

EXAMPLE Section 1 – Introduction

1.0 Background

Many companies spend thousands of dollars each year on the acquisition, design, development, implementation, and maintenance of information systems vital to mission programs and administrative functions. The need for safe, secure, and reliable system solutions is heightened by the increasing dependence on computer systems and technology to provide services and develop products, administer daily activities, and perform short- and long-term management functions. There is also a need to ensure privacy and security when developing information systems, to establish uniform privacy and protection practices, and to develop acceptable implementation strategies for these practices.

The company needs a systematic and uniform methodology for information systems development. Using this process or Peak Strategy Process© (PSP) will ensure that systems meet IT mission objectives; are easy to maintain and cost-effective to enhance. Sound life cycle management practices include planning and evaluation in each phase of the information system life cycle. The appropriate level of planning and evaluation is commensurate with the cost of the system, the stability and maturity of the technology under consideration, how well defined the user requirements are, the level of stability of program and user requirements and security considerations.

1.1 Purpose, Scope and Applicability

1.1.1 Purpose

This PSP methodology establishes procedures, practices, and guidelines governing the initiation, concept development, planning, requirements analysis, design, development, integration and test, implementation, and operations, maintenance and disposition of information systems (IS) within the company.

1.1.2 Scope

This methodology should be used for all company information systems and applications. It is applicable across all information technology (IT) environments (e.g., mainframe, client, server) and applies to contractually developed as well as in-house developed applications. The specific participants in the life cycle process, and the necessary reviews and approvals, vary from project to project. The guidance provided in this document should be tailored to the individual project based on cost, complexity, and criticality to the agency's mission. See Chapter 13 for Alternate PSP Work Patterns if a formal PSP is not feasible. Similarly, the documents called for in the guidance and shown in Appendix C should be tailored based on the scope of the effort and the needs of the decision authorities.

1.1.3 Applicability

This methodology can be applied to all company Departments, Boards, and Divisions who are responsible for information systems development. All Project Managers and development teams involved in system development projects represent the primary audience for this guide.

1.2 Introduction to PSP

The PSP includes ten phases during which defined IT work products are created or modified. The tenth phase occurs when the system is disposed of and the task performed is either eliminated or transferred to other systems. The tasks and work products for each phase are described in subsequent chapters. Not every project will require that the phases be sequentially executed. However, the phases are interdependent. Depending upon the size and complexity of the project, phases may be combined or may overlap. The major phases are Prepare, Evaluate, Act and Kaizen. Kaizen is Japanese for continuous and incremental improvement. We believe that processes should consistently be reviewed and improved. See Figure 1-1 below:



The company's PSP encompasses ten phases:

1.2.1 Initiation Phase

The initiation of a system (or project) begins when a business need or opportunity is identified. A Project Manager should be appointed to manage the project. This business need is documented in a Concept Proposal. After the Concept Proposal is approved, the System Concept Development Phase begins.

1.2.2 System Concept Development Phase

Once a business need is approved, the approaches for accomplishing the concept are reviewed for feasibility and appropriateness. The System Concept Development Document identifies the scope of the system and requires Senior Official approval and funding before beginning the Planning Phase.

1.2.3 Planning Phase

The concept is further developed to describe how the business will operate once the approved system is implemented, and to assess how the system will impact employee and customer privacy. To ensure the products and /or services provide the required capability on-time and within budget, project resources, activities, schedules, tools, and reviews are defined. Additionally, security certification and accreditation activities begin with the identification of system security requirements and the completion of a high level vulnerability assessment.

1.2.4 Requirements Analysis Phase

Functional user requirements are formally defined and delineate the requirements in terms of data, system performance, security, and maintainability requirements for the system. All requirements are defined to a level of detail sufficient for systems design to proceed. All requirements need to be measurable and testable and relate to the business need or opportunity identified in the Initiation Phase.

1.2.5 Design Phase

The physical characteristics of the system are designed during this phase. The operating environment is established, major subsystems and their inputs and outputs are defined, and processes are allocated to resources. Everything requiring user input or approval must be documented and reviewed by the user. The physical characteristics of the system are specified and a detailed design is prepared. Subsystems identified during design are used to create a detailed structure of the system. Each subsystem is partitioned into one or more design units or modules. Detailed logic specifications are prepared for each software module.

1.2.6 Development Phase

The detailed specifications produced during the design phase are translated into hardware, communications, and executable software. Software shall be unit tested, integrated, and retested in a systematic manner. Hardware is assembled and tested.

1.2.7 Integration and Test Phase

The various components of the system are integrated and systematically tested. The user tests the system to ensure that the functional requirements, as defined in the functional requirements document, are satisfied by the developed or modified system. Prior to installing and operating the system in a production environment, the system must undergo certification and accreditation activities.

1.2.8 Implementation Phase

The system or system modifications are installed and made operational in a production environment. The phase is initiated after the system has been tested and accepted by the user. This phase continues until the system is operating in production in accordance with the defined user requirements.

1.2.9 Operations and Maintenance Phase

The system operation is ongoing. The system is monitored for continued performance in accordance with user requirements, and needed system modifications are incorporated. The operational system is periodically assessed through In-Process Reviews to determine how the system can be made more efficient and effective. Operations continue as long as the system can be effectively adapted to respond to the company's needs. When modifications or changes are identified as necessary, the system may reenter the planning phase.

1.2.10 Disposition Phase

The disposition activities ensure the orderly termination of the system and preserve the vital information about the system so that some or all of the information may be reactivated in the future if necessary. Particular emphasis is given to proper preservation of the data processed by the system, so that the data is effectively migrated to another system or archived in accordance with applicable records management regulations and policies, for potential future access.

1.3 Control

This PSP calls for a series of comprehensive management controls. These include:

- Peak Strategy Process should be used to ensure a structured approach to information systems development and operation.
- Each system project must have an accountable sponsor.
- A single project manager must be appointed for each system project.
- A comprehensive project management plan is required for each system project.
- Data Management and security must be emphasized throughout the PSP.
- A system project may not proceed until resource availability is assured.

EXAMPLE POLICY 1

Information Sensitivity Policy

1.0 Purpose

The Information Sensitivity Policy is intended to help employees determine what information can be disclosed to non-employees, as well as the relative sensitivity of information that should not be disclosed outside of <Company Name> without proper authorization.

The information covered in these guidelines includes, but is not limited to, information that is either stored or shared via any means. This includes: electronic information, information on paper, and information shared orally or visually (such as telephone and video conferencing).

All employees should familiarize themselves with the information and handling guidelines that follow this introduction. It should be noted that the sensitivity level definitions were created as guidelines and to emphasize common sense steps that you can take to protect <Company Name> Confidential information (e.g., <Company Name> Confidential information should not be left unattended in conference rooms).

Please Note: The impact of these guidelines on daily activity should be minimal.

Questions about the proper classification of a specific piece of information should be addressed to your manager. Questions about these guidelines should be addressed to <Company>.

2.0 Scope

All <Company Name> information is categorized into two main classifications:

- <Company Name> Public
- <Company Name> Confidential

<Company Name> Public information is information that has been declared public knowledge by someone with the authority to do so, and can freely be given to anyone without any possible damage to <Company Name> Systems, Inc.

<Company Name> Confidential contains all other information. It is a continuum, in that it is understood that some information is more sensitive than other information, and should be protected in a more secure manner. Included is information that should be protected very closely, such as trade secrets, development programs, potential acquisition targets, and other information integral to the success of our company. Also included in <Company Name> Confidential is information that is less critical, such as telephone directories, general corporate information, personnel information, etc., which does not require as stringent a degree of protection.

A subset of <Company Name> Confidential information is "<Company Name> Third Party Confidential" information. This is confidential information belonging or pertaining to another corporation which has been entrusted to <Company Name> by that company under non-disclosure agreements and other contracts. Examples of this type of information include everything from joint development efforts to vendor lists, customer orders, and supplier information. Information in this category ranges from extremely sensitive to information about the fact that we've connected a supplier / vendor into <Company Name>'s network to support our operations.

<Company Name> personnel are encouraged to use common sense judgment in securing <Company Name> Confidential information to the proper extent. If an employee is uncertain of the sensitivity of a particular piece of information, he/she should contact their manager

3.0 Policy

The Sensitivity Guidelines below provides details on how to protect information at varying sensitivity levels. Use these guidelines as a reference only, as <Company Name> Confidential information in each column may necessitate more or less stringent measures of protection depending upon the circumstances and the nature of the <Company Name> Confidential information in question.

3.1 **Minimal Sensitivity:** General corporate information; some personnel and technical information

Marking guidelines for information in hardcopy or electronic form.

Note: any of these markings may be used with the additional annotation of "3rd Party Confidential".

Marking is at the discretion of the owner or custodian of the information. If marking is desired, the words "<Company Name> Confidential" may be written or designated in a conspicuous place on or in the information in question. Other Departments that may be used include "<Company Name> Proprietary" or similar Departments at the discretion of your individual business unit or department. Even if no marking is present, <Company Name> information is presumed to be "<Company Name> Confidential" unless expressly determined to be <Company Name> Public information by a <Company Name> employee with authority to do so.

Access: <Company Name> employees, contractors, people with a business need to know.

Distribution within <Company Name>: Standard interoffice mail, approved electronic mail and electronic file transmission methods.

Distribution outside of <Company Name> internal mail: U.S. mail and other public or private carriers, approved electronic mail and electronic file transmission methods.

Electronic distribution: No restrictions except that it be sent to only approved recipients.

Storage: Keep from view of unauthorized people; erase whiteboards, do not leave in view on tabletop. Machines should be administered with security in mind. Protect from loss; electronic information should have individual access controls where possible and appropriate.

Disposal/Destruction: Deposit outdated paper information in specially marked disposal bins on <Company Name> premises; electronic data should be expunged/cleared. Reliably erase or physically destroy media.

Penalty for deliberate or inadvertent disclosure: Up to and including termination, possible civil and/or criminal prosecution to the full extent of the law.

3.2 **More Sensitive:** Business, financial, technical, and most personnel information

Marking guidelines for information in hardcopy or electronic form.

Note: any of these markings may be used with the additional annotation of "3rd Party Confidential". As the sensitivity level of the information increases, you may, in addition or instead of marking the information "<Company Name> Confidential" or "<Company Name> Proprietary", wish to Departmentalize the information "<Company Name> Internal Use Only" or other similar Departmentalization at the discretion of your individual business unit or department to denote a more sensitive level of information. However, marking is discretionary at all times.

Access: <Company Name> employees and non-employees with signed non-disclosure agreements who have a business need to know.

Distribution within <Company Name>: Standard interoffice mail, approved electronic mail and electronic file transmission methods.

Distribution outside of <Company Name> internal mail: Sent via U.S. mail or approved private carriers.

Electronic distribution: No restrictions to approved recipients within <Company Name>, but should be encrypted or sent via a private link to approved recipients outside of <Company Name> premises.

Storage: Individual access controls are highly recommended for electronic information.

Disposal/Destruction: In specially marked disposal bins on <Company Name> premises; electronic data should be expunged/cleared. Reliably erase or physically destroy media.

Penalty for deliberate or inadvertent disclosure: Up to and including termination, possible civil and/or criminal prosecution to the full extent of the law.

3.3 **Most Sensitive:** Trade secrets & marketing, operational, personnel, financial, source code, & technical information integral to the success of our company

Marking guidelines for information in hardcopy or electronic form.

Note: any of these markings may be used with the additional annotation of "3rd Party Confidential". To indicate that <Company Name> Confidential information is very sensitive, you may should Departmentalize the information "<Company Name> Internal: Registered and Restricted", "<Company Name> Eyes Only", "<Company Name> Confidential" or similar

Departmentalization at the discretion of your individual business unit or department. Once again, this type of <Company Name> Confidential information need not be marked, but users should be aware that this information is very sensitive and be protected as such.

Access: Only those individuals (<Company Name> employees and non-employees) designated with approved access and signed non-disclosure agreements.

Distribution within <Company Name>: Delivered direct - signature required, envelopes stamped confidential, or approved electronic file transmission methods.

Distribution outside of <Company Name> internal mail: Delivered direct; signature required; approved private carriers.

Electronic distribution: No restrictions to approved recipients within <Company Name>, but it is highly recommended that all information be strongly encrypted.

Storage: Individual access controls are very highly recommended for electronic information. Physical security is generally used, and information should be stored in a physically secured computer.

Disposal/Destruction: Strongly Encouraged: In specially marked disposal bins on <Company Name> premises; electronic data should be expunged/cleared. Reliably erase or physically destroy media.

Penalty for deliberate or inadvertent disclosure: Up to and including termination, possible civil and/or criminal prosecution to the full extent of the law.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Definitions

Terms and Definitions

Appropriate measures

To minimize risk to <Company Name> from an outside business connection. <Company Name> computer use by competitors and unauthorized personnel must be restricted so that, in the event of an attempt to access <Company Name> corporate information, the amount of information at risk is minimized.

Configuration of <Company Name>-to-other business connections

Connections shall be set up to allow other businesses to see only what they need to see. This involves setting up both applications and network configurations to allow access to only what is necessary.

Delivered Direct; Signature Required

Do not leave in interoffice mail slot, call the mail room for special pick-up of mail.

Approved Electronic File Transmission Methods

Includes supported FTP clients and Web browsers.

Envelopes Stamped Confidential

You are not required to use a special envelope. Put your document(s) into an interoffice envelope, seal it, address it, and stamp it confidential.

Approved Electronic Mail

Includes all mail systems supported by the IT Support Team. These include, but are not necessarily limited to, [insert corporate supported mailers here...]. If you have a business need to use other mailers contact the appropriate support organization.

Approved Encrypted email and files

Techniques include the use of DES and PGP. DES encryption is available via many different public domain packages on all platforms. PGP use within <Company Name> is done via a license. Please contact the appropriate support organization if you require a license.

Company Information System Resources

Company Information System Resources include, but are not limited to, all computers, their data and programs, as well as all paper information and any information at the Internal Use Only level and above.

Expunge

To reliably erase or expunge data on a PC or Mac you must use a separate program to overwrite data, supplied as a part of Norton Utilities. Otherwise, the PC or Mac's normal erasure routine keeps the data intact until overwritten. The same thing happens on UNIX machines, but data is much more difficult to retrieve on UNIX systems.

Individual Access Controls

Individual Access Controls are methods of electronically protecting files from being accessed by people other than those specifically designated by the owner. On UNIX machines, this is accomplished by careful use of the `chmod` command (use *man chmod* to find out more about it). On Mac's and PC's, this includes using passwords on screensavers, such as Disklock.

Insecure Internet Links

Insecure Internet Links are all network links that originate from a locale or travel over lines that are not totally under the control of <Company Name>.

Encryption

Secure <Company Name> Sensitive information in accordance with the *Acceptable Encryption Policy*. International issues regarding encryption are complex. Follow corporate guidelines on export controls on cryptography, and consult your manager and/or corporate legal services for further guidance.

One Time Password Authentication

One Time Password Authentication on Internet connections is accomplished by using a one time password token to connect to <Company Name>'s internal network over the Internet. Contact your support organization for more information on how to set this up.

Physical Security

Physical security means either having actual possession of a computer at all times, or locking the computer in an unusable state to an object that is immovable. Methods of accomplishing

this include having a special key to unlock the computer so it can be used, thereby ensuring that the computer cannot be simply rebooted to get around the protection. If it is a laptop or other portable computer, never leave it alone in a conference room, hotel room or on an airplane seat, etc. Make arrangements to lock the device in a hotel safe, or take it with you. In the office, always use a lockdown cable. When leaving the office for the day, secure the laptop and any other sensitive material in a locked drawer or cabinet.

Private Link

A Private Link is an electronic communications path that <Company Name> has control over it's entire distance. For example, all <Company Name> networks are connected via a private link. A computer with modem connected via a standard land line (not cell phone) to another computer have established a private link. ISDN lines to employee's homes is a private link. <Company Name> also has established private links to other companies, so that all email correspondence can be sent in a more secure manner. Companies which <Company Name> has established private links include all announced acquisitions and some short-term temporary links

6.0 Revision History

EXAMPLE POLICY 2

Password Protection Policy

1.0 Overview

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of <Company Name>'s entire corporate network. As such, all <Company Name> employees (including contractors and vendors with access to <Company Name> systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

2.0 Purpose

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

3.0 Scope

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any <Company Name> facility, has access to the <Company Name> network, or stores any non-public <Company Name> information.

4.0 Policy

4.1 General

- All system-level passwords (e.g., root, enable, NT admin, application administration accounts, etc.) must be changed on at least a quarterly basis.
- All production system-level passwords must be part of the <Company> administered global password management database.
- All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every six months. The recommended change interval is every four months.
- User accounts that have system-level privileges granted through group memberships or programs such as "sudo" must have a unique password from all other accounts held by that user.
- Passwords must not be inserted into email messages or other forms of electronic communication.
- Where SNMP is used, the community strings must be defined as something other than the standard defaults of "public," "private" and "system" and must be different from the passwords used to log in interactively. A keyed hash must be used where available (e.g., SNMPv2).
- All user-level and system-level passwords must conform to the guidelines described below.

4.2 Guidelines

A. General Password Construction Guidelines

Passwords are used for various purposes at <Company Name>. Some of the more common uses include: user level accounts, web accounts, email accounts, screen saver protection, voicemail password, and local router logins. Since very few systems have support for one-time tokens (i.e., dynamic passwords which are only used once), everyone should be aware of how to select strong passwords.

Poor, weak passwords have the following characteristics:

- The password contains less than fifteen characters
- The password is a word found in a dictionary (English or foreign)
- The password is a common usage word such as:
 - Names of family, pets, friends, co-workers, fantasy characters, etc.
 - Computer terms and names, commands, sites, companies, hardware, software.
 - The words "<Company Name>", "sanjose", "sanfran" or any derivation.
 - Birthdays and other personal information such as addresses and phone numbers.
 - Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
 - Any of the above spelled backwards.
 - Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

Strong passwords have the following characteristics:

- Contain both upper and lower case characters (e.g., a-z, A-Z)

- Have digits and punctuation characters as well as letters e.g., 0-9, !@#\$%^&*()_+|~-=\`{}[]:;'<>?,./)
- Are at least fifteen alphanumeric characters long and is a pass phrase (Ohmy1stubbedmyt0e).
- Are not a word in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.
- Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

NOTE: Do not use either of these examples as passwords!

B. Password Protection Standards

Do not use the same password for <Company Name> accounts as for other non-<Company Name> access (e.g., personal ISP account, option trading, benefits, etc.). Where possible, don't use the same password for various <Company Name> access needs. For example, select one password for the Engineering systems and a separate password for IT systems. Also, select a separate password to be used for an NT account and a UNIX account.

Do not share <Company Name> passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, Confidential <Company Name> information.

Here is a list of "don'ts":

- Don't reveal a password over the phone to ANYONE
- Don't reveal a password in an email message
- Don't reveal a password to the boss
- Don't talk about a password in front of others
- Don't hint at the format of a password (e.g., "my family name")
- Don't reveal a password on questionnaires or security forms
- Don't share a password with family members
- Don't reveal a password to co-workers while on vacation

If someone demands a password, refer them to this document or have them call someone in the Information Security Department.

Do not use the "Remember Password" feature of applications (e.g., Eudora, Outlook, and Netscape Messenger).

Again, do not write passwords down and store them anywhere in your office. Do not store passwords in a file on ANY computer system (including Palm Pilots or similar devices) without encryption.

Change passwords at least once every six months (except system-level passwords which must be changed quarterly). The recommended change interval is every four months.

If an account or password is suspected to have been compromised, report the incident to <Company> and change all passwords.

Password cracking or guessing may be performed on a periodic or random basis by <Company> or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it.

C. Application Development Standards

Application developers must ensure their programs contain the following security precautions. Applications:

- should support authentication of individual users, not groups.
- should not store passwords in clear text or in any easily reversible form.
- should provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.
- should support TACACS+ , RADIUS and/or X.509 with LDAP security retrieval, wherever possible.

D. Use of Passwords and Pass phrases for Remote Access Users

Access to the <Company Name> Networks via remote access is to be controlled using either a one-time password authentication or a public/private key system with a strong pass phrase.

E. Pass phrases

Pass phrases are generally used for public/private key authentication. A public/private key system defines a mathematical relationship between the public key that is known by all, and the private key, that is known only to the user. Without the pass phrase to "unlock" the private key, the user cannot gain access.

Pass phrases are not the same as passwords. A pass phrase is a longer version of a password and is, therefore, more secure. A pass phrase is typically composed of multiple words. Because of this, a pass phrase is more secure against "dictionary attacks."

A good pass phrase is relatively long and contains a combination of upper and lowercase letters and numeric and punctuation characters. An example of a good pass phrase:

"The*?#>*@TrafficOnThe101Was*&#!#ThisMorning"

All of the rules above that apply to passwords apply to pass phrases.

5.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6.0 Definitions

Terms

Definitions

Application Administration Account Any account that is for the administration of an application (e.g., Oracle database administrator, ISSU administrator).

7.0 Revision History

EXAMPLE APPENDIX

Appendix C-9: Test Analysis Report

The Test Analysis Report documents software testing - unit/module, subsystem integration, system, user acceptance, and security - as defined in the test plan. The Test Analysis Report records results of the tests, presents the capabilities and deficiencies for review, and provides a means of assessing software progression to the next stage of development or testing. Results of each type of test are added to the software development document for the module or system being tested. Reports are created as required in the remaining phases. The set of Test Analysis Reports provides a basis for assigning responsibility for deficiency correction and follow up, and for preparation of a statement of project completion.

Test Problem Report forms are generated as required and are attached to the Test Analysis Reports during testing at the integration level and higher. The disposition of problems found, starting with integration testing, will be traced and reported under configuration control.

1.0 PURPOSE

This section should present a clear, concise statement of the purpose for the Test Analysis Report.

2.0 SCOPE

This section identifies the software application system tested and the test(s) conducted covered by this Test Analysis Report. The report summarizes the results of tests already conducted and identifies testing that remains to be conducted. Provide a brief summary of the project objectives, and identify the System Proponent and users.

3.0 REFERENCE DOCUMENTS

This section provides a bibliography of key project references and deliverables applicable to system software testing. These references might include the FRD, User Manual, Operations Manual, Maintenance Manual, Test Plan, and prior Test Analysis Reports.

3.1 Security

This section describes any security considerations associated with the system or module being tested, the test analysis, and the data being handled - such as confidentiality requirements, audit trails, access control, and recoverability. If this Test Analysis Report is not documenting the formal security test, also summarize the security capabilities included in the system or module test and itemize the specific security deficiencies detected while conducting the test.

The results of specific tests, findings, deficiency analysis, and recommendations will be discussed in the subsequent sections. Reference those portions of this document that specifically address system security issues. If no deficiencies were detected during the system or module test, state this fact.

3.2 Glossary

This section defines all terms and provides a list of abbreviations used in the Test Analysis Report. If the list is several pages in length, it may be placed as an appendix.

4.0 TEST ANALYSIS

This section describes the results of each test performed. Tests at each level should include verification of access control and system standards, functionality, and error processes. Repeat the subsections of this section for each test performed.

4.1 Test Name

The test performed for the specified unit, module, subsystem, or system is discussed in this section. For each test, provide the subsequent sections.

4.1.1 System Function

A high-level description of the function tested and a description of system capabilities designed to satisfy these functions are contained in this section. Each system function should be described separately.

4.1.2 Functional Capability

This section evaluates the performance of each function demonstrated in the test. This section also assesses the manner in which the test environment may be different from the operational environment and the effect of this difference on functional capabilities.

4.1.3 Performance Capability

This section quantitatively compares the software performance characteristics with the criteria stated in the test plan. The comparison should identify deficiencies, limitations, and constraints detected for each function during testing. If appropriate, a test history or log can be included as an appendix.

5.0 SOFTWARE AND HARDWARE REQUIREMENTS FINDINGS

Each numbered requirement should be described in a separate section. Repeat the subsections of this section for each numbered requirement covered by the test plan.

5.1 Requirement Number and Name

The requirement number provided in the title to this section is the number from the requirements traceability matrix in the test plan and the name provided is the requirement's short name.

5.1.1 Findings

This subsection briefly describes the requirement, including the software and hardware capabilities, and states the findings from one or more tests.

5.1.2 Limitations

This subsection describes the range of data values tested, including dynamic and static data, for this requirement and identifies deficiencies, limitations, and constraints detected in the software and hardware during the testing.

6.0 SUMMARY AND CONCLUSIONS

6.1 Demonstrated Capabilities

This section provides an overview and summary analysis of the testing program. Describe the overall capabilities and deficiencies of the testing software module or system. Where tests were intended to demonstrate one or more specific performance requirements, findings should be presented that compare the test results with the performance requirements. Include an assessment of any differences in the test environment versus the operational environment that may have had an effect on the demonstrated capabilities. Provide a statement, based on the results of the system or module test, concerning the adequacy of the system or module to meet overall security requirements.

6.2 System Deficiencies

This section describes test results showing software deficiencies. Identify all problems by name and number when placed under configuration control. Describe the cumulative or overall effect of all detected deficiencies on the system of module.

6.3 System Refinements

This section itemizes any indicated improvements in system design or operation based on the results of the test period. Accompanying each improvement or enhancement suggested should be a discussion of the added capability it provides and the effect on the system

design. The improvements should be indicated by name and requirement number when placed under configuration control.

6.4 Recommendations and Estimates

This section provides a statement describing the overall readiness for system implementation. For each deficiency, address the effect on system performance and design. Include any estimates of time and effort required for correction of each deficiency and any recommendations on the following:

- The urgency of each correction
- Parties responsible for corrections
- Recommended solution or approach to correcting deficiencies

6.5 Test Problem Report

This section contains copies of the test Problem Reports related to the deficiencies found in the test results. The Test Problem Report will vary according to the information system development project, its scope and complexity, etc. Test Problem Report forms are generated as required and are attached to the Test Analysis Reports during testing at the integration level and higher. The disposition of problems found, starting with integration testing, should be tracked and reported under configuration control.

6.6 Test Analysis Approval Determination Form

This section contains one copy of the Test Analysis Approval Determination form. This form briefly summarizes the perceived readiness for migration of the software. In the case of a User Acceptance Test, it serves as the user's recommendation for migration to production.