or taken down by a cyber attack. To reduce the consequences of such an attack, the contingency solutions listed below and in table 5–3 should be coordinated closely with incident response procedures designed to limit the impacts of a cyber incident.

(6) *Business impact analysis results.* Impacts and priorities discovered through the BIA of associated major applications and general support systems should be reviewed to determine related requirements.

Table 5–3
Web site contingency strategies

Document Web site
Code, program, and document Web site properly
Coordinate with security policies and controls
Consider contingencies of supporting infrastructure
Implement load balancing
Coordinate with incident response procedures

b. Web site contingency solutions. Web site contingency solutions should ensure the reliability and availability of the Web site and its resources. Web pages that do not change in content are considered static, whereas Web pages that change in content are called dynamic pages. Dynamic pages are a result of multiple transactions initiated from either the client, the server, or both. The content presented in dynamic pages may be stored on a server other than the Web site, such as a protected server behind a firewall. Thus, when choosing contingency solutions for a Web site, the Web site's supporting infrastructure should be considered carefully. In addition to servers, the supporting infrastructure could include the LAN hosting the Web site. Because of the number of requests Web sites could receive and process, load balancing is a popular contingency solution. Load balancing uses the cluster approach, in which Web traffic is balanced across at least two servers. Web clustering is not apparent to the user because it appears as if one server is answering the request. Therefore, if one server were to fail, traffic would be directed to the operational server. Load balancing can be accomplished through two approaches:

(1) *Domain name service.* When a user enters a URL using the Web browser, the request is directed to a DNS server that maps the URL to an IP address. The IP address is assigned to the Web server. The DNS server then directs the request to one of the clustered servers. One common DNS approach is the "round robin" method used by the Berkeley Internet Name Daemon.

(2) *Reverse proxy.* The reverse proxy approach bundles the requests of the browsers and reduces bandwidth by performing data caching. The proxy server is logically located between the client and the Web servers, where it receives client requests and forwards them to the Web servers. The server returns the response to the proxy, and the proxy forwards the response to the requesting client. With this method, one IP address is needed. To further segment traffic, the servers can be placed on different subnets to prevent a single subnet from being overloaded. In addition, logs can be collected and monitored in one location, which is the reverse proxy. The administrator also can determine the delegation configuration; therefore, if one machine crashes, the delegation configuration of the reverse proxy can be reconfigured. The result is that the crashed server will not return errors to the requesting browser.

5–4. Army Knowledge Online

a. AKO provides organizations and individuals with the ability to continue to operate through the Web (from outside of the Army network) in the event that their office computers, LANs, or their offices are not available. These capabilities can be used routinely to work from home, while on the road, during planned contingency exercises, and during ad hoc opportunities such as snow days. Routine use is the best way to exercise the skills needed during a contingency, and best tailors the information that individuals have stored on AKO to support their work. The following functions can be used to continue operations:

(1) *Push information to all members of the organization.* Groups can be prepared ahead of time and exercised for emergency notification via Web mail/email distribution. Such groups should be maintained and exercised, to include the use of recall rosters with telephone numbers. Web mail provides a redundant means of communication in the event that telecommunications networks are congested or inoperable, which can be more effective in contacting individuals who are traveling and can persist until it is checked, unlike a missed phone call. These information pushes can provide immediate instructions and direct individuals to authoritative sources for status and operating instructions.

(2) *Provide a virtual assembly area on the Web.* This allows members of an organization to individually pull information from an access-controlled Web site designated as the authoritative source for the organization. Contingency pages on AKO should be developed as part of contingency planning, prominently linked from subordinate organization AKO pages and Web sites and included as part of contingency training and exercises.

(3) *Provide Web access to Army information systems.* The AKO portal provides a growing capability to find a wide range of Web-based Army ISs, and a method of controlling access to them through the AKO login (single sign-on).

(4) *Provide Web storage of information.* Organizations and individuals can also use AKO to store work files and references, in a Web space they can make available to the Army, their select group, or to themselves. This enables the many different functional specialists in the Army to individually tailor the information available to continue their missions for their organizations in a contingency scenario.

(5) *Enable collaboration with individuals and groups.* In addition to an Armywide white pages e-mail directory, AKO provides a Web-based capability for chat and instant messaging for more real-time communication and collaboration. For more deliberate analysis, forums can be established to maintain a threaded discussion of a topic of interest, and standing forums can be used to find and collaborate with subject matter experts.

b. AKO should be incorporated into the planning, notification/activation, recovery, and reconstitution phases of contingency activities.

(1) *Planning.*

(a) Assign responsibility for establishing and maintaining policy and procedures on the use of AKO during contingencies, AKO groups for notifications, contingency pages, and training within the organization.

(b) Prepare AKO groups and contingency pages on AKO, and, as needed, on AKO-SIPRNET. Establish links from organizational AKO pages and Web sites to assist individuals (for example, new employees not yet trained or Family members) in finding the contingency site during an event.

(c) Train individuals on contingency policy and procedures, AKO capabilities, and equip them with Common Access Cards and Common Access Card reader devices for their laptops and home computers. Routine use of these capabilities is the best preparation of individuals for a contingency scenario.

(d) The better the preparation, the smoother the transition to Web-based operations. Those organizations and individuals whose mission does not require them to physically touch materiel or people could be operated as a virtual organization over AKO for a theoretically unlimited period. All organizations can use AKO to greatly improve their ability to communicate and adapt to a contingency scenario. Organizations are recommended to systematically encourage the use of these capabilities while traveling, during exercises, as part of a telecommuting program, and routinely from the office desktop.

(2) *Notification and activation.*

(a) Distribute notification messages to groups and post status and instructions to the contingency page.

(b) Distribute quick reference training materials to individuals covering the use of AKO to conduct business and communicate during a contingency scenario. Their materials may be unavailable, and specific new resources may be added.

(3) *Recovery and reconstitution.* During the recovery and reconstitution phases, Web-based operations on AKO can continue seamlessly as LAN and PC-based capabilities are reestablished. Conduct an effective after action review to determine what files and information were missing from AKO that would have assisted during the event and ensure the information is posted to AKO.

5–5. Local area networks

a. Local area networks. A LAN is owned by a single organization; it can be as small as two PCs attached to a single hub, or it may support hundreds of users and multiple servers. An overview of contingency strategies for LANs is provided in table 5–4. An example of a LAN is presented in figure 5–2. Several topologies are possible when designing a LAN. A protocol is a set of rules used between end points that govern a connection. The protocol determines how the sending and receiving nodes format the data packet. One of the main network standards, ethernet (both 10/100 and 10 gigabit), may be implemented on a LAN, in addition to less common standards such as token ring, asynchronous transfer mode (ATM), or fiber distributed data interface. LANs can also be implemented in two main architectures:

(1) *Peer-to-peer*. Each node has equivalent capabilities and responsibilities. For example, five PCs can be networked through a single hub to share data.

(2) *Client/server*. Each node on the network is either a client or a server. A client can be a PC or a printer where a client relies on a server for resources.

Table 5–4
Local area network contingency strategies

Document LAN
Coordinate with vendors
Coordinate with security policies and controls
Identify single points of failure
Implement redundancy in critical system components
Monitor LAN

Table 5–4
Local area network contingency strategies—Continued

Integrate remote access and wireless LAN technology

b. Local area networks topology. A LAN's topology (several examples of which are described in fig 5–3), protocol, architecture, and nodes will vary depending on the organization. Thus, contingency solutions for each organization will be different.

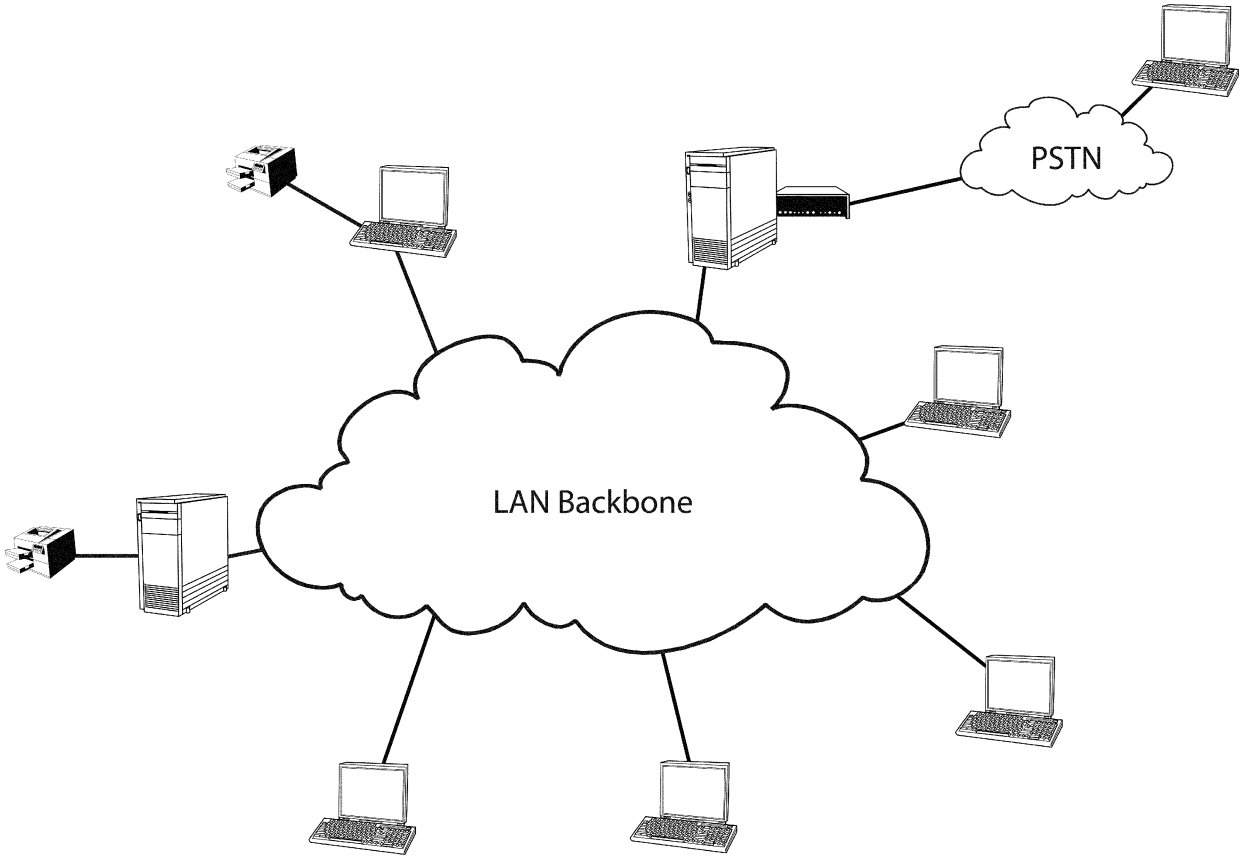


Figure 5–2. Sample local area network

c. Contingency considerations. When developing the LAN recovery strategy, follow the information presented earlier regarding desktops, servers, and Web sites. In addition, the following practices should be considered:

(1) *Local area network documentation.* The physical and logical LAN diagram should be up to date. The physical diagram should display the physical layout of the facility that houses the LAN and cable jack numbers should be documented on the physical diagram. The logical diagram should present the LAN and its nodes. Network discovery software can provide an accurate picture of the LAN. Both diagrams help recovery personnel to restore LAN services more quickly.

(2) *System configuration and vendor information documentation.* Document configurations of network connective devices that facilitate LAN communication (for example, switches, bridges, and hubs) to ease recovery. Vendors and their contact information should be documented in the ITCP to provide for prompt hardware and software re-supply.

(3) *Coordinate with security policies and security controls.* LAN contingency solution(s) should be coordinated with network security policies to protect against threats that could disrupt the network. Therefore, in choosing the appropriate technical LAN contingency solution(s), similar security controls and security-related activities (for example, risk assessment, vulnerability scanning) in the production systems should be implemented in the contingency solution(s) to

ensure that, during a network disruption, executing the technical contingency solution(s) does not compromise or disclose sensitive data.

(4) *Results of the business impact analysis.* Impacts and priorities discovered through the BIA of associated major applications and general support systems should be reviewed to determine LAN recovery priorities.

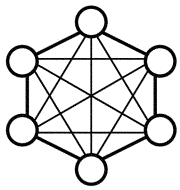
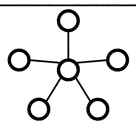
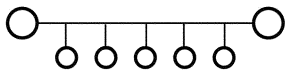
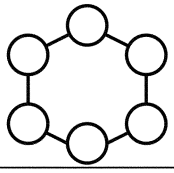
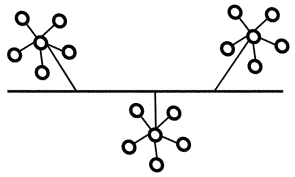
Topology	Diagram
Mesh Networked components are connected with many redundant interconnections between network nodes. In a true mesh topology, every node has a connection to every other node in the network.	
Star All nodes are connected to a central hub.	
Bus All nodes are connected to a central cable, called the bus or backbone.	
Ring All nodes are connected to one another in the shape of a closed loop so that each node is connected directly to two other nodes, one on either side of it.	
Tree A tree is a hybrid topology where a linear bus backbone connects star-configured networks.	

Figure 5–3. Local area network topologies

d. Contingency solutions. When developing the LAN ITCP, identify single points of failure that affect critical systems or processes outlined in the BIA. This analysis could include threats to the cabling system, such as cable cuts, electromagnetic and radio frequency interference, and damage resulting from fire, water, and other hazards. Standard Army IT designs call for flood wiring to accommodate adds, moves, and changes. Current Army standards call for fiber backbone cable (using high-speed fiber optic cabling) that provides spare capacity.

(1) Often, it is not cost-effective to run duplicate cables to each computer jack. However, each desktop jack usually is equipped with at least one phone jack and computer jack. When cables are installed, an organization may choose to install an extra data or phone jack every few drops; then, if a problem does occur in a cable run, an extra jack within a short distance would be available as backup. In this case, temporary cable can be run from the desktop to the extra jack to provide connectivity for the desktop until a new cable can be run to the problem jack. Also, if the phone system's connectivity block is located in the same location as the backbone hubs, a phone jack can be converted easily into a data jack, if the phone jack provides the appropriate bandwidth.

(2) Contingency planning should also consider network connecting devices, such as hubs, switches, routers, and bridges. The BIA should characterize the roles that each device serves in the network, and a contingency solution should be developed for each device based on its BIA criticality. As an example of a contingency strategy for network connecting devices, redundant intelligent network routers may be installed in a network, enabling a router to assume the full traffic workload if the other router failed. A more cost-effective approach would be to include structured

cabling systems according to Army standards that allow for spare capacity and flexibility in the horizontal cabling. Also, planners should take into consideration the need for power supply redundancies for voice over IP systems.

(3) Remote access is a service provided by servers and devices on the LAN. Remote access provides a convenience for users working off-site or allows for a means for servers and devices to communicate between sites. Remote access can be conducted through various methods, including dialup access and virtual private networks (VPN). If an emergency or serious system disruption occurs, remote access may serve as an important contingency capability by providing access to organization-wide data for recovery teams or users from another location. If remote access is established as a contingency strategy, data bandwidth requirements should be identified and used to scale the remote access solution. Additionally, security controls such as one-time passwords and data encryption should be implemented if the communications contains sensitive information.

(4) Wireless LANs and multiple area networks can serve as an effective contingency solution to restore network services following a wired LAN disruption. Wireless networks do not require the cabling infrastructure of conventional LANs; therefore, they may be installed quickly as an interim or permanent solution. However, wireless networks broadcast the data over a radio signal, enabling the data to be intercepted. When implementing a wireless network, security controls such as data encryption must be implemented in accordance with AR 25–2 if the communications traffic contains sensitive information.

(5) To reduce the effects of a LAN disruption through prompt detection, monitoring software can be installed. The monitoring software issues an alert if a node begins to fail or is not responding. The monitoring software can facilitate troubleshooting and often provides the administrator with a warning before users and other nodes notice problems. Many types of monitoring software may be configured to send an electronic page to a designated individual automatically when a system parameter falls out of its specification.

5–6. Wide area networks

a. Addition to connecting local area networks. In addition to connecting LANs, a WAN also can connect to another WAN, or it can connect a LAN to the internet. A sample WAN diagram is found in figure 5–4 and an overview of WAN contingency strategies is provided in table 5–5. Types of WAN communication links include the following methods:

(1) *Dialup.* Dialup connections over modems can provide minimal data transfer over a nonpermanent connection. The speed will depend on the modems used, up to 56 kilobits per second (Kbps).

(2) *Integrated services digital network.* Integrated services digital network (ISDN) is an international communications standard for sending voice, video, and data over digital or standard telephone wires. ISDN supports data transfer rates of 64 or 128 Kbps.

(3) *T–1.* T–1 is a dedicated phone connection supporting data rates of 1.544 megabits per second (Mbps). A T–1 line consists of 24 individual 64 Kbps channels, and each channel can be configured to carry voice or data signals. Fractional T–1 access also can be provided when multiples of 64 Kbps lines are required.

(4) *T–3.* T–3 is a dedicated phone connection supporting data rates of about 43 Mbps. A T–3 line consists of 672 individual channels, each of which supports 64 Kbps.

(5) *Frame relay.* Frame relay is a packet-switching protocol for connecting devices on a WAN. In frame relay, data is routed over virtual circuits. Frame relay networks support data transfer rates at T–1 and T–3 speeds.

(6) *Asynchronous transfer mode.* ATM is a network technology that transfers data at high speeds using packets of fixed size. Implementations of ATM support data transfer rates of from 25 to 622 Mbps and provides guaranteed throughput.

(7) *Synchronous optical network.* Synchronous optical network is the standard for synchronous data transmission on optical media. Synchronous optical network supports gigabit transmission rates.

(8) *Wireless.* A wireless LAN bridge can connect multiple LANs to form a WAN. Wireless supports distances of 20 to 30 miles with a direct line of sight.

(9) *Virtual private network.* A VPN is an encrypted channel between nodes on the Internet. While a VPN is not a WAN, it is a technology that uses WANs to provide a virtual network for users in various locations.

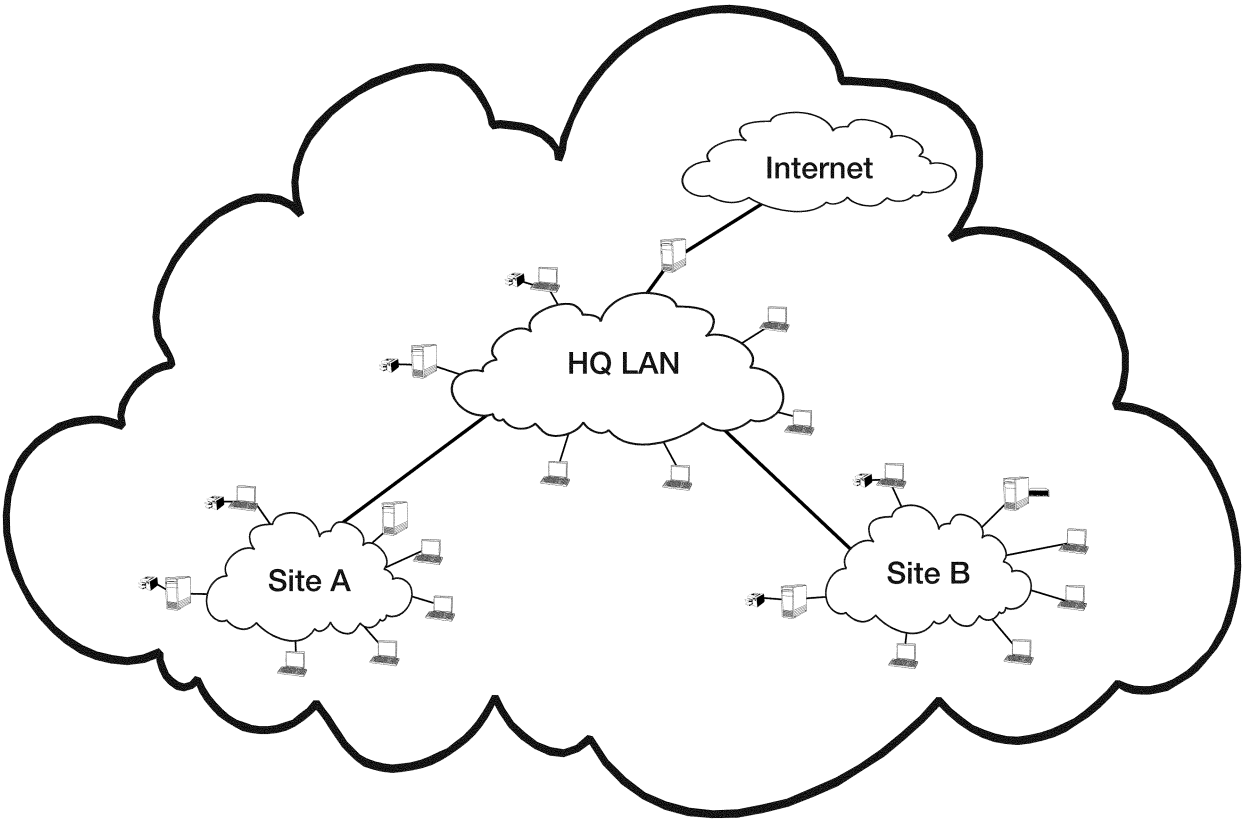


Figure 5–4. Wide area networks

b. Contingency considerations. WAN contingency considerations should enhance the ability of recovery personnel to restore WAN services after a disruption. The practices listed below complement WAN recovery strategies to create a more comprehensive WAN contingency capability.

(1) *Document wide area network.* The WAN architecture diagram should be kept up to date and should identify network connecting devices, unit addresses (IP addresses), and types of communication links and vendors.

(2) *Document systems configurations and vendors.* Document configurations of media access unit devices that facilitate WAN communication to ease recovery. The ITCP should include a vendor list to enable rapid replacement of hardware, software, and other WAN components following a disruption. The plan also should document the communications providers, including POC and contract information.

(3) *Coordinate with security policies and security controls.* WAN contingency solution(s) should be coordinated with network security policies to protect against threats that could compromise network availability. Thus, in choosing the appropriate technical contingency solution(s), similar security controls and security-related activities (for example, assessment or vulnerability scanning) in the production environment should be implemented in the contingency solution(s) to ensure that, during a disruption to WAN connectivity, executing the technical contingency solution(s) does not compromise or disclose sensitive data.

(4) *Use results from the business impact analysis.* Impacts and priorities discovered through the BIA of associated major applications and general support systems should be reviewed to determine related requirements.

Table 5–5
Wide area network contingency strategies

Document WAN
Coordinate with vendors
Coordinate with security policies and controls
Identify single points of failure
Implement redundancy in critical system components
Institute SLAs

c. Contingency solutions. WAN contingency solutions include all of the measures discussed for PCs, servers, Web sites, and LANs. In addition, WAN contingency planning should consider the communications links that connect the disparate LANs. WAN contingency strategies are influenced by the type of data routed on the network. A WAN that hosts a mission-critical distributed system may require a more robust recovery strategy than a WAN that connects multiple LANs for simple resource sharing purposes. Organizations should consider the following contingency solutions for ensuring WAN availability:

(1) *Redundant communications links.* Redundant communications links usually are necessary when the network processes critical data. The redundant links could be the same type, such as two T–1 connections, or the backup link could provide reduced bandwidth to accommodate only critical transmissions in a contingency situation. For example, an ISDN line could be used as a contingency communications link for a primary T–1 connection. If redundant links are used, the ITCP coordinator should ensure the links have physical separation and do not follow the same path; otherwise, a single incident, such as a cable cut, could disrupt both links.

(2) *Redundant network service providers.* If 100 percent data availability is required, redundant communications links can be provided through multiple network service providers (NSPs). If this solution is chosen, the manager should ensure the NSPs do not share common facilities at any point, including building entries or demarcations.

(3) *Redundant network connecting devices.* Duplicate network connecting devices, such as routers, switches, and firewalls, can create high availability at the LAN interfaces and provide redundancy if one device fails. Duplicate devices also provide load balancing in routing traffic.

(4) *Redundancy from network service provider or internet service provider.* ITCP coordinators should consult with the selected NSP or Internet service provider (ISP) to assess the robustness and reliability within their core networks (for example, redundant network-connecting devices and power protection). The ITCP coordinator should also be aware of NIPRNET connectivity to supported camps, posts, and stations.

d. Further redundancy. To provide further redundancy, independent Internet connections may be established from two geographically separated LANs. If one connection were to fail, Internet traffic could be routed through the remaining connection. However, this strategy highlights the balance that should be maintained between security and availability. Multiple Internet connections increase a network's vulnerability to hackers. Therefore, as emphasized previously, contingency strategies should be weighed against security considerations at all times.

e. Recovery. SLAs can facilitate prompt recovery following software or hardware problems associated with the network. A SLA also may be developed with the NSP or ISP to guarantee the desired network availability and establish tariffs if the vendor's network is unavailable. If the NSP or ISP is contracted to provide network-connecting devices, such as routers, the availability of these devices should be included in the SLA.

5–7. Distributed systems

Distributed systems are implemented in environments in which clients and users are widely dispersed. These systems rely on LAN and WAN resources to facilitate user access and the elements comprising the distributed system require synchronization and coordination to prevent disruptions and processing errors. A common form of distributed systems is a large database management system that supports agency-wide business functions in multiple geographic locations. In this type of application, data is replicated among servers at each location, and users access the system from their local server. An overview of contingency strategies for distributed systems is provided in table 5–6.

a. Distributed system. A distributed system is an interconnected set of multiple autonomous processing elements, configured to exchange and process data to complete a single business function. To the user, a distributed system appears to be a single source. Distributed systems use the client-server relationship model to make the application more accessible to users in different locations.

Table 5–6
Distributed system contingency strategies

Standardize components
Document system
Coordinate with vendors
Coordinate with security policies and controls
Consider server contingency solution
Consider LAN contingency solution
Consider WAN contingency solution

b. Contingency considerations. Contingency considerations for the distributed system draw on the concepts discussed for the previous platforms. Because the distributed system relies extensively on local and wide area network connectivity, distributed system contingency measures are similar to those discussed for LANs and WANs.

(1) *Standardize hardware, software, and peripherals.* System recovery may be expedited if hardware, software, and peripherals are standardized throughout the distributed system. Recovery costs may be reduced because standard configurations may be designated and resources may be shared. Standardized components also reduce system maintenance across the organization.

(2) *Document systems configurations and vendors.* Document the distributed system's architecture and the configurations of its various components. In addition, the ITCP should identify vendors and model specifications to facilitate rapid equipment replacement after a disruption.

(3) *Coordinate with security policies and security controls.* Distributed system contingency solution(s) should be coordinated with network security policies where similar security controls and security-related activities (for example, risk assessment or vulnerability scanning) in the production environment should be implemented in the contingency solution(s) to ensure that, during a system disruption, executing the technical contingency solution(s) does not compromise or disclose sensitive data.

(4) *Use results from the business impact analysis.* Impacts and priorities discovered through the BIA of associated LAN and/or WAN should be reviewed to determine recovery requirements and priorities.

c. Contingency solutions. Because a distributed system spans multiple locations, risks to the system and its supporting infrastructure should be analyzed thoroughly in the BIA process. As discussed above, distributed system contingency strategies typically reflect the system's reliance on LAN and WAN availability. Contingency solutions may be built into the distributed system during design and implementation. A distributed system, for example, may be constructed so that all data resides in one location (such as the organization's headquarters) and is replicated to the local sites. Changes at local sites could be replicated back to headquarters. If data is replicated to the local sites as read-only, the data in the distributed system is backed up at each local site. This means that if the headquarters server were to fail, data could still be accessed at the local sites over the WAN. Conversely, if data were uploaded hourly from local sites to the headquarters' site, then the headquarters' server would act as a backup for the local servers. As the example above illustrates, the distributed system typically provides some inherent level of redundancy that can be incorporated in the contingency strategy. For example, consider a critical system that is distributed between an agency headquarters and a small office. Assuming data is replicated at both sites, a cost-effective recovery strategy may be to establish a reciprocal agreement between the two sites. Under this agreement, in the event of a disruption at one office, essential personnel would relocate to the other office to continue to process system functions. This strategy could save significant contingency costs by avoiding the need to procure and equip alternate sites. Based on this fact, when developing a distributed system contingency strategy, the following technologies should be considered because they were addressed for LANs and WANs:

(1) System backups.
(2) RAID.
(3) Redundancy of critical system components.
(4) Electronic vaulting and remote journaling.
(5) Disk replication.
(6) Virtualization, NAS, or SAN.
(7) Remote access.
(8) Wireless networks.
(9) LAN cabling system redundancy.

(10) WAN communication link redundancy.

5–8. Mainframe systems

Unlike the client/server architecture, the mainframe architecture is centralized. The clients that access the mainframe are "dumb" terminals with no processing capabilities. The dumb terminals accept output only from the mainframe. However, PCs also can access a mainframe by using terminal emulation software. An overview of contingency strategies for mainframe systems in provided in table 5–7.

a. Mainframes. A mainframe is a multi-user computer designed to meet the computing needs of a large organization. The term was created to describe the large central computers developed in the late 1950s and 1960s to process bulk accounting and information management functions. Mainframe systems store all data in a central location rather than dispersing data among multiple machines, as with distributed systems.

Table 5–7
Mainframe contingency strategies

Back up data and store offsite
Document system
Coordinate with vendors
Coordinate with security policies and controls
Implement redundancy and fault tolerance in critical system components
Consider hot site or reciprocal agreement
Institute vendor SLAs
Replicate data
Implement storage solutions
Use uninterruptible power supplies

b. Contingency considerations. Although the mainframe computer is large and more powerful than the platforms discussed previously, it shares many of the same contingency requirements. Because a mainframe uses a centralized architecture, the mainframe does not have the inherent redundancy that a distributed system or network provides. As a result, mainframe availability and data backups are critical. The following measures should be considered when determining mainframe contingency requirements:

(1) *Store backup media off-site.* Backup media should be labeled, logged, and stored offsite in a secure, environmentally controlled facility. The storage facility should be located far enough away from the original site to reduce the likelihood that both sites would be affected by the same event.

(2) *Document system configurations and vendors.* Maintaining detailed records of system configurations enhances system recovery capabilities. In addition, vendors that supply essential hardware, software, and other components should be identified in the ITCP.

(3) *Coordinate with network security policy and system security controls.* Mainframe contingency solutions should be coordinated with network security policies, such as stringent access controls. Network security controls can help protect against attacks that could compromise the mainframe's availability.

(4) *Utilize results from the business impact analysis.* Impacts and priorities discovered through the BIA of associated major applications and general support systems should be reviewed to determine recovery requirements and priorities.

c. Contingency solutions. Mainframes require different contingency strategies from distributed systems because data is stored in a single location. Contingency strategies should emphasize the mainframe's data storage capabilities and underlying architecture. Redundant system components are critical to ensure that a failure of a system component, such as a power supply, does not cause a system failure. UPS and power monitoring and management systems also should be used to ensure power fluctuation will not affect the mainframe. Because mainframes typically process large, critical applications, a long-term backup power solution may be needed. A gas or diesel generator can ensure that mainframe processing is not interrupted by a power outage.

(1) Disk redundancy can be provided for the direct access storage devices by implementing a RAID solution.

(2) A contingency strategy is to have a replacement system available at an alternate warm or hot site because each

mainframe architecture is unique and centralized. However, backup mainframe platforms are very costly to purchase and maintain so many agencies share commercial systems. Also, agencies typically maintain vendor support contracts to repair the damaged unit. However, vendor support alone may not restore system functions within the allowable outage time. In all cases, vendor SLAs should be kept up to date and reviewed to ensure the vendor provides adequate support to meet system availability requirements.

(3) Mainframes should be backed up regularly and backup media should be stored offsite. Backup and retention schedules should be based on the criticality of the data being processed and the frequency the data is modified. As with servers, remote journaling or electronic vaulting to the alternate site could be an effective technical contingency solution. In addition, disk replication, virtualization, or NAS or SAN technologies that replicate various platforms to one replicating server could be used in some cases.

5–9. Contingency strategy summary

A variety of actions should be undertaken to prepare for and recover from contingency situations. A summary is provided in table 5–8. The boxes marked with an X suggest what actions might be prudent for the system attributed to the column.

Table 5–8
Contingency strategy summary

	Desktop computer/ portable system	Server	Web site	Local area network	Wide area network	Distributed system	Mainframe system
Contingency consideration							
Document system, configurations, and vendor information	X	X	X	X	X	X	X
Encourage individuals to back up data	X						
Code, program, and document properly			X				
Coordinate contingency solution with security policy	X	X	X	X	X	X	X
Coordinate contingency solution with system security controls	X	X	X	X	X	X	X
Consider contingencies of supporting infrastructure			X			X	
Consider hot site and reciprocal agreements							X
Coordinate with incident response procedures			X				
Coordinate with vendors				X	X	X	X
Institute vendor SLAs					X		X
Provide guidance on saving data on personal computers	X						
Standardize hardware, software, and peripherals	X	X				X	
Store backup media offsite	X	X					X
Store software offsite	X	X					
Contingency solution							
Back up system, applications, and/or data	X	X					
Ensure interoperability among components	X	X					
Identify single points of failure				X	X		

Table 5–8
Contingency strategy summary—Continued

	Desktop computer/ portable system	Server	Web site	Local area network	Wide area network	Distributed system	Mainframe system
Image disks	X						
Implement fault tolerance in critical components		X					X
Implement load balancing		X	X				
Implement redundancy in critical components	X	X		X	X		X
Implement storage solutions		X					X
Integrate remote access and wireless technologies				X			
Monitor				X			
Replicate data		X					X
Use alternate hard drives	X						
Use uninterruptible power supplies	X	X					X

Appendix A
References

Section I
Required Publications

AR 25–1
Army Knowledge Management and Information Technology Management (Cited in paras 1–1, 1–7, 2–2, 3–8*b*, 3–11*b*.)

AR 25–2
Information Assurance (Cited in paras 1–1, 1–5*a*, 1–6*a*, 3–1*d*, 3–8*b*, 3–11*b*, 5–5*d*(4).)

AR 25–50
Preparing and Managing Correspondence (Cited in para 4–1*a*.)

AR 70–1
Army Acquisition Policy (Cited in paras 1–1, 1–7d, 3–1*b*.)

AR 70–75
Survivability of Army Personnel and Materiel (Cited in paras 1–7d, 3–1*b*.)

AR 500–3
Army Continuity of Operations Program Policy and Planning (Cited in paras 1–1, 1–4, 2–6, 3–2*c*, 3–14.)

FM 5–0
The Operations Process (Incl C1) (Cited in paras 3–1, 4–1, 4–2.)

FM 5–19
Composite Risk Management (Cited in paras 2–8, 3–4.)

CJCSM 3122.05
Operating Procedures for Joint Operation Planning and Execution System (JOPES) — Information Systems (IS) Governance, 15 Dec 2011 (Cited in para 4–1.) (Available at http://www.dtic.mil.)

Section II
Related Publications
For all references that are United States Code, they can be found at http://uscode.house.gov/download/ascii.shtml. DOD directives and instructions are available at http://www.dtic.mil/whs/directives/.

AR 380–5
Department of the Army Information Security Program

DOD Memorandum
Federal Information Security Management Act (FISMA) Guidance - Fiscal Year (FY) 08

DOD Memorandum, dated 2 May 2009
LandWarNet - Global Network Enterprise Construct Strategy Implementation

DODD 3020.26
Department of Defense Continuity Programs

DODD 8500.01E
Information Assurance (IA)

DODI 3020.42
Defense Continuity Plan Development

DODI 8500.2
Information Assurance (IA) Implementation

Federal Executive Branch Continuity of Operations, July 1999
Federal Information Security Management Act of 2002 Title III of P.L. 107–347

Federal Preparedness Circular 65
Federal Executive Branch Continuity of Operations (Available at http://www.gsa.gov/.)

NIST SP 800–18
Guide for Developing Security Plans for Federal Information Systems (Available at http://csrc.nist.gov/.)

NIST SP 800–34
Contingency Planning Guide for Information Technology Systems (Available at http://csrc.nist.gov/.)

NIST SP 800–53 Rev. 4
Security and Privacy Controls for Federal Information Systems and Organizations (Available at http://csrc.nist.gov/.)

FCD 1
Federal Continuity Directive 1

FIPS Publication 199
Standards for Security Categorization of Federal Information and Information Systems (Available at http://csrc.nist.gov/.)

OMB Circular A–130
Management of Federal Information Resources (Available at http://www.whitehouse.gov/.)

P.L. 104–106
The National Defense Authorization Act for FY 1996, Information Technology Management (Clinger-Cohen Act)

P.L. 104–191
Health Insurance Portability and Accountability Act of 1996

P.L. 106–65
The National Defense Authorization Act for FY 2000

P.L. 107–347
The E–Government Act of 2002

10 USC 2224
Defense Information Assurance Program

40 USC 3
Organization of General Services Administration

40 USC 111
General

Section III
Prescribed Forms
This section contains no entries.

Section IV
Referenced Forms
Unless otherwise indicated, DA forms are available on the Army Publishing Directorate (APD) Web site (http://www.apd.army.mil).

DA Form 2028
Recommended Changes to Publications and Blank Forms

DA Form 7566
Composite Risk Management Worksheet

Appendix B
Operations Plan/Operation Order and Contingency Plan

B–1. Operations Plan
An OPLAN is any plan, except the Single Integrated Operations Plan, for the conduct of military operations in a hostile environment prepared by the commander of a unified or specified command in response to a requirement established by the Joint Chiefs of Staff. OPLANS are prepared in either complete or concept format.

B–2. Operations Plan in complete format
An OPLAN in complete format is an operation plan for the conduct of Joint operations that can be used as a basis for development of an OPORD. Complete plans include deployment/employment phases, as appropriate. An OPLAN in concept format is an operation plan in an abbreviated format that would require considerable expansion or alteration to convert it into an OPLAN or OPORD. For a sample guide of an annotated OPLAN and OPORD, see FM 5-0.

Glossary

Section I
Abbreviations

AKO
Army Knowledge Online

APC
area processing center

APMS
Army Portfolio Management Solution

AR
Army regulation

ATM
asynchronous transfer mode

AITR
Army Information Technology Registry

BIA
business impact analysis

CD
compact disc

CJCSM
Chairman of the Joint Chiefs of Staff Memorandums

CIO
Chief Information Officer

CONOPS
concept of operations

COOP
continuity of operations

CRM
composite risk management

DA
Department of the Army

DNS
domain name service

DOD
Department of Defense

DODD
Department of Defense directive

DODI
Department of Defense instruction

DVD
digital video disk

FCD
Federal Continuity Directive

FM
field manual

FIPS
Federal Information Processing Standards

FISMA
Federal Information Security Management Act of 2002

IA
information assurance

IP
internet protocol

IS
Information System

ISDN
integrated services digital network

ISP
internet service provider

IT
information technology

ITCP
Information Technology Contingency Plan

Kbps
kilobytes per second

LAN
local area network

MAC
mission assurance category

Mbps
megabits per second

MC
mission critical

ME
mission essential

MEF
mission essential function

NAS
network-attached storage

NEC
network enterprise center

NCS
National Communications System

NIPRNET
non-secure internet protocol router network

NIST
National Institute of Standards and Technology

NSP
network service provider

OPLAN
operations plan

OPORD
operations order

Pam
pamphlet

PC
personal computer

PEO
program executive officer

PM
program manager

POC
point of contact

RAID
redundant array of independent disks

RPO
recovery point objective

RTO
recovery time objective

SAN
storage area network

SIPRNET
secure internet protocol router network

SLA
service level agreement

SO
system owner

SP
Special Publication

UPS
uninterruptible power supply

URL
uniform resource locator

USC
United States Code

VPN
virtual private network

WAN
wide area network

Section II
Terms

Alternate site
A location to recover and perform system operations for an extended period in the event of an ITCP implementation. In general, three types of alternate sites are available: (1) A dedicated site owned or operated by the organization; (2) A site reserved via reciprocal agreement or memorandum of agreement with an internal or external entity; (3) A commercially leased facility.

Business continuity plan
The business continuity plan focuses on sustaining an organization's business functions during and after a disruption. IT systems are considered in the business continuity plan in terms of their support to the business processes.

Business impact analysis
An analysis of IT system's requirements, processes, and interdependencies used to characterize system contingency requirements and priorities in the event of a significant disruption.

Business recovery plan
The business recovery plan, also known as the business resumption plan, addresses the restoration of business processes after an emergency but, unlike the business recovery plan, does not include procedures for to ensure the continuity of critical processes throughout the emergency or disruption.

Cold site
These sites typically consist of a facility with adequate space and infrastructure (electric power, telecommunications connections, and environmental controls) to support the IT system. The space may have raised floors and other attributes suited for IT operations. The site does not contain IT equipment and usually does not contain office automation equipment, such as telephones, facsimile machines, or copiers. The organization using the cold site is responsible for providing and installing necessary equipment and telecommunications capabilities.

Command and control
Exercise of authority and direction by a properly designated commander over assigned forces in the accomplishment of the mission. These functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures that are employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission.

Concept of operations
A verbal or graphic statement, in broad outline, of a commander's assumptions or intent in regard to an operation or series of operations. The concept of operations frequently is embodied in campaign plans and operation plans; in the latter case, particularly when the plans cover a series of connected operations to be carried out simultaneously or in succession. The concept is designed to give an overall picture of the operation. It is included primarily for additional clarity of purpose. Also called commander's concept or CONOPS.

Contingency planning coordinator
The person with the responsibility for the overall contingency planning process and is typically a functional or resource manager within the agency.

Continuity of operation
The level in which there is a continuous commitment in the conduct of functions, tasks, or duties necessary to

accomplish a military action or mission in carrying out national military strategy. It includes the functions and duties performed by the commander, his or her staff, and others acting under the authority and direction of the commander.

Continuity of operation plan
A plan providing procedures and capabilities to sustain an organization's essential strategic functions at an alternate site for up to 30 days.

Continuity of support/information technology contingency plan
Plans for general support systems and contingency plans for major applications. Because an information technology contingency plan should be developed for each major application and general support system, multiple contingency plans may be maintained within the organization's business continuity plan.

Differential backup
A differential backup stores files that were created or modified since the last full backup.

Disaster recovery planning
A disaster recovery plan applies to major, usually catastrophic, events that deny access to the normal facility for an extended period. Frequently, disaster recovery planning refers to an IT-focused plan designed to restore operability of the target systems, applications, and an information technology contingency plan; however, the disaster recovery planning is narrower in scope and does not address minor disruptions that do not require relocation.

Electronic vaulting
This technology provides additional data backup capabilities, with backups made to remote tape drives over communication links. Electronic vaulting enables shorter recovery times and reduced data loss should the server be damaged between backups. The system is connected to an electronic vaulting provider to allow backups to be created off-site automatically. With this technology, data is transmitted to the electronic vault as changes occur on the servers between regular backups. These transmissions between backups are sometimes referred to as electronic journaling. (See also remote journaling.)

Full backup
A full backup captures all files on the disk or within the folder selected for backup. Because all backed-up files were recorded to a single media or media set, locating a particular file or group of files is simple. However, the time required to perform a full backup can be lengthy. In addition, full backups of files that do not change frequently (such as system files) could lead to excessive, unnecessary media storage requirements.

Hot site
Hot sites are office spaces appropriately sized to support system requirements and configured with the necessary system hardware, supporting infrastructure, and support personnel. Hot sites are typically staffed 24 hours a day, 7 days a week. Hot site personnel begin to prepare for the system arrival as soon as they are notified that the contingency plan has been activated.

Incremental backup
An incremental backup captures files that were created or changed since the last backup, regardless of backup type. Incremental backups afford more efficient use of storage media, and backup times are reduced. However, to recover a system from an incremental backup, media from different backup operations may be required. For example, consider a case in which a directory needed to be recovered. If the last full backup was performed three days prior and one file had changed each day, then the media for the full backup and for each day's incremental backups would be needed to restore the entire directory.

Information system
The organized collection, processing, transmission, and dissemination of information in accordance with defined procedures, whether automated or manual. For the purposes of APMS–AITR, the terms "application" and "information system" are used synonymously - a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of information. The application of IT to solve a business or operational (tactical) problem creates an information system.

Internet backup/online backup
Internet backup, or online backup, is a strategy that allows PC users to back up data to a remote location over the Internet. A utility is installed onto the PC that allows the user to schedule backups, select files and folders to be backed

up, and establish an "archiving" scheme to prevent files from being overwritten. Data can be encrypted for transmission; however, this will impede the data transfer speed over a modem connection. The advantage of Internet Backup is that the user is not required to purchase data backup hardware or media.

Information technology contingency planning policy statement
A formal organization policy that provides the authority and guidance necessary to develop an effective contingency plan.

Mirrored site
Mirrored sites are fully redundant facilities with full, real-time information mirroring. Mirrored sites are identical to the primary site in all technical respects. These sites provide the highest degree of availability because the data is processed and stored at the primary and alternate site simultaneously. These sites typically are designed, built, operated, and maintained by the organization.

Mission essential functions
MEFs are those functions that enable the installation NEC to provide vital services and sustain the post's IT infrastructure in an emergency. Any function that is vital to the continuation of operations of the organization or agency. These functions include those required by statute or executive order, and other functions deemed essential by the head of each organization. MEFs are those continuing activities that must be performed without interruption to execute critical Army missions. MEFs may be prioritized, which allows for a graduated response and relocation to the ERFs with minimum interruptions to operations during a national/local emergency or during normal operations.

Mobile site
Mobile sites are self-contained, transportable shells custom-fitted with specific telecommunications and IT equipment necessary to meet system requirements. These are available for lease through commercial vendors. The facility often is contained in a tractor-trailer and may be driven to and setup at the desired alternate location. In most cases, to be a viable recovery solution, mobile sites should be designed in advance with the vendor, and an SLA should be signed between the two parties. This is necessary because the time required to configure the mobile site can be extensive, and without prior coordination, the time to deliver the mobile site may exceed the system's allowable outage time.

Notification/activation phase
This phase defines the initial actions taken once a system disruption or emergency has been detected or appears to be imminent. This phase includes activities to notify recovery personnel, assess system damage, and implement the plan.

Operations order
States how the unit is organized for the operation and gives who is the main effort. The leader sufficiently weighs the main effort for each mission to ensure success.

Operations plan
An OPLAN is any plan for the conduct of military operations in a hostile environment prepared by the commander of a unified or specified command in response to a requirement established by the Joint Chiefs of Staff. Operation plans are prepared in either complete or concept format. An operation plan in complete format is an operation plan for the conduct of Joint operations that can be used as a basis for development of an OPORD. Complete plans include deployment/employment phases, as appropriate. An operation plan in concept format is an operation plan in an abbreviated format that would require considerable expansion or alteration to convert it into an OPLAN or OPORD.

Operations security
The process of denying adversaries information about friendly capabilities and intentions by identifying, controlling, and protecting indicators associated with planning and conducting military operations and other activities.

Parity
Parity refers to a technique of determining whether data has been lost or overwritten. Parity has a lower fault tolerance than mirroring. The advantage of parity is that data can be protected without having to store a copy of the data, as is required with mirroring.

Potential impact category
Security categories for both information and information systems. The security categories are based on the potential impact on an organization should certain events occur which jeopardize the information and information systems needed by the organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals

Recovery phase
The Recovery phase is the segment of the information technology contingency plan in which activities focus on contingency measures to execute temporary IT processing capabilities, repair damage to the original system, and restore operational capabilities at the original or new facility.

Recovery point objective
The RPO is the point in time in which data must be restored in order to resume processing.

Recovery time objective
The RTO is the maximum acceptable length of time that elapses before the unavailability of the system severely affects the organization.

Redundant arrays of independent disks
RAID provides disk redundancy and fault tolerance for data storage and decreases mean time between failures. RAID is used to mask disk drive and disk controller failures. In addition, RAID increases performance and reliability by spreading data storage across multiple disk drives, rather than a single disk. RAID can be implemented through hardware or software; in either case, the solution appears to the operating system as a single logical hard drive. With a RAID system, hot swappable drives can be used-that is, disk drives can be swapped without shutting down the system when a disk drive fails.

Remote journaling
This technology provides additional data backup capabilities, with backups made to remote tape drives over communication links. With remote journaling, transaction logs or journals are transmitted to a remote location. If the server needed to be recovered, the logs or journals could be used to recover transactions, applications, or database changes that occurred after the last server backup. Remote journaling can either be conducted through batches or be communicated continuously using buffering software. Remote journaling and electronic vaulting require a dedicated off-site location to receive the transmissions. The site can be the system's hot site, off-site storage site, or another suitable location. (See also electronic vaulting)

Risk assessment
A risk assessment identifies an organization's information assets and the threats to each asset.

Risk management
Risk management is not an event, it is a process. An ongoing commitment is essential to effective risk management. Risk management includes an array of activities used to identify, control, and mitigate risks to IT systems and the ability to provide IT services.

Server load balancing
Server load balancing increases server and application availability. Through load balancing, traffic can be distributed dynamically across groups of servers running a common application so that no one server is overwhelmed. With this technique, a group of servers appears as a single server to the network. Load balancing systems monitor each server to determine the best path to route traffic to increase performance and availability so that one server is not overwhelmed with traffic. Load balancing can be implemented among servers within a site or among servers in different sites. Using load balancing among different sites can enable the application to continue to operate as long as one or more sites remain operational. Thus, load balancing could be a viable contingency measure depending on system availability requirements.

Service level agreement
A formal agreement between the customer(s) and the service provider specifying service levels and the terms under which a service or a package of services is provided to the customer.

Striping
Striping improves the performance of the hardware array controller by distributing data across all the drives. In striping, a data element is broken into multiple pieces, and a piece is distributed to each hard drive. Data transfer performance is increased using striping because the drives may access each data piece simultaneously. Striping can be implemented in bytes or blocks. Byte-level striping breaks the data into bytes and stores the bytes sequentially across the hard drives. Block-level striping breaks the data into a given-size block, and each block is distributed to a disk.

System owner
The SO is a Government civilian or military person that will be identified for each IS used by or in support of the Army. The SO will be responsible for the introduction or operation of an IS used by or in support of the Army. The

SO is responsible for ensuring the security of the IS as long as it remains in Army inventory, or until transferred (temporarily or permanently) to another Government person or organization and such transfer is appropriately documented and provided as an artifact to the accreditation package. If a contractor provides IA services to a system with the intent of meeting some or all of the SOs IA responsibilities, the IA responsibilities do not shift from the SO to the contractor. The SO remains responsible for ensuring the IA services are provided. The SO is responsible for the certification and accreditation of the IS and will provide the certification and accreditation package are provided to the Army in sufficient time for review and determination of operational IA risk recommendation in support of designated approving authority approval to operate decision prior to operational use or testing on a live network or with live Army data. Not less than annually, all SO will provide a written statement or digitally signed email to the Army Certification Authority that either confirms the effectiveness of assigned IA controls and their implementation, recommends changes or improvements to the implementation of assigned IA controls, or assigns additional IA controls, changes or improvements to the design of the IS itself. The SO will forward to the receiving Army Command, installation and activity designated approving authority a copy of the accreditation decision, supporting certification and accreditation documentation. The SO may charge the information assurance manager with authority to perform many of the SO IA duties, if appropriate; however, final responsibility will remain with the SO. The SO could be a product, project or project manager, a staff or command element that purchases or develops IT equipment and systems, a NEC or anyone else who is responsible for an IS. The SO is responsible for ensuring that all IA requirements are identified and included in the design, acquisition, installation, operation, maintenance, upgrade or replacement of all DA IS in accordance with DODD 8500.1.

Vital records
Records required for the Army to conduct its business under other than standard operating conditions, to resume normal business afterward, and to identify and protect important records dealing with the legal and financial rights of the Army and persons directly affected by actions of the Army.

Warm site
Warm sites are partially equipped office spaces that contain some or all of the system hardware, software, telecommunications, and power sources. The warm site is maintained in an operational status ready to receive the relocated system. The site may need to be prepared before receiving the system and recovery personnel. In many cases, a warm site may serve as an operational facility for another system or function, and in the event of contingency plan activation, the standard activities are displaced temporarily to accommodate the disrupted system.

Section III
Special Abbreviations and Terms
No entries in this section.