Global Information Assurance Certification Paper

XYZ Corporation

AUTOMATED HUMAN RESOURCES PAYROLL (HRPAYROLL) SYSTEM SECURITY TEST PLAN

Prepared By:

Office of Information Security (OIS)

For XYZ Corporation use only

Version Control Log (Revision History)

Version No.	Date	Description
Version 1.0	2001	Initial Submission
Version 2.0		

Table of Contents

PREFACE

This document has been prepared in partial fulfillment of the SANS GIAC Certification Security Essentials (Track 1, GSEC) requirements. The scenario presented within this document is not fictional, but is based on a real-life project in which the author participated and performed productive work. This document has been sanitized of all proprietary information in compliance with directives set forth by the SANS Institute, and is in strict adherence with both the Privacy Act of 1974 (Public Law 93-579, 5 U.S.C. 552a (e) (10)) and the SANS GIAC Non-disclosure Agreement.

1 INTRODUCTION AND BACKGROUND INFORMATION

This document describes the security test plan for the new XYZ Corporation Human Resources Payroll (HRPayroll) system. It will be housed on a server[1] located at The XYZ Corporation Computer Center.

The system is designed to be comprised of data in two classifications, (1) Base Benefits, and (2) Time and Labor. Data characteristics are further defined as follows:

Base Benefits

Federal/State Income Taxes,
Social Security Tax
Medicare Tax
Medical Insurance
Life Insurance
Unemployment Compensation Tax, State and Federal
Savings Bonds
Charities Contributions

Time and Labor

Base Rate
Hours Worked
Accrued Personal Leave
Accrued Sick Leave
Accrued Leave for Jury Duty
Accrued Leave for Military/Reserve Duty
Leave without pay and unexplained absence

The HRPayroll system will process the following business processes:

a) Hire
b) Award
c) Earnings Code
d) Change to Lower Grade
e) Locality Pay/Pay Adjustment
f) Bonus (Relocation/Recruitment)
g) Promotion
h) Within Grade Increase (WGI)
i) Correction
j) Cancellation

[1] The selection, deployment, and protection of a specific server and operating system, along with communications security, is reserved for an anticipated future project.

k) Resignation
l) Retirement
m) Death
n) Rehire
o) Reassignment
p) Change in Tenure Group
q) Change in Work Schedule/Work Hour
r) Change in Duty Station
s) Name Change
t) Termination with prejudice
u) Suspension
v) Retro Actions
w) Leave Without Pay (LWOP)
x) Return to Duty

1.1 Background

Due to growth, XYZ Corporate management has decided to convert the HRPayroll function from a manual to a consolidated fully-automated system. Due to recent trends and developments, corporate management created an Information Systems Security Office (ISSO) which has been placed in responsible charge for IS/IT security corporate wide. The benefits of this system are perceived to be a vast improvement in speed, accuracy, and efficiency. Time records will be entered electronically each day, eliminating the need for line and staff supervisors to collect weekly timesheets, reducing the risk of timesheets being lost or misplaced, reducing the compromise of private information, and eliminating the need to utilize card-punching and manually typing employee paychecks.

1.2 Roles and Responsibilities

1.2.1 System Operation

The new HRPayroll system will be operated by the Human Resources Dept. The functional activities will resemble the activities performed by the former Personnel Dept., with the exception that the activities will be performed electronically vice manually. The HRPayroll system incorporates the following operator functions:

Add	Adds a new record
Update Display	Updates an existing record and displays that record only
Update Display All	Updates an existing record and can display all related records
Correction	Allows corrections to errors entered by another operator
Reports and Query	Previews/prints reports and runs pre-designed queries

In terms of functional duties, the end users are now referred to as "operators". The following definitions have been established for operator types:

Personnel Assistant	Accesses Base Benefits data all locations, works in HR Office
Personnel Manager	Accesses Base Benefits data all locations, works in HR Office
Personnel Management Specialist	Accesses Base Benefits data all locations, works in HR Office
Personnel Officer	Accesses Base Benefits data for location, works at field location and is considered HR Office clerical staff
Super TimeKeeper	Access Time and Labor data for correction only
TimeKeeper	Access Time and Labor data, line/staff supervisors located throughout corporation
Super User (HQ)	Accesses all data, all locations, bonded employee at HR Office
Super User (Field)	Accesses all data at field location, bonded employee at location

The *Administrative user* is a privileged account holder or person authorized to access system data and functions that are not accessible to the end user. Administrative users are part of the Office of Information Technology (OIT) and not the Accounting Dept. Their sole relationship to HRPayroll is to provide systemic help as needed..

1.2.2 System Oversight and Auditing

The Accounting Dept. will continue to have management oversight of the HRPayroll business process. The auditing component is expanded to include required Information Technology (IT) audits. IT audits are extremely important. Reconstruction of unauthorized activity enhances the proper investigation of security violations as well as (attempted) fraudulent activities. Audit criteria are discussed in Section 2, Security and Security Test Criteria and audit methodology is discussed in detail in Section 5, Technical Controls.

1.2.3 System Maintenance

The system will be maintained by the Corporate Office of Information Technology (OIT), which is responsible for hardware, software, and infrastructure corporation-wide. OIT will issue a monthly report to the Director, Accounting Dept. citing all activities involving the HRPayroll system. Interim reports will be issued to the Director, Accounting Dept. as needed (such as in an emergency). If during a given month there is no activity, a report citing "no activity" will be issued.

1.3 Requirements

Because this is a HRPayroll system, all processes must continue to comply to requirements set forth by the American Institute of Certified Public Accountants (AICPA) and the Financial Accounting Standards Board (FASB).

From an information security perspective, the new automated HRPayroll system must meet the three basic security requirements for any system: data confidentiality, system integrity, and system availability.

1.3.1 Data Confidentiality Requirements

The system stores and processes sensitive data on employees as well as sensitive financial information pertaining to productivity and factory overhead (time and labor) costs. This data must be protected in accordance with FASB requirements and the provisions of the Privacy Act of 1974. Unauthorized disclosure of this data could result in significant personal damage to individuals and litigation costs to the company.

1.3.2 System Integrity Requirements

The system contains information which must be protected from unauthorized, unanticipated, or unintentional modification.

1.3.3 System Availability Requirements

Payroll must be processed on time. Failure in this process will result in loss of public confidence, litigation activities, and adverse collective bargaining unit (union) action.

1.4 Purpose

This Security Test Plan is intended to describe the methodology used to validate and protect the Corporate HRPayroll from damage, either intentional or unintentional, by users of the system.

1.5 Scope

This security test plan describes the testing methodology and it explains the testing procedures engineered to run against the security features incorporated into the HRPayroll design to protect its information and processing capabilities from:

- Misuse
- Unplanned modification
- Unauthorized access
- Unavailability due to attack, natural disaster or power interruption.

This security test plan also describes the methodology utilized to ensure the safeguarding of information processed by the system and the measures taken to ensure the three basic security requirements for any system: data confidentiality, system integrity, and system availability. It also includes the security test criteria (scripts), which are followed during the actual security test.

Due to the dynamic nature of technology and frequent changes in human resources and HRPayroll requirements, this document will be reviewed every six months and updated as appropriate.

All information published on the Corporate HRPayroll is unclassified. However, some information processed and stored on the HRPayroll is considered Confidential. HRPayroll users provide personal data including User-ID and Password information, when they access the system. This Security Plan document is contains no Confidential material, but should be considered For Official Use Only (FOUO).

1.6 Document Overview

This document provides information about the following:

Security Test Criteria - Management Controls – Test scripts documenting the testing of security management methodology implemented by the Accounting Dept. and OIT staffs.

Security Test Criteria - Operational Controls – Test scripts documenting the testing of security procedures implemented by the Accounting Dept. and OIT staffs.

Security Test Criteria - Technical Controls – Test scripts documenting the testing of security measures implemented by the HRPayroll system's computer systems including hardware, software and communications equipment.

Security Test Report – A report documenting the findings, risks, mitigating actions and recommendations which were a result of this security test.

The Web-based references used in the research and development of this document are provided in Appendix A.

The bibliographic references used in the research and development of this document are provided in Appendix B.

The acronyms used in this document are summarized in Appendix C.

1.7 Test Execution

Security Test Criteria - Management Controls (STC-MC) – For the SCT-MC, see attachment # SCT-I-MC, for completed Test scripts documenting the existence and implementation of the security management methodology. This attachment will be updated and made available prior to the commencement of the following phases of security testing: Integration tests, initial systems tests, final systems tests, and User Acceptance Tests. Any changes/revisions resulting from past tests will be reflected in the next test cycle.

Security Test Criteria - Operational Controls (STC-OC) – For the SCT-OC, see attachment # SCT-I-OC, for completed Test scripts documenting the existence of security procedures implemented by the staff. This attachment will be updated and made available prior to the commencement of the following phases of security testing: Integration tests, initial systems tests, final systems tests, and User Acceptance Tests. Any changes/revisions resulting from past tests will be reflected in the next test cycle.

Security Test Criteria - Technical Controls – (STC-TC) – For the SCT-TC, see attachment # SCT-I-TC, for completed Test scripts documenting the testing of security measures implemented by the HRPayroll computer systems including hardware, software and communications equipment. This attachment will be updated and made available prior to the commencement of the following phases of security testing Integration tests, initial systems tests, final systems tests, and User Acceptance Tests. Any changes/revisions resulting from past tests will be reflected in the next test cycle.

Security Test Report – (STR) For the Phase I STR, the report documenting the findings, risks, mitigating actions and recommendations are a result of the Security Tests for all Phases. This section will be generated and made available after the completion of all Phases of the Security Test, per the Project Manager's request.

2 SECURITY AND SECURITY TEST CRITERIA

Corporate management has seen fit to establish standards applicable to the new automated HRPayroll system. Governance of the legacy manual system was concerned only with the financial reporting requirements mandated by law (FASB) and by industry standards (AICPA). While these standards are good, and will continue to be practiced, they do not suffice by themselves for a modern automated system. The OIS has recommended several criteria to be used for a model of compliance.

2.1 NIST SP 800-18, Guide for Developing Security Plans for Information Technology Systems

This standard was chosen because it serves as an excellent baseline for a medium-sized organization and is sufficient for the applications being performed within the organization. It is a "mainstay" standard which is well-respected in industry. The NIST SP 800-18 Table of Contents is included as Appendix D.

2.2 IS Auditing Criteria - CobiT

Adaptation of IS auditing functionality is a fundamental requirement of any IT security criteria. Currently, all major standards require auditing, but no specific auditing standard has been mandated by law or adapted by a major organization such as the AICPA, FASB, NIST, etc. Investigation by a multidisciplinary team resulted in the recommendation to adapt CobiT (Control Objectives for Information and related Technology as the XYZ Corporation IS auditing standard.

CobiT was first released by the Information Systems Audit and Control Foundation (ISACF) in 1996. The 2nd edition, reflecting an increase in the number of source documents, a revision in the high-level and detailed control objectives and the addition of the *Implementation Tool Set*, was published in 1998. The 3rd edition marks the entry of a new primary publisher for COBIT: the IT Governance Institute. The IT Governance Institute was formed by the Information System Audit and Control Association (ISACA) and its related Foundation in 1998 in order to advance the understanding and adoption of IT governance principles. Detailed information about CobiT can be obtained at http://www.Itgovernance.org

The correlation between NIST SP 800-18 and the CobiT standard is tabulated in Appendix E. This mapping was undertaken to:

1. Confirm that no conflicts exist between NIST 800-18 and CobiT
2. Validate the relationships between NIST 800-18 and CobiT
3. Reinforce validation of CobiT as an applicable standard
4. Provide a singular, centralized and uniform procedure to be followed by all auditors
5. Provide a baseline for future refinements

2.3 International Standards Organization (ISO) 15408 Common Criteria

Due to continuing economic globalization, XYZ Corporation's international/overseas has started to expand. Substantial future expansion is anticipated. Accordingly, future IT acquisitions and upgrades will be expected to meet recognized international criteria. In anticipation of future requirements, the test procedures in the security test plan have been mapped to the ISO 15408 Common Criteria (CC). The CC is useful as a guide for the development of products or systems with IT security functions and for the procurement of commercial products and systems with such functions. The CC addresses protection of information from unauthorized disclosure, modification, or loss of use. Currently, the CC is the only internationally recognized guidance with respect to information systems security. XYZ Corporation has decided to consider it in all future acquisitions and upgrades.

The following legal notice is cited directly from the CC:

This Legal NOTICE has been placed in all Parts of the CC by request:
The seven governmental organisations (collectively called "the Common Criteria Project Sponsoring Organisations") listed just below and identified fully in Part 1Annex A, as the joint holders of the copyright in the Common Criteria for Information Technology Security Evaluations, version 2.1 Parts 1 through 3(called "CC 2.1"), hereby grant non-exclusive license to ISO/IEC to use CC 2.1 in the continued development/maintenance of the ISO/IEC 15408 international standard. However, the Common Criteria Project Sponsoring Organisations retain the right to use, copy, distribute, translate or modify CC 2.1 as they see fit.

Canada:	Communications Security Establishment
France:	Service Central de la Sécurité des Systèmes d'Information
Germany:	Bundesamt für Sicherheit in der Informationstechnik
Netherlands:	Netherlands National Communications Security Agency
United Kingdom:	Communications-Electronics Security Group
United States:	National Institute of Standards and Technology
United States:	National Security Agency

The CC lists IT security requirements and activities in "families" and subdivides families into "classes". The major elements of the CC are summarized in Appendix F.

2.4 Office of Management and Budget (OMB) Circular A-130

Federal (U.S. Government) contracts currently make up a relatively small portion of XYZ Corporation 's business base, however, substantial growth is foreseen in this area. For this reason, management directed the OIS to research any issue that could potentially result in a conflict. This research lead to the decision to adapt OMB Circular A-130 as a compliance document for all US Government work and as a general-purpose guideline for all other work. For that reason, "A-130" is referenced within numerous security test procedures following in this document.

In validating the decision mentioned above, the following excerpt is taken directly from OMB Circular A-130:

"This Circular is issued pursuant to the Paperwork Reduction Act (PRA) of 1980, as amended by the Paperwork Reduction Act of 1995 (44 U.S.C. Chapter 35); the Privacy Act, as amended (5 U.S.C. 552a); the Chief Financial Officers Act (31 U.S.C. 3512 et seq.); the Federal Property and Administrative Services Act, as amended (40 U.S.C. 759 and 487); the Computer Security Act (40 U.S.C. 759 note); the Budget and Accounting Act, as amended (31 U.S.C. Chapter 11); Executive Order No. 12046 of March 27, 1978; and Executive Order No. 12472 of April 3, 1984."

3 SECURITY TEST CONTROLS – MANAGEMENT CONTROLS

This section of the document describes the Security Test Criteria (STC) of the Management Controls for the XYZ Corporation's HRPayroll. The STC attempts to validate the system in terms of the Risks associated with System/Information Integrity, Data Confidentiality and System Availability.

3.1 Risk Assessment and Management

3.1.1 System/Information Integrity Risk Assessment

References:

NIST SP 800-18	**Subsection 3.7.2, Section 4.1, Section 4.2, Paragraph 3**
ISO 15408	**Family/Class FDP_IFC.2.2**
CobiT P02	**2.2 Corporate Data Dictionary and Data Syntax Rules**
	2.3 Data Classification Scheme
	2.4 Security Levels
CobiT P09	**Assess Risks**
OMB A-130	**Appendix III, Section B, Paragraph 5**
STC-I-MC-01	Confirm the existence of Data Item Definitions (DID)s by receiving them in the Office of Information Security (OIS) for review.
STC-I-MC-02	Confirm the existence of Data Flow Diagrams (DFD)s by receiving them in the Office of Information Security (OIS) for review.
STC-I-MC-03	Confirm the existence of the Software Requirements Specifications (SRS) document by receiving it in the Office of Information Security (OIS) for review.
STC-I-MC-04	Confirm the existence of a Description of External Interfaces by receiving it in the Office of Information Security (OIS) for review.
STC-I-MC-05	Confirm the existence of a High Level Design by receiving it in the Office of Information Security (OIS) for review.
STC-I-MC-06	Confirm the existence of the System Administrators Guide (SAG) by receiving it in the Office of Information Security (OIS) for review.
STC-I-MC-07	Confirm the existence of the Security Features User Guide (SFUG) by receiving it in the Office of Information Security (OIS) for review.

3.1.2 Data Confidentiality Risk Assessment

References:

NIST SP 800-18	**Subsection 3.7.2**
CobiT P02	**2.2 Corporate Data Dictionary and Data Syntax Rules** **2.3 Data Classification Scheme** **2.4 Security Levels**
STC-I-MC-08	Confirm the existence of a Configuration Management Plan by receiving it in the Office of Information Security (OIS) for review.
STC-I-MC-09	Confirm the existence of Delivery Procedures by receiving them in the Office of Information Security (OIS) for review.
STC-I-MC-10	Confirm the existence of Installation and Start-up Procedures by receiving them in the Office of Information Security (OIS) for review.
STC-I-MC-11	Confirm the existence of Procedures for labeling and storing media by receiving them in the Office of Information Security (OIS) for review.
STC-I-MC-12	Confirm the existence of Procedures for disposal of damaged Media by receiving them in the Office of Information Security (OIS) for review.

3.1.3 System Availability Risk Assessment

Reference: NIST SP 800-18, Subsection 3.7.2, Section 4.2, Paragraph 3

STC-I-MC-13 Confirm that the system allows expedient and consistent access for all operator types.

1. Access the system from a workstation
2. Confirm that the system allows access
3. Record the lapse of time to complete the logon process

Repeat the above steps for each of the following operator types:

1. Personnel Assistant
2. Personnel Manager
3. Personnel Management Specialist
4. Personnel Officer
5. Super TimeKeeper
6. TimeKeeper

3.2 Review of Security Controls

Compliance Criteria:

NIST SP 800-18	**Section 4.2, Review of Security Controls**
OMB A-130	**Appendix III A.3.B.b. Controls for Major Applications**
ISO15408	**Family/Class FDP, ADV, Development**

3.2.1 System/Information Integrity Risk Assessment

References:

NIST SP 800-18	**Subsection 3.7.2, Section 4.2, Paragraph 3**
ISO 15408	**Family/Class FDP_IFC.2.2**

STC-I-MC-14 Validate Data Item Definitions (DID)s by reviewing them in the Office of Information Security (OIS).

STC-I-MC-15 Validate Data Flow Diagrams (DFD)s by reviewing them in the Office of Information Security (OIS).

STC-I-MC-16 Validate the Software Requirements Specifications (SRS) document by reviewing it in the Office of Information Security (OIS).

STC-I-MC-17	Validate the Description of External Interfaces by reviewing it in the Office of Information Security (OIS).
STC-I-MC-18	Validate the High Level Design by reviewing it in the Office of Information Security (OIS).
STC-I-MC-19	Validate the System Administrators Guide (SAG) by reviewing it in the Office of Information Security (OIS).
STC-I-MC-20	Validate the Security Features User Guide (SFUG) by reviewing it in the Office of Information Security (OIS). Confirm that security test criteria addressed by the SFUG complies with the following: 1. Contains warnings about user-accessible functions and privileges that should be controlled in a secure operating environment 2. Clearly presents user responsibilities for secure operation 3. Does not provide conflicting information, i.e., implies different outcomes when the same input is supplied 4. Does not provide misleading or incomplete information

3.2.2 Data Confidentiality Risk Assessment

References:

NIST SP 800-18	**Subsection 3.7.2, Section 4.2, Paragraph 3**
STC-I-MC-21	Validate the Configuration Management Plan by receiving it in the Office of Information Security (OIS) for review.
STC-I-MC-22	Confirm that measures are in place such that only authorized changes are made to configuration items.
STC-I-MC-23	Validate Delivery Procedures by reviewing them in the Office of Information Security (OIS).
STC-I-MC-24	Validate Installation and Start-up Procedures by reviewing them in the Office of Information Security (OIS).
STC-I-MC-25	Validate Procedures for labeling and storing media by reviewing them in the Office of Information Security (OIS).
STC-I-MC-26	Validate Procedures for disposal of damaged Media by reviewing them in the Office of Information Security (OIS) .
STC-I-MC-27	Confirm that a policy is in place so that visiting maintenance/service personnel are subject to the following: 1. Required to sign-in upon arrival 2. Placed under constant supervision while on premises 3. Prohibited from running remote diagnostics 4. Required to complete a descriptive log of activities conducted on the premises 5. Required to sign-out upon departure using the same location where the sign-in was accomplished 6. Are subject to inspection upon departure

3.2.3 System Availability Risk Assessment

Reference: NIST SP 800-18, Subsection 3.7.2, Section 4.2, Paragraph 3

STC-I-MC-28 Confirm Personnel Assistant operator class accesses as follows:

1. HR and Base Benefits - Access to employee level data
2. HRPayroll - No Access
3. Time and Labor - No Access

STC-I-MC-29 Confirm that the Personnel Assistant operator class can access employee level data and is able to perform the following:

1. Add
2. Update Display
3. Update Display All
4. Correction

STC-I-MC-30 Confirm Personnel Manager operator class accesses as follows:

1. HR and Base Benefits - Access to employee level data
2. HRPayroll - No Access
3. Time and Labor - No Access

STC-I-MC-31 Confirm that the Personnel Manager operator class can access employee level data and is able to perform the following:

1. Reports and Query
2. Add
3. Update Display
4. Update Display All
5. Correction

STC-I-MC-32 Confirm Personnel Management Specialist operator class accesses as follows:

1. HR and Base Benefits - Access to employee level data
2. HRPayroll - No Access
3. Time and Labor - No Access

STC-I-MC-33 Confirm that the Personnel Management Specialist operator class can access employee level data and is able to perform the following:

1. Add
2. Update Display
3. Update Display All

STC-I-MC-34 Confirm Personnel Management Specialist operator class accesses as follows:

1. HR and Base Benefits - Access to employee level data
2. HRPayroll - No Access
3. Time and Labor - No Access

STC-I-MC-35 Confirm that the Personnel Management Specialist operator class can access employee level data and is able to perform the following:

4. Add
5. Update Display
6. Update Display All

STC-I-MC-36 Confirm Personnel Officer (PO) operator class accesses as follows:

1. HR and Base Benefits - Access to employee level data for location
2. HRPayroll - No Access
3. Time and Labor - No Access

STC-I-MC-37 Confirm that the Personnel Manager operator class can access employee level data and is able to perform the following:

1. Reports and Query
2. Add
3. Update Display
4. Update Display All
5. Correction

STC-I-MC-38 Confirm Super TimeKeeper operator class accesses as follows:

1. HR and Base Benefits - No Access
2. HRPayroll - No Access
3. Time and Labor - Access to employee level data for input and correction only

STC-I-MC-39 Confirm that the Super TimeKeeper operator class can access employee level data and is able to perform the following:

1. Input only

STC-I-MC-40 Confirm Super User (HQ) operator class accesses as follows:

1. HR/Base Benefits - Access to employee level data corporate-wide
2. HRPayroll - Access to employee level data corporate-wide
3. Time and Labor - Access to employee level data corporate-wide

STC-I-MC-41 Confirm that the Super User (HQ) operator class can access employee level data and is able to perform the following:

1. Reports and Query
2. Add
3. Update Display
4. Update Display All
5. Correction
6. View only for tables

STC-I-MC-42 Confirm Super User (Field) operator class accesses as follows:

1. HR/Base Benefits - Access to employee level data for Location
2. HRPayroll - Access to employee level data for entire Location
3. Time and Labor - Access to employee level data for Location

STC-I-MC-43 Confirm that the Super User (Field) operator class can access employee level data and is able to perform the following:

1. Reports and Query
2. Add
3. Update Display
4. Update Display All
5. Correction
6. View only for tables

STC-I-MC-44 Confirm TimeKeeper operator class accesses as follows:

1. HR and Base Benefits - No Access
2. HRPayroll - No Access
3. Time and Labor - Access to employee level data for input

STC-I-MC-45 Confirm that the TimeKeeper operator class can access employee level data and is able to perform the following:

1. Input only

3.3 Security Audit Guidelines

3.3.1 System/Information Integrity Risk Assessment

References:

NIST SP 800-18	**6.MA.4, Audit Trails**
OMB A-130	**Appendix III, B.3) Review of Security Controls**
ISO15408	**Family/Class FAU, Security Audit**

STC-I-MC-46 Review the System Administrator's Guide (SAG) to confirm that mechanisms are in place to ensure the following events will trigger an audit record:

1. User login, both successful and failed
2. Attempts to access objects denied by lack of privileges/rights
3. Successful access to security-critical items
4. Changes to user's privileges/profiles
5. Changes to system security configuration
6. Modification to system-supplied software
7. Creation/deletion of objects

STC-I-MC-47 Confirm that mechanisms are in place to ensure each audit record will contain at least the following:

1. Date and time of the event
2. Type of event
3. Subject identity,
4. The outcome (success or failure) of the event
5. The functional components included

3.3.2 Data Confidentiality Risk Assessment

References:

NIST SP 800-18	**6.MA.4, Audit Trails**
OMB A-130	**Appendix III, B.3) Review of Security Controls**
ISO15408	**Family/Class FAU, Security Audit**
STC-I-MC-48	Confirm that the PayMint system is able to protect the stored audit records from unauthorized deletion and be able to prevent and/or detect modifications to the audit records.
STC-I-MC-49	Confirm that the PayMint system is able to overwrite the oldest stored audit records in the event that storage space is exhausted.

3.3.3 System Availability Risk Assessment

References:

NIST SP 800-18	**6.MA.4, Audit Trails**
OMB A-130	**Appendix III, B.3) Review of Security Controls**
ISO15408	**Family/Class FAU, Security Audit**
STC-I-MC-50	Confirm that only authorized individuals can access audit Records
STC-I-MC-51	Confirm that the system is capable of maintaining profiles of system usage, where an individual user profile represents the historical patterns of usage by individual members
STC-I-MC-52	Confirm that the system is capable of maintaining a suspicion rating associated with each user whose activity is recorded in a profile, where the suspicion rating represents the degree to which the user's current activity is found inconsistent with the established patterns of usage represented in the profile.
STC-I-MC-53	Confirm that the system is capable of indicating an imminent violation of system when a user's suspicion rating exceeds defined threshold conditions

3.4 Rules of Behavior

3.4.1 System/Information Integrity Risk Assessment

References:

NIST SP 800-18	**Section 4.3, Rules of Behavior**
OMB A-130	**Appendix III.A.3.,2) System Security Plan. a) Rules of the System**
ISO15408	**Family/Class FMT, Security Management**
STC-I-MC-54	Ensure that all personnel accessing PayMint have been advised on the availability of The Security Awareness training package and how to access it.
STC-I-MC-55	Ensure that all personnel accessing PayMint have been issued written copies of the rules of behavior and have submitted signature pages.
STC-I-MC-56	Ensure that all personnel accessing PayMint will be notified as revisions to the rules of behavior or policy documents containing the rules of behavior occur.

3.4.2 Data Confidentiality Risk Assessment

References:

NIST SP 800-18	**Section 4.3, Rules of Behavior**
OMB A-130	**Appendix III.A.3.,2) System Security Plan. a) Rules of the System**
ISO15408	**Family/Class FMT, Security Management**
STC-I-MC-57	Identify all job functions where dial-in access may be allowed, and all users assigned to those job functions. Verify the methodology by which call logs are to be maintained.
STC-I-MC-58	Confirm that users have been notified that non-compliance of rules will be enforced through sanctions commensurate with the level of infraction.
STC-I-MC-59	Confirm that users have been notified that the Office of Information Security (OIS) is responsible for ensuring an adequate level of protection by means of technical, administrative, and managerial controls; policies and procedures; awareness sessions; inspections and spot checks; periodic vulnerability analyses.
STC-I-MC-60	Confirm that users have been notified that the rules are not to be used in place of existing policy, rather they are intended to enhance and further define the specific rules each user must follow while accessing PayMint.

STC-I-MC-61	Confirm that users have been notified about the rules governing Work-at-Home Arrangements
STC-I-MC-62	Confirm that users have been notified about the rules governing Dial-in Access
STC-I-MC-63	Confirm that users have been notified about the rules governing Connection to the Internet
STC-I-MC-64	Confirm that users have been notified about the rules governing Protection of Software Copyright :Licenses
STC-I-MC-65	Confirm that users have been notified about the rules governing Unofficial Use of Government Equipment

3.4.3 System Availability Risk Assessment

References:

NIST SP 800-18	**Section 4.3, Rules of Behavior**
OMB A-130	**Appendix III.A.3.,2) System Security Plan. a) Rules of the System**
ISO15408	**Family/Class FMT, Security Management**
STC-I-MC-66	Identify the methodology whereby each dial-in access call will use a one-time password. Confirm that passwords used in this manner cannot be repeated and/or duplicated.
STC-I-MC-67	Identify all job functions requiring access to the Internet. Confirm that where such access is allowed, all external connections are carefully documented and a copy provided to the OIS. Identify how the OIS will be notified of external connection updates
STC-I-MC-68	Confirm that all work-at-home arrangements comply with the following conditions: 1. Each arrangement is in writing 2. Identifies clearly the time period the work at home will be allowed 3. Identifies the government equipment and supplies needed by the employee at home, and how that equipment and supplies will be transferred and accounted for 4. Identifies if telecommuting will be needed and allowed. 5. Is made available for review by the Office of Information Security (OIS) prior to commencement

4 SECURITY TEST CRITERIA - OPERATIONAL CONTROLS

4.1 Personnel Security

XYZ Corporation has in place specific procedures for evaluating the sensitivity levels required for all positions coming into contact with the HRPayroll system. These procedures include comprehensive background screenings commensurate with the level of information handled by the HRPayroll system. XYZ Corporation also has in place specific procedures for administering all aspects of user accounts, division of functional tasks, user accountability and traceability. Specific procedures related to user monitoring, accountability, non-prejudicial and prejudicial disciplinary actions/termination are already in place at Mint facilities. These procedures shall be understood to apply to all personnel having access to HRPayroll . Personnel privacy shall be maintained in accordance with both the Common Criteria and legislated requirements.

4.1.1 Position Sensitivity and Access Limitation

Compliance Criteria:

NIST SP 800-18	**5.MA.1, Personnel Security, Paragraph 3, Position Sensitivity Analysis**
OMB A-130	**9.f.3**
ISO 15408	**Family/Class FMT_SMR, Security Management Roles**

All positions having access to HRPayroll shall be reviewed for sensitivity. Access will be limited to the minimum necessary to perform job-related tasks and shall be compliant with CSD Level 2 as a minimum.

STC-I-OC-01 Provide a listing of all positions having access to HRPayroll . Include the following:

1. Position title
2. Sensitivity level
3. Number of incumbents in the position
4. Number of vacancies for the position
5. Projection for growth of the position (10-year projection preferred)

4.1.2 Personnel Background Investigations

Compliance Criteria:

NIST SP 800-18	**5.MA.1, Personnel Security, Paragraph 4, Screening**
ISO 15408	**Family/Class FMT, Security Management**

STC-I-OC-02 Confirm that all personnel having HRPayroll access have undergone background investigations.

1. Provide an up-to-date list of all persons having HRPayroll access showing the date a background investigation was completed.
2. Confirm that system access is limited to only personnel who have a completed background investigation.
3. Confirm that system access is denied personnel whose background investigations are pending or incomplete.
4. Confirm that personnel background investigation information is backed up in a redundant file, that the file is up-to-date, and is stored in a safe location off-site.

4.2 Physical Security

Compliance Criteria:

NIST SP 800-18 **OMB A-130**	**5.MA.2. Physical and Environmental Protection** **Section 4.c.(3).(b).4**
STC-I-OC-03	Confirm compliance of entry and egress points with respect to the following items (Reference NIST SP 800-18, 5.MA.2.1, Explanation of Physical and Environmental Security, Paragraph 1, Access Controls): 1. Entrance doors are of solid material and at least 1-3/4 inches thick 2. Hinge pins are modified to prevent removal 3. Deadbolts are installed on all doors 4. Perimeter walls are slab-to-slab and attached to floor and ceiling 5. Ground level and second story windows are positive locking devices and not equipped with spring-loaded latches 6. Availability of escorts for unauthorized personnel 7. Availability and accuracy of sign-in and sign-out logs
STC-I-OC-04	Confirm compliance of locks with respect to the following items (Reference NIST SP 800-18, 5.MA.2.1, Explanation of Physical and Environmental Security, Paragraph 1, Access Controls): 1. Limitations on distribution of keys 2. Cipher lock combinations are changed at least every six months or more frequently 3. Cipher lock combinations are changed in the event of a resignation, termination, or attempted break-in 4. Cipher lock combinations use four or more numbers 5. Cipher lock mechanisms are shielded from view

STC-I-OC-05 Confirm that emergency backup power is available for (Reference NIST SP 800-18, 5.MA.2.1, Explanation of Physical and Environmental Security, Paragraph 3, Failure of Supporting Utilities):

1. Servers
2. Administrative workstations
3. Emergency evacuation lighting
4. Intrusion detection devices
5. Fire alarms

4.3 Production, Input/Output Controls

Compliance Criteria:

NIST SP 800-18	**5.MA.3, Production, Input/Output Controls**
OMB A-130	**Appendix III A.3.B.b. Controls for Major Applications**
ISO15408	**Family/Class FAU, FDP, FIA**

The following section addresses the controls used for the marking, handling, processing, storage, and disposal of input and output information and media, as well as labeling and distribution procedures for the information and media. In addition, the controls used to monitor the installation of, and updates to, software are listed. This section also describes the procedures, planned or in place, to support the system.

4.3.1 User Support and Access Controls - Electronic Information

Reference: NIST SP 800-18, Section 5.MA.3, Production, Input/Output Controls, Paragraphs 3,4,6.

Ensure that unauthorized individuals cannot read, copy, alter, or steal printed or electronic information.

STC-I-OC-06 Verify the following and report the findings. The system is able to:

1. Enforce access control on all system resources
2. Explicitly authorize access to resources based on attributes
3. Explicitly deny access to resources based on attributes
4. Export data without the user/sender's associated security attributes
5. Control information flow by selecting the most stringent security attribute where multiple security attributes exist in a given object.
6. Provide residual information protection, i.e., ensure that previous information content of a resource is made unavailable upon the completion of each transaction
7. Maintain stored data integrity
8. Maintain data exchange confidentiality
9. Detect and log authentication failures
10. Maintain security attribute definitions
11. Successfully identify and authenticate legitimate users/groups

4.3.2 User Support and Access Controls - Printed Information and Media

Reference: NIST SP 800-18, Section 5.MA.3, Production, Input/Output Controls, Paragraph 14

STC-I-OC-07 Verify the following and report the findings. Describe and verify the procedures in place to deal with:

1. Labeling, marking, transporting, and storing Sensitive But Unclassified (SBU) materials both within XYZ Corporation property and aboard public conveyances
2. Report and disposition security violations or the perception of security violations
3. Declassification reviews
4. Identifying and authenticating credentials such as badges and shields
5. Courier activities
6. Periodic changes of combinations
7. Defense Investigative Service DD Form 254 compliance
8. Properly classifying written materials and media to the most stringent applicable classification

4.3.3 Input/Output Audit Trails

Reference: NIST SP 800-18, Section 5.MA.3, Production, Input/Output Controls, Paragraph 10

STC-I-OC-08 Verify the following and report the findings:

1. Auditable events can be associated with individual user identities
2. The system can generate a record of start-up and shut-down of auditable functions
3. The system can maintain a profile of system usage
4. The system can maintain a suspicion rating associated with each user whose activity is recorded in a profile
5. The system can warn of an imminent violation when a user's suspicion rating exceeds a discretionary threshold
6. The system is able to provide audit records to authorized users
7. The system provides the capability to perform selective queries, searches, and ordering of audit data
8. The system can protect stored audit records from unauthorized access, modification, and deletion
9. The system can issue appropriate notifications when audit records approach a set threshold

STC-I-OC-09 Verify that each audit record contains, as a minimum, the following:

1. Date and time of the event
2. Type of event
3. Subject (user/group) identity
4. Outcome (success or failure) of the event

4.4 Contingency Planning

Compliance Criteria:

NIST SP 800-18	**5.MA.4, 5.MA.6, 5.MA.7, 5.MA.8**
OMB A-130	**Appendix III A. 3.b.2.d), Contingency Planning**
ISO15408	**Family/Class FPT_PHP, Physical Protection**

4.4.1 Business Continuity and Contingency Plan (BCCP)

Reference; NIST SP 800-18, Section 5.MA.4, Paragraph 1

STC-I-OC-10 Review the BCCP for possible disagreements with compliance documents and for updates needed to address unique HRPayroll requirements.

4.4.2 Disaster Recovery Plan (DRP)

Reference; NIST SP 800-18, Section 5.MA.4, Paragraph 2

STC-I-OC-11 Review the DRP for possible disagreements with compliance documents and for updates needed to address unique HRPayroll requirements.

4.5 Application Software Maintenance Controls

Compliance Criteria:

NIST SP 800-18	**5.MA.5, Application Software Maintenance Controls,** **5.MA.6 Data Integrity/Validation Controls** **5.MA.7, Documentation** **5.MA.8, Security Awareness and Training**
OMB A-130	**Appendix III A.3.B.b. Controls for Major Applications**
ISO 15408	**Family/Class FCO, FDP, and FIA**

4.5.1 Formal Change Control Process

Reference: NIST SP 800-18, Section 5.MA.5, Paragraph 7

STC-I-OC-12 A formal change control process is in place. Review this process for possible disagreements with compliance documents and for updates needed to address unique HRPayroll requirements.

4.5.2 Illegal Use of Copyrighted Software

Reference: NIST SP 800-18, Section 5.MA.6, Paragraphs 6,13

STC-I-OC-13 Existing XYZ Corporation organizational policies prohibit the illegal use of copyrighted software and shareware. Review the procedures for possible disagreements with system design documents.

4.5.3 Virus Remediation Software

Reference: NIST SP 800-18, Section 5.MA.7, Paragraph 3

STC-I-OC-14 Existing XYZ Corporation operating procedures and practices require the availability and use of virus remediation software on all systems.
Investigate and confirm that such software does not inhibit, interfere with, or weaken the required security functionality.

4.5.4 Penetration Testing

Reference: NIST SP 800-18, Section 5.MA.6, Paragraphs 5,8

STC-I-OC-15 Arrange for separate (independent) penetration testing, which may be done as part of the system functional testing or at a time following the completion of system functional testing. Successful penetration testing will be necessary before the system can be authenticated and released to active duty.

4.5.5 Documentation

Reference: NIST SP 800-18, Section 5.MA.7, Entire Section

STC-I-OC-16 Review all Documentation for the HRPayroll system including descriptions of the hardware and software, policies, standards, and procedures. Identify and remediate conflicts as needed.

4.5.6 Security Awareness and Training

Reference: NIST SP 800-18, Section 5.MA.8, Entire Section

STC-I-OC-17 The XYZ Corporation requires all employees to take the Corporate Security Awareness training at least once a year. The Corporate Intranet provides an online security awareness-training package. Confirm that this is available to all personnel accessing the HRPayroll system.

Confirm that all personnel accessing HRPayroll are aware of or have completed and have acknowledged completion of this package.

The Security Awareness training package can be found on the XYZ Corporation's Intranet at http://xyzcorporate/training/html.

5 SECURITY TEST CRITERIA - TECHNICAL CONTROLS

5.1 Identification and Authentication

The Common Criteria, Family/Class FIA, states that " Identification and Authentication is required to ensure that users are associated with the proper security attributes (e.g. identity, groups, roles, security or integrity levels).

5.1.1 Passwords

Compliance Criteria:

NIST SP 800-18	**6.MA.1**
OMB A-130	**Appendix III A.3.B.b. Controls for Major Applications**
ISO15408	**Family/Class FIA and FTA**

The XYZ Corporation rules for passwords are:

a) XYZ Corporation assigns each new user a temporary password, which the user is prompted to change when first logging onto XYZ Corporation network.
b) A maximum of 64 characters.
c) Passwords must be changed at least once every 40 days. The user is reminded to change his or her password by the system starting ten days before the change is required.
d) Can the same password be used again. – NO.
e) The Security Administrator is notified when an employee resigns or has been terminated and ensures that the former employee's password has been removed from the system.
f) Passwords are associated with a user ID that is assigned to an individual person.
g) The user is disconnected from the Corporate network for ten minutes after five invalid attempts to log on.
h) Password files are encrypted and are not available from the system.
i) If users forget their password, the Security Administrator will reset the user account to a temporary password. The user will be prompted to change the temporary password when logging on again.
j) If a password is compromised the Security Administrator must be notified so that the password can be reset.
k) The identification and resolution of all other remaining I&A issues are TBD.

STC-I-TC-01	Ensure that all personnel accessing HRPayroll have completed The Security Awareness training package and acknowledge and understanding of password requirements.
STC-I-TC-02	Validate Secure Logon from the Workstation, Confirm Identification/Authentication is

1. Accepted using known valid User ID and VALID password
2. Declined using known valid User ID and INVALID password
3. Declined using known INVALID User ID and VALID password
4. Declined using known INVALID User ID and INVALID password

Logical Access Controls

Compliance Criteria:

NIST SP 800-18	**6.MA.2**
OMB A-130	**Appendix III A.3.B.b. Controls for Major Applications**
ISO15408	**Family/Class FCO**

5.2.1 Common Criteria Non-repudiation Requirements

The Common Criteria, Family/Class FCO: Communication, sets forth specific non-repudiation requirements.

5.2.1.1 Non-repudiation of Origin

Reference: ISO 15408 Family/Class FCO_NRO, Non-repudiation of Origin

Non-repudiation of origin defines requirements to provide evidence to users/subjects about the identity of the originator of some information. The originator cannot successfully deny having sent the information because evidence of origin (e.g. digital signature) provides evidence of the binding between the originator and the information sent. The recipient or a third party can verify the evidence of origin. This evidence should not be forgeable.

5.2.1.2 Non-repudiation of Receipt

Reference: ISO 15408 Family/Class FCO_NRR, Non-repudiation of Receipt

Non-repudiation of receipt defines requirements to provide evidence to users/subjects that the information was received by the recipient. The recipient cannot successfully deny having received the information because evidence of receipt (e.g. digital signature) provides evidence of the binding between the recipient attributes and the information. The originator or a third party can verify the evidence of receipt. This evidence should not be forgeable.

STC-I-TC-03	Confirm that within HRPayroll , originators and recipient cannot deny sending or receiving information.

5.2.2 Operator Class Permissions

Reference: NIST SP 800-18, Section 6.MA.2, Logical Access Controls

The HRPayroll system has very specific role-based operator permissions.

STC-I-TC-04 Validate Operator Class User permissions

For each operator class select a known valid user.
Access a record for each category and confirm the following:

1. Record can be accessed with DISPLAY ONLY Access operation where permission is granted
2. Record cannot be accessed with DISPLAY ONLY Access operation where permission is denied

3. Record can allow an ADD operation where permission is granted
4. Record cannot allow an ADD operation where permission is denied

5. Record can allow an UPDATE/DISPLAY operation where permission is granted
6. Record cannot allow an UPDATE/DISPLAY operation where permission is denied

7. Record can allow an UPDATE/DISPLAY ALL operation where permission is granted
8. Record cannot allow an UPDATE/DISPLAY ALL operation where permission is denied

9. Record can allow a CORRECTION operation where permission is granted
10. Record cannot allow a CORRECTION operation where permission is denied

5.3 Public Access Controls

Compliance Criteria:

NIST SP 800-18	**6.MA.3, Public Access Controls**
OMB A-130	**Appendix III A.3.B.b. Controls for Major Applications**

The HRPayroll system is not designed or intended for public access.

STC-I-TC-05	Ensure that public access via the Internet is impossible

5.4 Audit Trails

Compliance Criteria:

NIST SP 800-18	**6.MA.4, Audit Trails**
OMB A-130	**Section 8.2 Records Management**
ISO15408	**Family/Class FAU and FIA**

Security auditing involves recognizing, recording, storing, and analyzing information related to security relevant activities. The resulting audit records can be examined to determine which security relevant activities took place and who (which user) is responsible for them.

5.4.1 Audit Data Generation with Identity

Reference: NIST SP 800-18, Section 6.MA.4, Paragraphs 13, 14

STC-I-TC-06 Confirm that the following events will trigger an audit record:

1. User login, both successful and failed
2. Attempts to access objects denied by lack of rights
3. Successful access to security-critical items
4. Changes to user's profiles
5. Changes to system security configuration
6. Modification to system-supplied software
7. Creation/deletion of objects

STC-I-TC-07 Confirm that mechanisms are in place to ensure each audit record will contain at least the following:

Reference: NIST SP 800-18, Section 6.MA.4, Paragraph 6

1. Date and time of the event
2. Type of event
3. Subject identity,
4. The outcome (success or failure) of the event
5. The functional components included

5.4.2 Accountability

Reference: NIST SP 800-18, Section 6.MA.4, Paragraph 2

The Common Criteria requires traceability through Family/Class FIA, Identification and Authentication which states that " The unambiguous identification of authorized users and the correct association of security attributes with users and subjects is critical to the enforcement of the intended security policies. The families in this class deal with determining and verifying the identity of users, determining their authority to interact with the TOE, and with the correct association of security attributes for each authorized user. Other classes of requirements (e.g. User Data Protection, Security Audit) are dependent upon correct identification and authentication of users in order to be effective."

STC-I-TC-08 Confirm the identity of all users

STC-I-TC-09 Identify the user's authority (permissions) to interact with the system

STC-I-TC-10 Confirm the correctness of security attributes associated with each authorized user

5.4.5 Audit Review Requirements

Reference: NIST SP 800-18, Section 6.MA.4, Entire Section

STC-I-TC-11 Confirm that the system is capable of the following:

1. The capability to allow reading information from the audit records.
2. No other users except those that have been specifically identified can read the information.
3. The availability of audit review tools to select the audit data to be reviewed based on criteria (i.e., queries, sorts, etc.)

6 SECURITY TEST REPORT

This section reserved for a future project

6.1 Findings

6.2 Discussion

6.2.1 Risks

6.2.2 Mitigating Actions

6.3 Recommendations

APPENDIX A
WEB-BASED REFERENCES

Security Plan Development

National Institute of Standards and Technology (NIST) Special Publication 800-18
Guide for Developing Security Plans for Information Technology Systems,
December 1998
http://csrc.nist.gov/publications/nistpubs/

Information Systems Auditing

IT Governance Institute
CobiT (COntrol oBjectives for Information and related Technology)
Audit Guidelines, 3rd Edition, July 2000
http://www.Itgovernance.org

Information Systems Audit and Control Association (ISACA)
IS Auditing Guideline, 1999
http://www.isaca.org/

Information Systems Test Criteria

International Standards Organization
ISO 15408 Common Criteria
http://csrc.nist.gov/cc/

Software Quality Control and Systems Management Best Practices

The American Society for Quality Home Page
http://www.asq.org

The American Society for Quality Code of Ethics
http://www.asq.org/join/about/ethics.html

APPENDIX B
BIBLIOGRAPHIC REFERENCES

Frank, Marriott, and Warzusen, The Software Quality Engineer Primer, Quality Council of Indiana, Second Edition, April 2000

Parsowith, Scott B., Fundamentals of Quality Auditing, ASQ Quality Press, Milwaukee, WI, ISBN 0-87389-240-2, 1995

Shim, Siegel, Operations Management, Barron's Educational Series, Inc., ISBN 0-7641-0510-8, 1999

Swanson, Marianne, Guide for Developing Security Plans for Information Technology Systems, National Institute of Standards and Technology (NIST), Special Publication 800-18, December 1998

Anderson, Caldwell, Needles, Financial and Managerial Accounting, A corporate Approach, Houghton Mifflin Company, Boston, MA, ISBN: 0-395-72221-7

International Standards Organization, ISO 15408, Common Criteria for Information Technology Security Evaluation, CCIMB-99, 1999

APPENDIX C
ACRONYMS

AICPA	American Institute of Certified Public Accountants
CC	The ISO 15408 Common Criteria
FASB	Financial Accounting Standards Board
FOUO	For Official Use Only
HR	Human Resources
ISACA	Information System Audit and Control Association
ISO	International Standards Organization
ISSO	Information Systems Security Office
IT	Information Technology
MC	Management Control
NIST	National Institute of Standards and Technology (US Gov. Agency - Dept. of Commerce)
OC	Operational Control
OIT	Office of Information Technology
OMB	Office of Management and Budget (US Government Agency - White House)
STC	Security Test Control (used in conjunction with MC, OC, TC)
TC	Technical Control
TOE	Target of Evaluation (from ISO 15408)
TSF	TOE Security Function (from ISO 15408)

APPENDIX D

Table of Contents NIST SP 800-18

APPENDIX E - Correlation Between NIST SP 800-18 and CobiT

Table E-1

NIST 800 18 Para.	NIST 800 18 Title	CobiT Sect.	CobiT Topic	CobiT Subtopic	
2	System Analysis				
2.1	System Boundaries	PO6	Communicate Management Aims and Direction	6.4	Policy Implementation Resources
				6.8	Security and Internal Control Framework Policy
		PO2	Define the Information Architecture	2.1	Information Architecture Model
2.2	Multiple Similar Systems	PO10	Manage Projects	10.1	Project Management Framework
2.3	System Category	PO1	Define a Strategic IT Plan	1.2	IT Long-Range Plan
2.3.1	Major Applications	PO1	Define a Strategic IT Plan	1.3	IT Long-Range Planning—Approach and Structure
2.3.2	General Support System	PO1	Define a Strategic IT Plan	1.5	Short-Range Planning for the IT Function
3	Plan Development – All Systems	PO1	Define a Strategic IT Plan	1.1	IT as Part of the Organization's Long- and Short-Range Plan
3.1	Plan Control	PO1	Define a Strategic IT Plan	1.6	Communication of IT Plans
		PO6	Communicate Management Aims and Direction	6.3	Communication of Organization Policies
3.2	System Identification	N/A	N/A	N/A	N/A
3.2.1	System Name/Title	N/A	N/A	N/A	N/A
3.2.2	Responsible Organization	PO4	Define the IT Organization & Relationships	4.1	IT Planning or Steering Committee
3.2.3	Information Contact(s)	PO4	Define the IT Organization & Relationships	4.4	Roles and Responsibilities
3.2.4	Assignment of Security Responsibility	PO4	Define the IT Organization & Relationships	4.6	Responsibility for Logical and Physical Security
3.3	System Operational Status	DS3	Manage Performance and Capacity	3.5	Proactive Performance Management
3.4	General Description/Purpose	AI1	Identify Automated Solutions	1.1	Definition of Information Requirements
		PO6	Communicate Management Aims & Direction	6.3	Communication of Organization Policies
				6.11	Communication of IT Security Awareness
3.5	System Environment	PO3	Determine Technological Direction	3.1	Technological Infrastructure Planning
3.6	System Interconnection/Information Sharing	AI3	Acquire and Maintain Technology Infrastructure	3.3	System Software Security
				3.5	System Software Maintenance
				3.6	System Software Change Controls
				3.7	Use and Monitoring of System Utilities

Table E-1 (Continued)

Para.	NIST 800 18 Title	Sect.		CobiT Topic	CobiT Subtopic
3.7	Sensitivity of Information Handled	PO2	Define the Information Architecture		See 2.3, 2.4 below
3.7.1	Laws, Regulations, and Policies Affecting the System	PO8	Ensure Compliance with External Requirements		
3.7.2	General Description of Sensitivity	PO2	Define the Information Architecture	2.2	Corporate Data Dictionary & Data Syntax Rules
				2.3	Data Classification Scheme
				2.4	Security Levels
4	Management Controls				
4.1	Risk Assessment and Management	PO9	Assess Risks	9.1	Business Risk Assessment
				9.2	Risk Assessment Approach
				9.3	Risk Identification
				9.4	Risk Measurement
				9.5	Risk Action Plan
				9.6	Risk Acceptance
				9.7	Safeguard Selection
				9.8	Risk Assessment Commitment
4.2	Review of Security Controls	DS5	Ensure Systems Security	ALL	All Subtopics in this section apply
		DS13	Manage Operations	ALL	All Subtopics in this section apply
4.3	Rules of Behavior	AI4	Develop and Maintain Procedures	ALL	All Subtopics in this section apply
		DS7	Educate and Train Users	ALL	All Subtopics in this section apply
4.4	Planning for Security in the Life Cycle				
4.4.1	Initiation Phase	PO4	Define the IT Organization & Relationships	4.6	Responsibility for Logical & Physical Security
		AI3	Acquire & Maintain Technology Infrastructure	2.17	Reassessment of System Design
		DS9	Manage the Configuration	9.2	Configuration Baseline
4.4.2	Development/Acquisition Phase				
		AI2	Acquire and Maintain Application Software	1.12	Controllability
4.4.3	Implementation Phase			2.14	IT Integrity Provisions . . .

Table E-1 (Continued)

Para.	NIST 800 18 Title	Sect.		CobiT Topic	CobiT Subtopic
4.4.4	Operation/Maintenance Phase	DS13	Manage Operations	ALL	All Subtopics in this section apply
		M1	Monitor the Processes	ALL	All Subtopics in this section apply
		DS11	Manage Data	ALL	All Subtopics in this section apply
		DS8	Assist and Advise Customers	8.1	Help Desk
4.4.5	Disposal Phase	N/A	None Indicated	N/A	None Indicated
4.5	Authorize Processing	M2	Assess Internal Control Adequacy	2.1	Internal Control Monitoring
5	Operational Controls				
5.MA.	Major Application – Operational Controls	AI1	Identify Automated Solutions	1.9	Cost-Effective Security Controls
				1.1	Audit Trails Design
5.MA.1	Personnel Security	PO7	Manage Human Resources	7.6	Personnel Clearance Procedures
5.MA.2	Physical and Environmental Protection	DS12	Manage Facilities	12.1	Physical Security
5.MA.2.1	Explanation of Physical/Environment Security	DS12	Manage Facilities	ALL	All Subtopics in this section apply
5.MA.2.2	Computer Room Example	DS12	Manage Facilities	ALL	All Subtopics in this section apply
5.MA.3	Production, Input/Output Controls	AI2	Acquire and Maintain Application Software	2.7	Input Requiem's Definition & Documentation
				2.11	Output Requiem's Definition & Documentation
5.MA.4	Contingency Planning	DS4	Ensure Continuous Service	ALL	All Subtopics in this section apply
5.MA.5	Application Software Maintenance Controls	DS13	Manage Operations	ALL	All Subtopics in this section apply
		M1	Monitor the Processes	1.2	Assessing Performance
				1.4	Management Reporting
5.MA.6	Data Integrity/Validation Controls	DS11	Manage Data	11.29	Electronic Transaction Integrity
				11.30	Continued Integrity of Stored Data
5.MA.7	Documentation	PO11	Manage Quality	11.11	Program Documentation Standards
		AI2	Acquire and Maintain Application Software	2.4	File Requirements Definition and Documentation
				2.7	Input Requirements Definition and Documentation
				2.10	Processing Requiem's Definition & Documentation
				2.11	Output Requiem's Definition & Documentation
		AI6	Manage Changes	6.5	Documentation and Procedures
		DS13	Manage Operations	13.2	Start-up Process & Other Operations Documentation

Table E-1 (Continued)

NIST 800 18 Para.	NIST 800 18 Title	CobiT Sect.	CobiT Topic	CobiT Subtopic	
5.MA.8	Security Awareness and Training	DS7	Educate and Train Users	7.3	Security Principles & Awareness Training
6.MA	Major Application - Technical Controls	DS5	Ensure Systems Security	ALL	All Subtopics in this section apply
		DS13	Manage Operations	ALL	All Subtopics in this section apply
		M2	Assess Internal Control Adequacy	2.4	Operational Security & Internal Control Assurance
6.MA.1.1	Identification	DS5	Ensure Systems Security	5.2	Identification, Authentication and Access
6.MA.1.2	Authentication	DS5	Ensure Systems Security	5.2	Identification, Authentication and Access
6.MA.2	Logical Access Controls (Authorization/Access Controls)	DS5	Ensure Systems Security	5.1	Manage Security Measures
				5.2	Identification, Authentication and Access
		M2	Assess Internal Control Adequacy	2.4	Operational Security & Internal Control Assurance
6.MA.3	Public Access Controls	DS5	Ensure Systems Security	5.9	Central Identification and Access Rights Management
				5.19	Malicious Software Prevention, Detection & Correction
		DS13	Manage Operations	13.8	Remote Operations
6.MA.4	Audit Trails	M3	Obtain Independent Assurance	ALL	All Subtopics in this section apply
		M4	Provide for Independent Audit	ALL	All Subtopics in this section apply

APPENDIX F
SUMMARY - ISO 15408 CC ELEMENTS

Class	Family	Designator
Class FAU: Security audit	Security audit automatic response	(FAU_ARP)
	Security audit data generation	(FAU_GEN)
	Security audit analysis	(FAU_SAA)
	Security audit review	(FAU_SAR)
	Security audit event selection	(FAU_SEL)
	Security audit event storage	(FAU_STG)
Class FCO: Communication	Non-repudiation of origin	(FCO_NRO)
	Non-repudiation of receipt	(FCO_NRR)
Class FCS: Cryptographic support	Cryptographic key management	(FCS_CKM)
	Cryptographic operation	(FCS_COP)
Class FDP: User data protection	Access control policy	(FDP_ACC)
	Access control functions	(FDP_ACF)
	Data authentication	(FDP_DAU)
	Export to outside TSF control	(FDP_ETC)
	Information flow control policy	(FDP_IFC)
	Information flow control functions	(FDP_IFF)
	Import from outside TSF control	(FDP_ITC)
	Internal TOE transfer	(FDP_ITT)
	Residual information protection	(FDP_RIP)
	Rollback	(FDP_ROL)
	Stored data integrity	(FDP_SDI)
	Inter-TSF user data confidentiality transfer protection	(FDP_UCT)
	Inter-TSF user data integrity transfer protection	(FDP_UIT)
Class FIA: Identification and Authentication	Authentication failures	(FIA_AFL)
	User attribute definition	(FIA_ATD)
	Specification of secrets	(FIA_SOS)
	User authentication	(FIA_UAU)
	User identification	(FIA_UID)
	User-subject binding	(FIA_USB)

Class	Family	Designator
Class FMT: Security management	Management of functions in TSF	(FMT_MOF)
	Management of security attributes	(FMT_MSA)
	Management of TSF data	(FMT_MTD)
	Revocation	(FMT_REV)
	Security attribute expiration	(FMT_SAE)
	Security management roles	(FMT_SMR)
Class FPR: Privacy	Anonymity	(FPR_ANO)
	Pseudonymity	(FPR_PSE)
	Unlinkability	(FPR_UNL)
	Unobservability	(FPR_UNO)
Class FPT: Protection of the TSF	Underlying abstract machine test	(FPT_AMT)
	Fail secure	(FPT_FLS)
	Availability of exported TSF data	(FPT_ITA)
	Confidentiality of exported TSF data	(FPT_ITC)
	Integrity of exported TSF data	(FPT_ITI)
	Internal TOE TSF data transfer	(FPT_ITT)
	TSF physical protection	(FPT_PHP)
	Trusted recovery	(FPT_RCV)
	Replay detection	(FPT_RPL)
	Reference mediation	(FPT_RVM)
	Domain separation	(FPT_SEP)
	State synchrony protocol	(FPT_SSP)
	Time stamps	(FPT_STM)
	Inter-TSF TSF data consistency	(FPT_TDC)
	Internal TOE TSF data replication consistency	(FPT_TRC)
	TSF self test	(FPT_TST)
Class FRU: Resource utilization	Fault tolerance	(FRU_FLT)
	Priority of service	(FRU_PRS)
	Resource allocation	(FRU_RSA)
Class FTA: TOE access	Limitation on scope of selectable attributes	(FTA_LSA)
	Limitation on multiple concurrent sessions	(FTA_MCS)
	Session locking	(FTA_SSL)
	TOE access banners	(FTA_TAB)

Family	Class	Designator
Class APE: Protection Profile evaluation	TOE description	(APE_DES)
	Security environment	(APE_ENV)
	Security objectives	(APE_OBJ)
	IT security requirements	(APE_REQ)
	Explicitly stated IT security requirements	(APE_SRE)
Class ASE: Security Target evaluation	TOE description	(ASE_DES)
	Security environment	(ASE_ENV)
	ST introduction	(ASE_INT)
	Security objectives	(ASE_OBJ)
	PP claims	(ASE_PPC)
	IT security requirements	(ASE_REQ)
	Explicitly stated IT security requirements	(ASE_SRE)
	TOE summary specification	(ASE_TSS)
Class ACM: Configuration management	CM automation	(ACM_AUT)
	CM capabilities	(ACM_CAP)
	CM scope	(ACM_SCP)
Class ADO: Delivery and operation	Delivery	(ADO_DEL)
	Installation, generation and start-up	(ADO_IGS)
Class ADV: Development	Functional specification	(ADV_FSP)
	High-level design	(ADV_HLD)
	Implementation representation	(ADV_IMP)
	TSF internals	(ADV_INT)
	Low-level design	(ADV_LLD)
	Representation correspondence	(ADV_RCR)
	Security policy modeling	(ADV_SPM)

Class AGD: Guidance documents	Administrator guidance	(AGD_ADM)
	User guidance	(AGD_USR)
Class ALC: Life cycle support	Development security	(ALC_DVS)
	Flaw remediation	(ALC_FLR)
	Life cycle definition	(ALC_LCD)
	Tools and techniques	(ALC_TAT)
Class ATE: Tests	Coverage	(ATE_COV)
	Depth	(ATE_DPT)
	Functional tests	(ATE_FUN)
	Independent testing	(ATE_IND)
Class AVA: Vulnerability Assessment	Covert channel analysis	(AVA_CCA)
	Misuse	(AVA_MSU)
	Strength of TOE security functions	(AVA_SOF)
	Vulnerability analysis	(AVA_VLA)
Class AMA: Maintenance of Assurance	Assurance maintenance plan	(AMA_AMP)
	TOE component categorization report	(AMA_CAT)
	Evidence of assurance maintenance	(AMA_EVD)
	Security impact analysis	(AMA_SIA)

Table F-1 NIST SP 800-18 Cross-referenced with ISO 15408

NIST 800 18 Para.	NIST 800 18 Title	Family	Class/Family Description
2	System Analysis	APE_DES	TOE Description
2.1	System Boundaries	APE_ENV	Security Environment
		ADV_FSP	Functional Specification
		ADV_HLD	High Level Design
2.2	Multiple Similar Systems		
2.3	System Category	ADV_FSP	Functional Specification
2.3.1	Major Applications	ADV_FSP	Functional Specification
2.3.2	General Support System	ADV_FSP	Functional Specification
3	Plan Development – All Systems	ADV_FSP	Functional Specification
		ADV_HLD	High Level Design
3.1	Plan Control	ADV_INT	TSF Internals
		ADV_LLD	Low Level Design
3.2	System Identification	ADV_HLD	High Level Design
3.2.1	System Name/Title	ADV_HLD	High Level Design
3.2.2	Responsible Organization	ADV_HLD	High Level Design
3.2.3	Information Contact(s)	ADV_HLD	High Level Design
3.2.4	Assignment of Security Responsibility	ASE_REQ	IT Security Requirements
3.3	System Operational Status	ADO	Delivery and Operation
3.4	General Description/Purpose	ADV_FSP	Functional Specification
3.5	System Environment	ADV_HLD	High Level Design
		APE_ENV	Security Environment
3.6	System Interconnection/Information Sharing	FCS_CKM	Cryptographic Support (where applicable)
		FDP_ACF	Access Control Functions
		FDP_ETC	Export to Outside TSF Control
		FDP_ITC	Import from Outside TSF Control
		FDP_UCT	Inter-TSF User Data Confidentiality Transfer Protection
		FDP_UIT	Inter-TSF User Data Integrity Transfer Protection
		FPT_ITA	Availability of Exported TSF Data
		FPT_ITC	Confidentiality of Exported TSF Data
		FPT_ITI	Integrity of Exported TSF Data
3.7	Sensitivity of Information Handled	FTA	TOE Access
3.7.1	Laws, Regulations, and Policies Affecting the System		No Specific Reference
3.7.2	General Description of Sensitivity	FDP	User Data Protection
		FIA_SOS	Specification of Secrets
4	Management Controls		
4.1	Risk Assessment and Management	ADV_HLD	High Level Design
		ADV_LLD	Low Level Design
		FDP_ACC	Access Control policy
		FMT_MOF	Management of Functions in TSF
		FMT_MSA	Management of Security Attributes
		FMT_SMR	Security Management Roles
		FDP_IFC	Information Flow Control Policy

NIST 800 18 Para.	Title	Family	Class/Family Description
4.2	Review of Security Controls	FDP_ACC	Access Control Policy
		FDP_ACF	Access Control Functions
		FIA_UAU	User Authentication
		FIA_UID	User Identification
		FIA_USB	User Subject Binding
		FMT_REV	Revocation
		FPR_UNO	Unobservability
		FPT_STM	Time Stamps
4.3	Rules of Behavior	FMT_SMR	Security Management Roles
4.4	Planning for Security in the Life Cycle		
4.4.1	Initiation Phase	ADV_FSP	Functional Specification
		ADV_HLD	High Level Design
4.4.2	Development/Acquisition Phase		
		ADV	Development
		ACM	Configuration Management
4.4.3	Implementation Phase	ADO	Delivery and Operation
4.4.4	Operation/Maintenance Phase	FRU	Resource Utilization
4.4.5	Disposal Phase		No Specific Reference
4.5	Authorize Processing	FTA	TOE Access
5	Operational Controls		
5.MA.	Major Application – Operational Controls		
5.MA.1	Personnel Security	FMT	Security Management
5.MA.2	Physical and Environmental Protection	FMT	Security Management
5.MA.2.1	Explanation of Physical/Environment Security	FMT	Security Management
5.MA.2.2	Computer Room Example	FMT	Security Management
5.MA.3	Production, Input/Output Controls	FCO	Communication
		FCS	Cryptographic Support
		FDP	User Data Protection
5.MA.4	Contingency Planning	FMT	Security Management
5.MA.5	Application Software Maintenance Controls	FCO	Communication
		FDP	User Data Protection
5.MA.6	Data Integrity/Validation Controls	FDP	User Data Protection
		FIA	Identification and Authentication
5.MA.7	Documentation	FMT	Security Management
5.MA.8	Security Awareness and Training	FMT	Security Management
6.MA	Major Application - Technical Controls	FAU	
6.MA.1.1	Identification	FIA	Identification and Authentication
6.MA.1.2	Authentication	FIA	Identification and Authentication
6.MA.2	Logical Access Controls	FCO	Communication
	(Authorization/Access Controls)	FDP	User Data Protection
		FIA	Identification and Authentication
6.MA.3	Public Access Controls	FDP	User Data Protection
		FIA	Identification and Authentication
6.MA.4	Audit Trails	FAU	

APPENDIX G
SUMMARY - SECURITY TEST CONTROLS

System/Information Integrity Risk Assessment

STC-I-MC-01	Confirm the existence of Data Item Definitions (DID)s by receiving them in the Office of Information Security (OIS) for review.
STC-I-MC-02	Confirm the existence of Data Flow Diagrams (DFD)s by receiving them in the Office of Information Security (OIS) for review.
STC-I-MC-03	Confirm the existence of the Software Requirements Specifications (SRS) document by receiving it in the Office of Information Security (OIS) for review.
STC-I-MC-04	Confirm the existence of a Description of External Interfaces by receiving it in the Office of Information Security (OIS) for review.
STC-I-MC-05	Confirm the existence of a High Level Design by receiving it in the Office of Information Security (OIS) for review.
STC-I-MC-06	Confirm the existence of the System Administrators Guide (SAG) by receiving it in the Office of Information Security (OIS) for review.
STC-I-MC-07	Confirm the existence of the Security Features User Guide (SFUG) by receiving it in the Office of Information Security (OIS) for review.

Data Confidentiality Risk Assessment

STC-I-MC-08	Confirm the existence of a Configuration Management Plan by receiving it in the Office of Information Security (OIS) for review.
STC-I-MC-09	Confirm the existence of Delivery Procedures by receiving them in the Office of Information Security (OIS) for review.
STC-I-MC-10	Confirm the existence of Installation and Start-up Procedures by receiving them in the Office of Information Security (OIS) for review.
STC-I-MC-11	Confirm the existence of Procedures for labeling and storing media by receiving them in the Office of Information Security (OIS) for review.
STC-I-MC-12	Confirm the existence of Procedures for disposal of damaged Media by receiving them in the Office of Information Security (OIS) for review.

System Availability Risk Assessment

STC-I-MC-13 Confirm that the system allows expedient and consistent access for all operator types.

1. Access the system from a workstation
2. Confirm that the system allows access
3. Record the lapse of time to complete the logon process

Repeat the above steps for each of the following operator types:

1. Personnel Assistant
2. Personnel Manager (SBU)
3. Personnel Management Specialist (PMS)
4. Personnel Management Specialist (SBU)
5. Personnel Officer
6. Super TimeKeeper
7. Super User (HQ)
8. Super User (Field)
9. TimeKeeper

System/Information Integrity Risk Assessment

STC-I-MC-14 Validate Data Item Definitions (DID)s by reviewing them in the Office of Information Security (OIS).

STC-I-MC-15 Validate Data Flow Diagrams (DFD)s by reviewing them in the Office of Information Security (OIS).

STC-I-MC-16 Validate the Software Requirements Specifications (SRS) document by reviewing it in the Office of Information Security (OIS).

STC-I-MC-17 Validate the Description of External Interfaces by reviewing it in the Office of Information Security (OIS).

STC-I-MC-18 Validate the High Level Design by reviewing it in the Office of Information Security (OIS).

STC-I-MC-19 Validate the System Administrators Guide (SAG) by reviewing it in the Office of Information Security (OIS).

STC-I-MC-20 Validate the Security Features User Guide (SFUG) by reviewing it

in the Office of Information Security (OIS). Confirm that security test criteria by are addressed by the SFUG.

1. Contains warnings about user-accessible functions and privileges that should be controlled in a secure operating environment
2. Clearly presents user responsibilities for secure operation
3. Does not provide conflicting information, i.e., implies different outcomes when the same input is supplied
4. Does not provide misleading or incomplete information

Data Confidentiality Risk Assessment

STC-I-MC-21 Validate the Configuration Management Plan by receiving it in the Office of Information Security (OIS) for review.

STC-I-MC-22 Confirm that measures are in place such that only authorized Changes are made to configuration items.

STC-I-MC-23 Validate Delivery Procedures by reviewing them in the Office of Information Security (OIS).

STC-I-MC-24 Validate Installation and Start-up Procedures by reviewing them in the Office of Information Security (OIS).

STC-I-MC-25 Validate Procedures for labeling and storing media by reviewing them in the Office of Information Security (OIS).

STC-I-MC-26 Validate Procedures for disposal of damaged Media by reviewing them in the Office of Information Security (OIS) .

STC-I-MC-27 Confirm that a policy is in place so that visiting maintenance/service personnel are subject to the following:

1. Required to sign-in upon arrival
2. Placed under constant supervision while on premises
3. Prohibited from running remote diagnostics
4. Required to complete a descriptive log of activities conducted on the premises
5. Required to sign-out upon departure using the same location where the sign-in was accomplished
6. Are subject to inspection upon departure

System Availability Risk Assessment

STC-I-MC-28 Confirm Personnel Assistant (PA) operator class accesses as follows:

HR and Base Benefits - Access to employee level data
Payroll - No Access
Time and Labor - No Access

STC-I-MC-29 Confirm that the Personnel Assistant (PA) operator class can access employee level data and is able to perform the following:

1. Add
2. Update Display
3. Update Display All
4. Correction

STC-I-MC-30 Confirm Personnel Manager (SBU) operator class accesses as follows:

1. HR and Base Benefits - Access to employee level data
2. Payroll - No Access
3. Time and Labor - No Access

STC-I-MC-31 Confirm that the Personnel Manager (SBU) operator class can access employee level data and is able to perform the following:

6. Reports and Query
7. Add
8. Update Display
9. Update Display All
10. Correction

STC-I-MC-32 Confirm Personnel Management Specialist (PMS) operator class accesses as follows:

1. HR and Base Benefits - Access to employee level data
2. Payroll - No Access
3. Time and Labor - No Access

STC-I-MC-33	Confirm that the Personnel Management Specialist (PMS) operator class can access employee level data and is able to perform the following: 1. Add 2. Update Display 3. Update Display All
STC-I-MC-34	Confirm Personnel Management Specialist (SBU) operator class accesses as follows: HR and Base Benefits - Access to employee level data Payroll - No Access Time and Labor - No Access
STC-I-MC-35	Confirm that the Personnel Management Specialist (SBU) operator class can access employee level data and is able to perform the following: 1. Add 2. Update Display 3. Update Display All
STC-I-MC-36	Confirm Personnel Officer (PO) operator class accesses as follows: 1. HR and Base Benefits - Access to employee level data for location 2. Payroll - No Access 3. Time and Labor - No Access
STC-I-MC-37	Confirm that the Personnel Manager (SBU) operator class can access employee level data and is able to perform the following: 1. Reports and Query 2. Add 3. Update Display 4. Update Display All 5. Correction

STC-I-MC-38 Confirm Super TimeKeeper operator class accesses as follows:

1. HR and Base Benefits - No Access
2. Payroll - No Access
3. Time and Labor - Access to employee level data for input and correction at the field site only

STC-I-MC-39 Confirm that the Super TimeKeeper operator class can access employee level data and is able to perform the following:

1. Input only

STC-I-MC-40 Confirm Super User (HQ) operator class accesses as follows:

1. HR/Base Benefits - Access to employee level data for entire Mint
2. Payroll - Access to employee level data for entire Mint
3. Time and Labor - Access to employee level data for entire Mint

STC-I-MC-41 Confirm that the Super User (HQ)operator class can access employee level data and is able to perform the following:

1. Reports and Query
2. Add
3. Update Display
4. Update Display All
5. Correction
6. View only for tables

STC-I-MC-42 Confirm Super User (Field) operator class accesses as follows:

1. HR/Base Benefits - Access to employee level data for Location
2. Payroll - Access to employee level data for entire Location
3. Time and Labor - Access to employee level data for Location

STC-I-MC-43 Confirm that the Super User (HQ)operator class can access employee level data and is able to perform the following:

1. Reports and Query
2. Add
3. Update Display
4. Update Display All
5. Correction
6. View only for tables

STC-I-MC-44 Confirm TimeKeeper operator class accesses as follows:

1. HR and Base Benefits - No Access
2. Payroll - No Access
3. Time and Labor - Access to employee level data for input

STC-I-MC-45 Confirm that the TimeKeeper operator class can access employee level data and is able to perform the following:

1. Input only

System/Information Integrity Risk Assessment

STC-I-MC-46 Review the System Administrator's Guide (SAG) to confirm that mechanisms are in place to ensure the following events will trigger an audit record:

1. User login, both successful and failed
2. Attempts to access objects denied by lack of privileges/rights
3. Successful access to security-critical items
4. Changes to user's privileges/profiles
5. Changes to system security configuration
6. Modification to system-supplied software
7. Creation/deletion of objects

STC-I-MC-47 Confirm that mechanisms are in place to ensure each audit record will contain at least the following:

1. Date and time of the event
2. Type of event
3. Subject identity,
4. The outcome (success or failure) of the event
5. The functional components included

Data Confidentiality Risk Assessment

STC-I-MC-48 Confirm that the PayMint system is able to protect the stored audit records from unauthorized deletion and be able to prevent and/or detect modifications to the audit records.

STC-I-MC-49 Confirm that the PayMint system is able to overwrite the oldest stored audit records in the event that storage space is exhausted.

System Availability Risk Assessment

STC-I-MC-50 Confirm that only authorized individuals can access audit Records

STC-I-MC-51 Confirm that the system is capable of maintaining profiles of system usage, where an individual user profile represents the historical patterns of usage by individual members

STC-I-MC-52 Confirm that the system is capable of maintaining a suspicion rating associated with each user whose activity is recorded in a profile, where the suspicion rating represents the degree to which the user's current activity is found inconsistent with the established patterns of usage represented in the profile.

STC-I-MC-53 Confirm that the system is capable of indicating an imminent violation of The PayMint system when a user's suspicion rating exceeds defined threshold conditions

System/Information Integrity Risk Assessment

STC-I-MC-54 Ensure that all personnel accessing PayMint have been advised On the availability of The Security Awareness training package and how to access it.

STC-I-MC-55 Ensure that all personnel accessing PayMint have been issued written copies of the rules of behavior and have submitted signature pages.

STC-I-MC-56 Ensure that all personnel accessing PayMint will be notified as revisions to the rules of behavior or policy documents containing the rules of behavior occur.

2.4.2 Data Confidentiality Risk Assessment

STC-I-MC-57 Identify all job functions where dial-in access may be allowed, and All users assigned to those job functions. Verify the methodology by which call logs are to be maintained.

STC-I-MC-58 Confirm that users have been notified that non-compliance of rules will be enforced through sanctions commensurate with the level of infraction.

STC-I-MC-59 Confirm that users have been notified that the Office of Information Security (OIS) is responsible for ensuring an adequate level of protection by means of technical, administrative, and managerial controls; policies and procedures; awareness sessions; inspections and spot checks; periodic vulnerability analyses.

STC-I-MC-60 Confirm that users have been notified that the rules are not to be used in place of existing policy, rather they are intended to enhance and further define the specific rules each user must follow while accessing PayMint.

STC-I-MC-61 Confirm that users have been notified about the rules governing Work-at-Home Arrangements

STC-I-MC-62 Confirm that users have been notified about the rules governing Dial-in Access

STC-I-MC-63 Confirm that users have been notified about the rules governing Connection to the Internet

STC-I-MC-64 Confirm that users have been notified about the rules governing Protection of Software Copyright :Licenses

STC-I-MC-65 Confirm that users have been notified about the rules governing Unofficial Use of Government Equipment

System Availability Risk Assessment

STC-I-MC-66 Identify the methodology whereby each dial-in access call will use a one-time password. Confirm that passwords used in this manner cannot be repeated and/or duplicated.

STC-I-MC-67 Identify all job functions requiring access to the Internet. Confirm that where such access is allowed, all external connections are carefully documented and a copy provided to the OIS. Identify how the OIS will be notified of external connection updates

STC-I-MC-68 Confirm that all work-at-home arrangements comply with the following conditions:

1. Each arrangement is in writing
2. Identifies clearly the time period the work at home will be allowed
3. Identifies the government equipment and supplies needed by the employee at home, and how that equipment and supplies will be transferred and accounted for
4. Identifies if telecommuting will be needed and allowed.
5. Is made available for review by the Office of Information Security (OIS) prior to commencement

OPERATIONAL CONTROLS

STC-I-OC-01 Provide a listing of all positions having access to PayMint. Include the following:

1. Position title
2. Sensitivity level
3. Number of incumbents in the position
4. Number of vacancies for the position
5. Projection for growth of the position (10-year projection preferred)

STC-I-OC-02 Confirm that all personnel having PayMint access have undergone background investigations.

1. Provide an up-to-date list of all persons having PayMint access showing the date a background investigation was completed.
2. Confirm that system access is limited to only personnel who have a completed background investigation.
3. Confirm that system access is denied personnel whose background investigations are pending or incomplete.
4. Confirm that personnel background investigation information is backed up in a redundant file, that the file is up-to-date, and is stored in a safe location off-site.

STC-I-OC-03 Confirm compliance of entry and egress points with respect to the following items:

1. Entrance doors are of solid material and at least 1-3/4 inches thick
2. Hinge pins are modified to prevent removal
3. Deadbolts are installed on all doors
4. Perimeter walls are slab-to-slab and attached to floor and ceiling
5. Ground level and second story windows are positive locking devices and not equipped with spring-loaded latches
6. Availability of escorts for unauthorized personnel
7. Availability and accuracy of sign-in and sign-out logs

STC-I-OC-04 Confirm compliance of locks with respect to the following items:

1. Limitations on distribution of keys
2. Cipher lock combinations are changed at least every six months or more frequently
3. Cipher lock combinations are changed in the event of a resignation, termination, or attempted break-in
4. Cipher lock combinations use four or more numbers
5. Cipher lock mechanisms are shielded from view

STC-I-OC-05 Confirm that emergency backup power is available for:

1. Servers
2. Administrative workstations
3. Emergency evacuation lighting
4. Intrusion detection devices
5. Fire alarms

User Support and Access Controls - Electronic Information

Ensure that unauthorized individuals cannot read, copy, alter, or steal printed or electronic information.

STC-I-OC-06 Verify the following and report the findings. The system is able to:

1. Enforce access control on all system resources
2. Explicitly authorize access to resources based on attributes
3. Explicitly deny access to resources based on attributes
4. Export data without the user/sender's associated security attributes
5. Control information flow by selecting the most stringent security attribute where multiple security attributes exist in a given object.
6. Provide residual information protection, i.e., ensure that previous information content of a resource is made unavailable upon the completion of each transaction
7. Maintain stored data integrity
8. Maintain data exchange confidentiality
9. Detect and log authentication failures
10. Maintain security attribute definitions
11. Successfully identify and authenticate legitimate users/groups

User Support and Access Controls - Printed Information and Media

STC-I-OC-07 Verify the following and report the findings. Describe and verify the procedures in place to deal with:

1. Labeling, marking, transporting, and storing Sensitive But Unclassified (SBU) materials both within XYZ Corporation property and aboard public conveyances
2. Report and disposition security violations or the perception of security violations
3. Declassification reviews
4. Identifying and authenticating credentials such as badges and shields
5. Courier activities
6. Periodic changes of combinations
7. Defense Investigative Service DD Form 254 compliance
8. Properly classifying written materials and media to the most stringent applicable classification

Input/Output Audit Trails

STC-I-OC-08 Verify the following and report the findings:

1. Auditable events can be associated with individual user identities
2. The system can generate a record of start-up and shut-down of auditable functions
3. The system can maintain a profile of system usage
4. The system can maintain a suspicion rating associated with each user whose activity is recorded in a profile
5. The system can warn of an imminent violation when a user's suspicion rating exceeds a discretionary threshold
6. The system is able to provide audit records to authorized users
7. The system provides the capability to perform selective queries, searches, and ordering of audit data
8. The system can protect stored audit records from unauthorized access, modification, and deletion
9. The system can issue appropriate notifications when audit records approach a set threshold

STC-I-OC-09 Verify that each audit record contains, as a minimum, the following:

1. Date and time of the event
2. Type of event
3. Subject (user/group) identity
4. Outcome (success or failure) of the event

Business Continuity and Contingency Plan (BCCP)

STC-I-OC-10 Review the BCCP for possible disagreements with compliance documents and for updates needed to address unique PayMint requirements.

Disaster Recovery Plan (DRP)

STC-I-OC-11 Review the DRP for possible disagreements with compliance documents and for updates needed to address unique PayMint requirements.

Formal Change Control Process

STC-I-OC-12 A formal change control process is in place. Review this process for possible disagreements with compliance documents and for updates needed to address unique PayMint requirements.

Illegal Use of Copyrighted Software

STC-I-OC-13 Existing U.S. Mint organizational policies prohibit the illegal use of copyrighted software and shareware. Review the procedures for possible disagreements with system design documents.

Virus Remediation Software

STC-I-OC-14 Existing U.S. Mint operating procedures and practices require the availability and use of virus remediation software on all systems.
Investigate and confirm that such software does not inhibit, interfere with, or weaken the required security functionality.

Penetration Testing

STC-I-OC-15 Arrange for separate (independent) penetration testing, which may be done as part of the system functional testing or at a time following the completion of system functional testing. Successful penetration testing will be necessary before the system can be authenticated and released to active duty.

Documentation

STC-I-OC-16 Review all Documentation for the PayMint system including descriptions of the hardware and software, policies, standards, and procedures. Identify and remediate conflicts as needed.

Security Awareness and Training

STC-I-OC-17 The U.S. Mint requires all employees to take the Mint's Security Awareness training at least once a year. The Mint's Intranet provides an online security awareness-training package. Confirm that this is available to all personnel accessing the PayMint system.

Confirm that all personnel accessing PayMint are aware of or have completed and have acknowledged completion of this package.

The Security Awareness training package can be found on the XYZ Corporation Intranet at http://xyz corporation/corporate/training/security/default.shtm

TECHNICAL CONTROLS

STC-I-TC-01 Ensure that all personnel accessing PayMint have completed The Security Awareness training package and acknowledge and understanding of password requirements.

STC-I-TC-02 Validate Secure Logon from the Workstation, Confirm Identification/Authentication is

1. Accepted using known valid User ID and VALID password
2. Declined using known valid User ID and INVALID password
3. Declined using known INVALID User ID and VALID password
4. Declined using known INVALID User ID and INVALID password

STC-I-TC-03 Confirm that within PayMint, originators and recipient cannot deny sending or receiving information.

Operator Class Permissions

The PayMint system has very specific role-based operator permissions.

STC-I-TC-04 Validate Operator Class User permissions

For each operator class select a known valid user.
Access a record for each category and confirm the following:

1. Record can be accessed with DISPLAY ONLY Access operation where permission is granted
2. Record cannot be accessed with DISPLAY ONLY Access operation where permission is denied

3. Record can allow an ADD operation where permission is granted
4. Record cannot allow an ADD operation where permission is denied

5. Record can allow an UPDATE/DISPLAY operation where permission is granted
6. Record cannot allow an UPDATE/DISPLAY operation where permission is denied

7. Record can allow an UPDATE/DISPLAY ALL operation where permission is granted
8. Record cannot allow an UPDATE/DISPLAY ALL operation where permission is denied

9. Record can allow a CORRECTION operation where permission is granted
10. Record cannot allow a CORRECTION operation where permission is denied

The PayMint system is not designed or intended for public access.

STC-I-TC-05 Ensure that public access via the Internet is impossible

Audit Data Generation with Identity

STC-I-TC-06	Confirm that the following events will trigger an audit record: 1. User login, both successful and failed 2. Attempts to access objects denied by lack of rights 3. Successful access to security-critical items 4. Changes to user's profiles 5. Changes to system security configuration 6. Modification to system-supplied software 7. Creation/deletion of objects
STC-I-TC-07	Confirm that mechanisms are in place to ensure each audit record will contain at least the following: 1. Date and time of the event 2. Type of event 3. Subject identity, 4. The outcome (success or failure) of the event 5. The functional components included
STC-I-TC-08	Confirm the identity of all users
STC-I-TC-09	Identify the user's authority (permissions) to interact with the system
STC-I-TC-10	Confirm the correctness of security attributes associated with each authorized user
STC-I-TC-11	Confirm that the system is capable of the following: 1. The capability to allow reading information from the audit records. 2. No other users except those that have been specifically identified can read the information. 3. The availability of audit review tools to select the audit data to be reviewed based on criteria (i.e., queries, sorts, etc.)

SANS GIAC Security Essentials
Practical Assignment
Submitted By: Robert L Krise

QUESTIONS

MULTIPLE CHOICE

(1) Three essential security requirements for any given information system include:

A. Confidentiality, integration, availability
B. Confidentiality, integrity, auditability
C. Confidentiality, integrity, availability
D. Confidentiality, integrity, access controls
E. Congeniality, integrity, availability

(2) With respect to the ISO 15408 Common Criteria, the seven governmental organizations known as "the Common Criteria Project Sponsoring Organizations" have representatives from the following:

A. Canada, China, France, Germany, United Kingdom, United States
B. Canada, France, Germany, Netherlands, United Kingdom, United States
C. Canada, France, Germany, United Kingdom, Union of Soviet Socialist Republics, United States
D. Canada, France, Germany, Norway, United Kingdom, United States

(3) Auditing IT records is required by:

A. AICPA, FASB, IEEE, NIST
B. AICPA, NIST, A-130, ISO156408
C. AICPA, CobiT, NIST
D. A-130, NIST, ISO15408
E. NIST, CobiT
F. A-130, NIST
G. NIST, ISO15408

(4) As a minimum, emergency backup power should be available to the following entities in the event of an outage:

A. Servers, administrative workstations, stairwell lighting, intrusion detection devices, fire alarms.
B. Servers, administrative workstations, emergency evacuation lighting, intrusion detection devices, fire alarms.
C. Servers, super-user workstations, emergency evacuation lighting, intrusion detection devices, fire alarms.
D. Servers, administrative workstations, emergency evacuation lighting, intrusion detection devices, fire water supply pumps.

(5) An "individual user profile" is comprised of:

A. Username, workstation label, workstation location, privileges/limitations.
B. The historical patterns of password changes.
C. The historical patterns of usage.
D. The historical patterns of website access

(6) The IT Governance Institute was formed by:

A. The Office of Management and Budget (OMB)
B. NIST in collaboration with the National Security Agency
C. The AICPA in collaboration with CobiT
D. The Information System Audit and Control Association (ISACA)

TRUE/FALSE

(7) According to most policies, the username should be changed at least every 40 days.

(8) OMB Circular A-130 recommends compliance with NIST standards.

(9) Every facility equipped with or utilizing an IS must adhere to OMB Circular A-130.

(10) Successful user logins should trigger an audit record.

(11) Physical security is an important part of the IS security picture.

(12) Work-at-home arrangements offer much latitude regarding the time spent on tasks.

(13) The ISO15408 Common Criteria is an international standard. It is not related to any requirements set forth by the United States government.

(14) A Disaster Recovery Plan may be recommended, but is not really required for a domestic information system.

(15) According to NIST SP 800-18, cipher locks used for server room access must have their combinations changed at least every 40 days.

(16) A Security Plan is required by the Paperwork Reduction Act (44 U.S.C. Chapter 35).

(17) The Information Owner is not responsible for establishing the rules for appropriate use and protection of the subject data/information (rules of behavior) when the data/information are shared with other organizations.

(18) A Memorandum of Agreement is a signed document designating which personnel are assigned Operator Class permissions for a given system.

(19) Successful penetration testing will be necessary before the system can be authenticated and released to active duty.

(20) OMB Circular A-130 requires the preparation of a formal risk analysis.

ANSWER KEY

MULTIPLE CHOICE

(1) Three essential security requirements for any given information system include:

A. Confidentiality, integration, availability
B. Confidentiality, integrity, auditability
C. Confidentiality, integrity, availability
D. Confidentiality, integrity, access controls
E. Congeniality, integrity, availability

The three essential security requirements are confidentiality, integrity, availability, answer G. Integration is not an essential security requirement, therefore answer A is incorrect. Auditability and access controls are procedural mechanisms and not basic high-level requirements, thus answers B and D are incorrect. Congeniality is not an essential security requirement, therefore answer E is incorrect.

(2) With respect to the ISO 15408 Common Criteria, the seven governmental organizations known as "the Common Criteria Project Sponsoring Organizations" have representatives from the following:

A. Canada, China, France, Germany, United Kingdom, United States
B. Canada, France, Germany, Netherlands, United Kingdom, United States
C. Canada, France, Germany, United Kingdom, Union of Soviet Socialist Republics, United States
D. Canada, France, Germany, Norway, United Kingdom, United States

The correct answer is B. Six countries are represented. There are seven entities because two different United States organizations are represented, namely NIST and the National Security Agency (NSA). China and Norway are not members of the CC Project Sponsoring Organization, thus answers A and D are incorrect. (Note that Norway HQ Defense Command/Security Division is a participant in the May 2000 International Arrangement on the Recognition of Common Criteria Certificates). The Union of Soviet Socialist Republics no longer exists as an entity and none of the former republics are members, thus answer C is incorrect.

ANSWER KEY (Continued)

(3) Auditing IT records is required by:

A. AICPA, FASB, IEEE, NIST
B. AICPA, NIST, A-130, ISO156408
C. AICPA, CobiT, NIST
D. A-130, NIST, ISO15408
E. NIST, CobiT
F. A-130, NIST
G. NIST, ISO15408

Answer F is correct. A-130 is mandated by law via Presidential Decision Directive 63 (aka PDD-63). A-130 cites NIST.

AICAP and FASB govern financial audits, not IT audits, and the IEEE governs electrical and electronics engineering standards, thus answers A,B, and C are incorrect.

CobiT and ISO15408 render excellent audit guidelines but are not mandated by law. As an international standard, ISO15408 is not enforceable in the US courts. There is currently no legislation to enact CobiT as a standard. Thus, answers D, E, and G are incorrect.

(4) As a minimum, emergency backup power should be available to the following entities in the event of an outage:

A. Servers, administrative workstations, stairwell lighting, intrusion detection devices, fire alarms.
B. Servers, administrative workstations, emergency evacuation lighting, intrusion detection devices, fire alarms.
C. Servers, super-user workstations, emergency evacuation lighting, intrusion detection devices, fire alarms.
D. Servers, administrative workstations, emergency evacuation lighting, intrusion detection devices, fire water supply pumps.

B is the correct answer. A is incorrect because stairwell lighting is only one smaller component of emergency evacuation lighting. C is incorrect because the term " super-user workstations" is ambiguous. Super-user workstations may or may not include administrative workstations, but without a formal systems design or Configuration Management document, no assumptions should ever be made. D is incorrect because computer facilities use either carbon dioxide or a "dry" chemical such as Halon or Purple K. Fire water supply pumps are usually found in remote locations, industrial facilities or aboard ships.

ANSWER KEY (Continued)

(5) An "individual user profile" is comprised of:

A. Username, workstation label, workstation location, privileges/limitations.
B. The historical patterns of password changes.
C. The historical patterns of usage.
D. The historical patterns of website access

C is correct. A is incorrect because it refers to demographic "administrivia". B and D are incorrect because "usage" encompasses much more than password changes and web site access.

An individual user profile representing the historical patterns of usage can be used to establish a suspicion rating associated with each user whose activity is recorded in a profile. When the user's current activity is found inconsistent with the established patterns of usage represented in the profile, the system can initiate an alarm. Most systems are capable of indicating an imminent violation when a user's suspicion rating exceeds defined threshold conditions.

(6) The IT Governance Institute was formed by:

A. The Office of Management and Budget (OMB)
B. NIST in collaboration with the National Security Agency
C. The AICPA in collaboration with CobiT
D. The Information System Audit and Control Association (ISACA)

Answer D is correct. A and B are incorrect since the entities named therein are government agencies and not industry associations. C is incorrect because the AICPA is a dedicated accounting standards association that predates the ISACA and CobiT is the specific standard taken over by the ISACA.

TRUE/FALSE

(7) According to most policies, the username should be changed at least every 40 days.

FALSE: The password, not the username should be changed.

(8) OMB Circular A-130 recommends compliance with NIST standards.

FALSE: A-130 requires compliance with NIST. OMB Circular A-130 states "Ensure that appropriate security controls must be specified, designed into, tested, and accepted in the application in accordance with appropriate guidance issued by NIST. "

(9) Every facility equipped with or utilizing an IS must adhere to OMB Circular A-130.

FALSE: A-130 is applicable to United States Federal Government entities only, however, it is a good IS security guideline that can be adapted global and/or private enterprise entities as well.

(10) Successful user logins should trigger an audit record.

TRUE. Reference NIST SP 800-18, Section 6.MA.4

(11) Physical security is an important part of the IS security picture.

TRUE: See NIST SP 800-18, 5.MA.2.1 Explanation of Physical and Environment Security

(12) Work-at-home arrangements offer much latitude regarding the time spent on tasks.

FALSE: Work-at-home arrangements must identify clearly the time period the work at home will be allowed

(13) The ISO 15408 Common Criteria is an international standard. It is not related to any requirements set forth by the United States government.

FALSE: Two US Government entities helped create the standard, namely NIST and the National Security Agency. Appendices to the Practical Assignment paper show a mapping correlation between NIST SP 800-18 and ISO 15408.

(14) A Disaster Recovery Plan may be recommended, but is not really required for a domestic information system.

FALSE: A Disaster Recovery Plan is required, although its specific title may be something other than "Disaster Recovery Plan". Reference: NIST SP 800-18, Section 5.MA.4 Contingency Planning

(15) According to NIST SP 800-18, cipher locks used for server room access must have their combinations changed at least every 40 days.

FALSE: Cipher lock combinations are changed at least every six months or more frequently. Reference NIST SP 800-18, 5.MA.2.1, Explanation of Physical and Environmental Security, Paragraph 1, Access Controls

(16) A Security Plan is required by the Paperwork Reduction Act (44 U.S.C. Chapter 35).

TRUE: Reference NIST SP 800-18, Section 1.5 Security Plan Responsibilities, Paragraph 3: "OMB Circular A-130 requires a summary of the security plan to be incorporated into the strategic IRM plan required by the Paperwork Reduction Act (44 U.S.C. Chapter 35)".

(17) The Information Owner is not responsible for establishing the rules for appropriate use and protection of the subject data/information (rules of behavior) when the data/information are shared with other organizations.

FALSE: Reference NIST SP 800-18, Section 1.5 Security Plan Responsibilities, Paragraph 1: "The System Owner[2] is responsible for ensuring that the security plan is prepared and for implementing the plan and monitoring its effectiveness. Security plans should reflect input from various individuals with responsibilities concerning the system, including functional "end users," Information Owners,[3] the System Administrator, and the System Security Manager".

(18) A Memorandum of Agreement is a signed document designating which personnel are assigned Operator Class permissions for a given system.

FALSE: : Reference NIST SP 800-18, Section 3.6, System Interconnection/Information Sharing: " OMB Circular A-130 requires that written management authorization (often in the form of a Memorandum of Understanding or Agreement,) be obtained prior to connecting with other systems and/or sharing sensitive data/information. The written authorization shall detail the rules of behavior and controls that must be maintained by the interconnecting systems".

(19) Successful penetration testing will be necessary before the system can be authenticated and released to active duty.

TRUE: Reference NIST SP 800-18, Appendix C, Template, General Support System Security Plan, Integrity Controls, Page 15C

(20) OMB Circular A-130 requires the preparation of a formal risk analysis.

FALSE: Reference NIST SP 800-18, Section 4.1, Risk Assessment and Management:
" OMB Circular A-130 no longer requires the preparation of a formal risk analysis. It does, however, require an assessment of risk as part of a risk-based approach to determining adequate, cost-effective security for a system".

[2] The System Owner is responsible for defining the system's operating parameters, authorized functions, and security requirements. The information owner for information stored within, processed by, or transmitted by a system may or may not be the same as the System Owner. Also, a single system may utilize information from multiple Information Owners.

[3] The Information Owner is responsible for establishing the rules for appropriate use and protection of the subject data/information (rules of behavior). The Information Owner retains that responsibility even when the data/information are shared with other organizations.