

BITS

FINANCIAL SERVICES
R O U N D T A B L E

FINANCIAL INSTITUTION SHARED ASSESSMENTS PROGRAM

AGREED UPON PROCEDURES

VERSION 2.0

ASSESSMENT GUIDE

BITS
1001 PENNSYLVANIA AVENUE, NW
SUITE 500 SOUTH
WASHINGTON, DC 20004
(202) 289-4322
www.bitsinfo.org/fisap

	<p><i>Financial Institution Shared Assessments Program</i> <i>Agreed Upon Procedures</i> Version 2.0</p>
--	---

©BITS 2006

Complete and accurate documents created under the Financial Institution Shared Assessments Program may be downloaded from the official BITS web site at www.bitsinfo.com/fisap.

While retaining copyrights in the AUP and SIG documents, the Financial Institution Shared Assessments Program makes them freely available to the public for the purpose of conducting self-assessments and third-party security assessments. Licenses for other uses are available from BITS. Individuals or organizations should review the terms of use prior to downloading, copying, using or modifying the AUP or SIG.

This notice must be included on any copy of the Financial Institution Shared Assessments Program documents.

Background

When applications, systems and services are outsourced, responsibility for reputation, transaction, regulatory and other risks associated with the outsourcing relationship remains with the financial institution. To develop an appropriate risk-mitigation strategy and to address risks associated with outsourced services, the institution must be able to identify and understand the controls upon which the service provider relies.

The Financial Institution Shared Assessments Program was created to develop a standardized approach to obtaining consistent information about a service provider's information technology practices, processes and controls. As part of the program, and consistent with ISO 17799:2005,* ten areas of information security management have been used as the foundation for two complementary tools designed to document the service provider's ability to actively manage information security controls.

Standardized Information Gathering Questionnaire (SIG): Developed by BITS members to leverage the *BITS IT Service Providers Expectations Matrix* and address the control areas covered in ISO 17799:2005, the SIG can be used to obtain required documentation and establish a profile on operations and controls for each of the control areas to obtain verifiable information for each control area. When used as a standalone document, the questionnaire provides information the financial institution needs to evaluate the security controls the service provider has in place.

Agreed Upon Procedures (AUP): Developed by BITS members with the Big 4 accounting firms acting as technical advisors, the AUPs provide objective and consistent procedures that will be performed on each of the control areas. Procedures address control objectives in security policy, organization of information security, asset management, human resources security, physical and environmental security, communications and operations management, access control, information systems acquisition, development and maintenance, information security incident management, business continuity management, and compliance. Procedure outcomes enable organizations to view results in the context of industry risk management and regulatory requirements.

When the SIG and AUP are combined, financial institutions will have both the service provider's assertions of implemented controls backed by verifiable evidence that the controls exist and will assist financial institutions in better identifying risks, complying with regulatory requirements, and reducing inconsistencies in the evaluation of information received from service providers.

How to Use this Document

This document describes the Agreed Upon Procedures (AUPs) that comprise the Financial Institution Shared Assessments Program. More information on the Standardized Information Gathering Questionnaire (SIG) may be found on the BITS website, www.bitsinfo.org/fisap.

Update Process

Technology, threats and regulations change. The Financial Institution Shared Assessments Program's revision process ensures the SIG and AUP documents continue to meet risk management and regulatory requirements.

For additional details and revision schedules, see the Financial Institution Shared Assessments Program web site at www.bitsinfo.org/fisap.

* For more information about ISO/IEC 17799, visit www.ansi.org.

Each Control Area includes:

BITS Matrix Reference: This is a reference to the original *BITS IT Service Providers Expectations Matrix* control area. The BITS Matrix Reference includes a High Level Expectation, which describes the financial industry expectations of vendors and *service providers*. The expectations are broad requirements that give context to the AUP.

ISO 17799 Matrix Reference: This is a reference to the ISO 17799:2005 control area.

Documentation that may be Requested: This is a list of documents that a practitioner may request of the *service provider* in order to perform the AUPs.

Each AUP is described as follows:

Objective: Statement regarding the controls that *service providers* should have in place to meet industry risk management and regulatory requirements.

Procedure: Actions that a practitioner will perform to address the objectives outlined under each control area, including, where necessary, practitioners' notes

Note: Italicized phrases appearing in the body of the document are defined in the Glossary.

TABLE OF CONTENTS

A. SECURITY POLICY	7
A.1 SECURITY POLICY CONTENT	7
A.2 SECURITY POLICY APPROVAL	7
A.3 SECURITY POLICY REVISIONS	8
A.4 SECURITY POLICY DATE OF LAST REVIEW	8
A.5 CONSTITUENT ACCEPTANCE OF ACCEPTABLE USE	8
B. ORGANIZATION OF INFORMATION SECURITY	9
B.1 SECURITY POLICY – CONSTITUENT ACCEPTANCE OF CONFIDENTIALITY.....	9
C. ASSET MANAGEMENT	10
C.1 ASSET ACCOUNTING AND INVENTORY	10
D. HUMAN RESOURCES SECURITY	12
D.1 Security Awareness Training Attendance List.....	12
E. PHYSICAL AND ENVIRONMENTAL SECURITY	
E.1 ENVIRONMENTAL CONTROLS – COMPUTING HARDWARE	13
E.2 PHYSICAL SECURITY CONTROLS – COMPUTING HARDWARE.....	14
F. COMMUNICATIONS AND OPERATIONS MANAGEMENT	15
F.1 NETWORK SECURITY – IDS/IPS SIGNATURE UPDATES	15
F.2 NETWORK MANAGEMENT – ENCRYPTED AUTHENTICATION CREDENTIALS	16
F.3 EXTERNALLY FACING OPEN PORTS.....	17
F.4 REMOTE ACCESS AND REMOTE ADMINISTRATION	17
F.5 NETWORK LOGGING.....	18
F.6 VIRUS PROTECTION (SERVERS)	19
F.7 VIRUS PROTECTION (WORKSTATIONS).....	19
F.8 CONTROL OF SERVER CONFIGURATION.....	20
F.9 ADMINISTRATIVE ACTIVITY LOGGING	20
F.10 LOG-ON ACTIVITY LOGGING	21
F.11 LOG RETENTION	22
F.12 APPLICATION CHANGE CONTROL.....	22
F.13 OPERATING SYSTEM CHANGE CONTROL	23
F.14 WEB SITE PRIVACY POLICY	24
F.15 WEB SITE - CLIENT ENCRYPTION	24
F.16 EMAIL RELAYING	24
F.17 PHYSICAL MEDIA TRACKING.....	25
F.18 SECURITY OF MEDIA IN TRANSIT	29
F.19 UNAPPROVED WIRELESS NETWORKS	26
F.20 WIRELESS NETWORKS ENCRYPTION	27
F.21 NETWORK SECURITY – FIREWALLS	27
F.22 NETWORK SECURITY – AUTHORIZED NETWORK TRAFFIC.....	28
F.23 NETWORK SECURITY – IDS ATTRIBUTES	29
G. ACCESS CONTROL	31
G.1 PASSWORD CONTROLS	32
G.2 REVOKE SYSTEM ACCESS.....	33
G.3 ACCESS AUTHORIZATION	33

G.4 INACTIVE ACCOUNTS 33

G.5 CONTROLS FOR UNATTENDED SYSTEMS 34

H. INFORMATION SYSTEMS ACQUISITION, DEVELOPMENT AND MAINTENANCE..... 35

H.1 PATCH LEVELS OF VULNERABLE SYSTEMS 35

H.2 ROUTER VULNERABILITIES 36

H.3 FIREWALL PATCH LEVELS..... 37

I. INFORMATION SECURITY INCIDENT MANAGEMENT..... 38

J. BUSINESS CONTINUITY MANAGEMENT 39

J.1 BUSINESS IMPACT ANALYSIS 39

J.2 THREAT ASSESSMENT 39

K. COMPLIANCE 41

K.1 PRESENCE OF LOG-ON BANNERS 41

K.2 TECHNICAL COMPLIANCE CHECKING - VULNERABILITY TESTING AND REMEDIATION 41

L. GLOSSARY OF TERMS..... 43

M. APPROVED SCANNING TOOLS..... 46

N. SAMPLING PARAMETERS 47

A. Security Policy

BITS Matrix Reference

High Level Expectation

All vendors and service providers should have a written and comprehensive set of information security policy documents, which act as the rules and guidelines for dealing with the protection of information and information assets.

ISO 17799 Matrix Reference

Information Security Policy (5.1)

Information Security Policy Document (5.1.1)

Review of Information Security Policy (5.1.2)

Documentation that may be Requested

Information security policy, privacy policy, policy revision and approval documents, policy acceptance documents, list of constituents

A.1 Security Policy Content

Objective:

Security policy contains the following attributes.

- 1) Information handling
- 2) System management
- 3) Vulnerability management
- 4) Incident response
- 5) Access control
- 6) Employee accountability
- 7) Policy maintenance

Procedure:

- a. Obtain a copy of the *security policy*.
- b. Inspect the table of contents for the presence of the following *attributes*.
 - 1) Information handling
 - 2) System management
 - 3) Vulnerability management
 - 4) Incident response
 - 5) Access control
 - 6) Employee accountability
 - 7) Policy maintenance

A.2 Security Policy Approval

Objective:

Security policy has been approved.

Procedure:

Using the *security policy* obtained in *A.1 Security Policy Content*, inspect the document for evidence of approval and note the last five approvers' names, titles, and most recent date of approval.

A.3 Security Policy Revisions

Objective:

Security policy contains revision history.

Procedure:

Using the *security policy* obtained in *A.1 Security Policy Content*, inspect the document for the presence of the following *attributes*.

- 1) Revision history
- 2) Date of last revision
- 3) Change log

A.4 Security Policy Date of Last Review

Objective:

Security policy has been reviewed within the last 12 months.

Procedure:

Using the *security policy* obtained in *A.1 Security Policy Content*, inspect for the most recent “date of review” *attribute*.

A.5 Constituent Acceptance of Acceptable Use

Objective:

Constituents sign a copy of the company acceptable use policy every 12 months. Signed policy is maintained in the employee personnel file or other compliance tracking tool.

Procedure:

- a. Obtain a *constituent* list during the time period being tested and document the date of the list.
- b. Using the sampling parameters in Section N, select a sample of *constituents*.
- c. Request the existing acceptance document(s) (electronic or paper) for each selected *constituent* and report where no documents exist.
- d. Inspect the date of signature for each corresponding acceptance for a date within the last 12 months from the date of testing.

B. Organization of Information Security

BITS Matrix Reference

N/A

ISO 17799 Matrix Reference

Confidentiality Agreements (6.1.5)

Documentation that may be Requested

N/A

B.1 Security Policy – Constituent Acceptance of Confidentiality

Objective:

Constituents have acknowledged their obligation to maintain *confidentiality*.

Procedure:

- a.** Using the *constituent* list obtained in *A.5 Constituent Acceptance of Acceptable Use*, select a sample of *constituents* using the sampling procedures in Section N.
- b.** For the selected *constituents*, request the existing electronic or paper confirmation of acceptance of their individual responsibility for the protection of information and information assets and report where no confirmation exists.
- c.** Document the name of the acceptance confirmation and date of the most recent acknowledgement of each *constituent* sampled.

C. Asset Management

BITS Matrix Reference

High Level Expectation

Service providers should have in place an appropriate asset control policy structure, including appropriate ownership, management, licensing and other controls that address the following asset types: information assets, hardware and software assets, physical assets, and services.

ISO 17799 Matrix Reference

Inventory of Assets (7.1.1)

Information Classification (7.2)

Classification Guidelines (7.2.1)

Information Labeling and Handling (7.2.2)

Documentation that may be Requested

Asset control policy, hardware and software inventory reports

C.1 Asset Accounting and Inventory

Objective 1 (Hardware):

Hardware *inventory* reports include the following *attributes*.

- 1) *Asset control tag*
- 2) Serial number
- 3) Host name
- 4) Physical location (e.g., room, building, city, state)
- 5) *IP* address
- 6) System owner
- 7) System steward
- 8) System class (e.g., mainframe, mid-range, server, workstation)
- 9) Operating system
- 10) Environment (e.g., development, test, production)
- 11) Business functions supported

Objective 2 (Software):

Software *inventory* reports include the following *attributes*.

- 1) *Asset control tag*
- 2) Host name
- 3) Environment (e.g., development, test, production)
- 4) Business functions supported
- 5) Software version

Procedure:

- a. Obtain a hardware and software *inventory* report for all *target systems* and record the date of the report.
- b. Using the sampling parameters in Section N, select a sample from the *inventory* of *target systems* report.
- c. Inspect the hardware *inventory* reports for each sample item for the presence of the following *attributes*.
 - 1) *Asset control tag*
 - 2) Serial number

- 3) Host name
 - 4) Physical location (e.g., room, building, city, state)
 - 5) *IP* address
 - 6) System owner
 - 7) System steward
 - 8) System class (e.g., mainframe, mid-range, server, workstation)
 - 9) Operating system
 - 10) Environment (e.g., development, test, production)
 - 11) Business functions supported
- d.** Inspect the software *inventory* reports for each sample item for the presence of the following *attributes*.
- 1) *Asset control tag*
 - 2) Host name
 - 3) Environment (e.g., development, test, production)
 - 4) Business functions supported
 - 5) Software version

D. Human Resources Security

BITS Matrix Reference

High Level Expectation

Service providers should have and adhere to policies and procedures that require them to perform background checks on those individuals who will be administering systems or who will have access to receiver company information. These policies and procedures should ensure that personnel responsible for design, development, implementation, and operation are qualified to fulfill their responsibilities.

All employees of the service provider's organization, and where relevant, third-party users, should be made aware of information security threats and concerns, and should be equipped to support the organizational security policy in the course of their normal work. Users should be trained in information-security procedures and the correct use of information-processing facilities to minimize possible security threats.

Incidents affecting security should be reported through appropriate management channels as quickly as possible. All employees and contractors should be made aware of the procedures for reporting different types of incidents (security breach, threats, vulnerabilities, or security-related software malfunction) that might have an impact on the receiver company's operations. All employees and contractors should be required to report any observed or suspected threats, vulnerabilities, or incidents as quickly as possible to the designated point of contact.

ISO 17799 Matrix References

Information Security Awareness, Education, and Training (8.2.2)

Documentation that may be Requested

Employment policy, non-disclosure agreements, background check documents for staff supporting very sensitive services or data, copy of insurance declaration pages, security awareness training attendee or evidence of completion records

D.1 Security Awareness Training Attendance List

Objective:

Security awareness training attendance reports are maintained in the *constituent's* personnel file or other compliance tracking tool.

Procedure:

- a. Using the *constituent* list obtained in *A.5 Constituent Acceptance of Acceptable Use*, select a sample of *constituents* using the sampling procedures in Section N.
- b. Obtain an attendance document (electronic or paper) for the selected *constituents* and inspect each document for evidence of attendance at the company's security awareness training and document results.

E. Physical and Environmental Security

BITS Matrix Reference

High Level Expectation

Business information processing, storage or distribution facilities should be housed in secure areas, protected by a defined security perimeter, with appropriate security barriers and entry controls. Facilities should be physically protected from unauthorized access, damage and interference. Access should be logged and the logs should be securely maintained.

Equipment should be physically protected from security threats and environmental hazards in order to prevent loss, damage or compromise of assets and interruption to business activities.

Information and information-processing facilities should be protected from disclosure to, modification of, or theft by unauthorized persons. Controls should be in place to minimize loss or damage.

ISO 17799 Matrix Reference

Secure Areas (9.1)

Physical Security Perimeter (9.1.1)

Physical Entry Controls (9.1.2)

Protection against External and Environmental Threats (9.1.4)

Equipment Security (9.2)

Equipment Siting and Protection (9.2.1)

Documentation that may be Requested

Floor plan, badge control policy, physical access logging policy, copy of insurance declaration pages

E.1 **Environmental Controls – Computing Hardware**

Objective:

Hardware is protected with environmental controls.

Procedure:

- a. Using the sampling parameters in Section N, select a sample of hardware systems from the report of the inventory of *target systems* obtained in *C.1 Asset Accounting and Inventory*.
- b. Obtain from the *service provider* the location of each *target system* selected in reference to these defined areas: *secure* and *general perimeter*.
- c. At the location of each *target system* as identified in step b, observe whether the following items exist.

Secure Perimeter:

- 1) Climate control system
- 2) Thermostat
- 3) Raised floor
- 4) Smoke detector
- 5) Heat detector
- 6) *Vibration alarm sensor* (seismic)
- 7) Fluid or water sensor
- 8) Fire suppression system

General Perimeter:

- 1) Climate control system
- 2) Thermostat
- 3) Raised floor
- 4) Smoke detector
- 5) Heat detector
- 6) *Vibration alarm sensor* (seismic)
- 7) Fluid or water sensor
- 8) Fire suppression system

E.2 Physical Security Controls – Computing Hardware**Objective:**

Hardware is protected with physical security controls.

Procedure:

- a. Using the sampling parameters in Section N, select a sample of hardware systems from the report of the inventory of *target systems* obtained in *C.1 Asset Accounting and Inventory*.
- b. For each sample item selected, observe the *immediate*, *secure*, and *general perimeters* for the existence of following controls.

Immediate Perimeter:

- 1) Mounted camera at points of entry
- 2) Locked cabinets
- 3) Badge/biometric readers or locked doors requiring a key or *PIN* on all points of entry

Secure Perimeter:

- 1) Motion sensor
- 2) Mounted camera at points of entry
- 3) *Anti-tailgating/piggybacking* mechanisms at points of entry
- 4) Walls extend from *true floor* to *true ceiling*
- 5) Security guards at each unlocked point of entry
- 6) Badge/biometric readers or locked doors requiring a key or *PIN* on all points of entry.

General Perimeter:

- 1) Mounted camera at points of entry
- 2) *Anti-tailgating/piggybacking* mechanisms at points of entry
- 3) Security guards at each unlocked point of entry
- 4) Badge/biometric readers or locked doors requiring a key or *PIN* on all points of entry

F. Communications and Operations Management

BITS Matrix Reference

High Level Expectation

Responsibilities and procedures for the management and operation of all information-processing facilities should be established and adhered to. This includes the development of operating instructions, and change control and incident-response procedures. Segregation of duties and environments—development, testing, staging, and production—should be implemented to reduce the risk of negligent, inadvertent or deliberate misuse of information-processing facilities, and systems.

Controls should be in place to prevent and detect the introduction and dissemination of malicious software. Recovery plans should be prepared, updated and tested regularly.

ISO 17799 Matrix Reference

Change Management (10.1.2)
System Acceptance (10.3.2)
Protection against Malicious and Mobile Code (10.4)
Controls against Malicious Code (10.4.1)
Backup (10.5)
Information Backup (10.5.1)
Network Security Management (10.6)
Security of Network Services (10.6.2)
Media Handling (10.7)
Disposal of Media (10.7.2)
Security of System Documentation (10.7.4)
Physical Media in Transit (10.8.3)
Electronic Messaging (10.8.4)
Monitoring (10.1)
Audit Logging (10.10.1)
Monitoring System Use (10.10.2)
Administrator and Operator Logs (10.10.4)
Clock Synchronization (10.10.6)

Documentation that may be Requested

Network configuration diagrams; dataflow diagrams; run books; standard operating procedures and desktop procedures; operations (network, processing) and incident response team organization charts; office/employee awareness materials and corporate policies (signed annually); change control manual (should include emergency change control procedures); minutes and reports; system and network outage and capacity utilization reports; incident-identification and response reports; test plans and results; third-party due diligence reports and contracts; policies, standards and guidelines; system and network criteria; planning and acceptance reports

F.1 Network Security – IDS/IPS Signature Updates

Objective:

Network intrusion detection system (IDS)/intrusion prevention sensors (IPS) are running the latest signatures.

Procedure:

- a. Obtain from the *service provider* the hostname, management IP, vendor, and model number of the network *IDS/IPS* sensors that monitor the *target systems*.
- b. Using the sampling parameters in Section N, select a sample of network *IDS/IPS* sensors from the list of network *IDS/IPS* sensors.
- c. Obtain a list of the five most recently released signatures, or rules, from each vendor's web site.
- d. Request a report or a screen shot from the *service provider* of the signatures, or rules, resident on the selected *IDS/IPS*.
- e. Report the signatures obtained in step c that are not present on each selected sensor.

Practitioners' Notes

It is highly recommended that the practitioner utilize the *service provider's* staff to display the Network *IDS/IPS* signatures while the practitioner views and compiles the results. The recommendation to utilize *service provider's* staff is being made within several of the Practitioners' Notes. This is for two reasons:

- 1) *Service providers* typically will not permit the practitioner to log on to production systems.
- 2) *Service provider's* staff has the specialized support knowledge of the local environment and the diverse systems that they manage.

Network Security – IDS/IPS Signature Updates

The *IDS/IPS* is not like an anti-virus system where there is an assumed signature level at any given point in time. Certain signatures are removed based on the needs and risks of the organization. Nevertheless, the *service provider* should be monitoring for the latest and most critical attacks and exploits.

F.2 Network Management – Encrypted Authentication Credentials

Objective:

Authentication credentials transmitted to network devices are encrypted in transit.

Procedure:

- a. During the *scoping meeting*, obtain the list of network devices.
- b. Using the sampling parameters in Section N, select a sample of network devices.
- c. Using the Practitioners' Notes, execute the prescribed commands and obtain the authentication parameters.
- d. Document the authentication methods utilized for each of the sample devices.

Practitioners' Notes

It is highly recommended that the practitioner utilize the *service provider's* staff to display the authentication parameters while the practitioner views and compiles the results.

Assumption

Network Devices have been documented at the scoping level.

Network Management – Encrypted Authentication Credentials

The main network devices that are typically deployed in organizations are Cisco devices; these use similar common commands across network platforms.

Cisco

- 1) Log on to device.
- 2) Execute the command:
 - PIX# *show run*; or
 - PIX# *show run | grep authentication (if supported)*
- 3) View authentication parameters, looking in particular for <type>

Example 1:

```
aaa authentication <type>
aaa authentication SSH console TACACS+
aaa authentication telnet console local
```

Example 2:

```
set authentication login tacacs enable <type>
set authentication login tacacs enable telnet primary
set authentication login tacacs enable http primary
```

Other Network Devices

Have *Service Provider* staff execute and observe the output.

Authentication Encryption Matrix:Authentication Method - Encryption Supported*

Telnet - No
 SSH - Yes
 HTTP - No
 HTTPS - Yes

* For supported authentication methods not listed above, read the Request for Comments (RFC) web site at www.rfc-archive.org, or the respective vendor web site, to ascertain whether encryption is enabled.

F.3 Externally Facing Open Ports**Objective:**

High-risk ports cannot be accessed from the Internet.

Procedure:

- a. Obtain from the *service provider* the public *IP* address range(s) corresponding to all *target systems*.
- b. Using the sampling parameters in Section N, select a sample of hardware systems from the report of the inventory of *target systems* obtained in *C.1 Asset Accounting and Inventory*.
- c. Obtain from the *service provider* a vulnerability assessment report generated within the past seven days that shows the open ports between 0 and 65,535 for each *IP* address sampled and document all open ports.

F.4 Remote Access and Remote Administration**Objective:**

Only approved remote access services exist.

Procedure:

- a. Obtain from IT a list of approved *IP* addresses that provide remote services (*VPN* or remote administration) from the Internet or public networks.
- b. Obtain a report from the *service provider* that indicates the results of conducting an external port scan within the scope of the *target systems*.
- c. Scan the report obtained in step b for the following remote access or remote administration services: Citrix, IPsec, L2TP, pcAnywhere, PPTP, Radmin, RDP, Rlogin, SSH, Telnet, VNC, GoToMyPC.
- d. Compare all *IP* addresses with remote administration or remote access services identified in the external port scan to the approved remote *IP* access services list and report the differences.

F.5 Network Logging

Objective:

Network connections are logged and the *attributes* listed below exist in the log files.

- 1) Source *IP*
- 2) Destination *IP*
- 3) Destination port
- 4) Protocol type (e.g., TCP, UDP, ICMP)
- 5) Timestamp

Procedure:

- a. Obtain logs from the client as per the Practitioners' Notes for each sample network device selected in *F.2 Network Management – Encrypted Authentication Credentials* for routers, *firewalls*, and switches and observe whether they are available for the two date ranges defined: one within 30 days and the second between 30 to 60 days.
- b. For both date ranges, inspect the logs for the presence of the following *attributes*.
 - 1) Source *IP*
 - 2) Destination *IP*
 - 3) Destination port
 - 4) Protocol type (e.g., TCP, UDP, ICMP)
 - 5) Timestamp

Practitioners' Notes

It is highly recommended that the practitioner utilize the *service provider's* staff to display the network logs while the practitioner views and compiles the results.

Assumption

Network Devices have been documented at the scoping level.

Network Logging

The main network devices that are typically deployed are Check Point, Cisco PIX (Router), Juniper and Syslog Server.

Check Point

- 1) Select Start, Programs, Check Point Client, Log Viewer, Log in.
- 2) Open logs for both intervals above.
- 3) To Filter: Select Column, right click, Selection, include target traffic under Selected Objects.
- 4) Repeat for all prescribed *attributes*

Cisco

- 1) SSH to Cisco device
- 2) Execute the command: `show log | grep <IP> | grep <attribute2> | grep <attribute3> | grep, etc.`
- 3) Repeat for all prescribed *attributes*.

Juniper

- 1) Log in into the NSM.
- 2) Select Log Viewer
- 3) To Filter: Select Column, right click, filter, set filter, enter target under "Add."
- 4) Repeat for all prescribed *attributes*.

Syslog Server

- 1) Log in to syslog system.
- 2) Identify logs for the two ranges
- 3) Execute the command: `Cat <logrange> | grep <IP> | grep <attribute2> | grep <attribute3> | grep, etc.`
- 4) Repeat for all prescribed *attributes*.

Other Network Devices

Have *Service Provider* staff execute and note the output.

F.6 Virus Protection (Servers)**Objective:**

Virus signature files are up-to-date for target servers.

Procedure:

- a. Using the sampling parameters in Section N, select a sample of Unix, Linux, Mac OS X and Windows servers from the report of the inventory of *target systems* obtained in *C.1 Asset Accounting and Inventory*.
- b. Request from IT a dated anti-virus software report and document the number of installed servers and the signature file in use on each system; the name of the anti-virus software vendor; software product; date of installed signature files; and the date of information capture for each system in the sample.
- c. Using the vendor's web site, obtain the three latest available signature files for each virus protection product identified in step b.
- d. For each system sampled, compare the anti-virus software report obtained in step b to the vendor's latest available signature and report differences.

F.7 Virus Protection (Workstations)**Objective:**

Virus signature files are up-to-date for target workstations.

Procedure:

- a. Using the sampling parameters in Section N, select a sample of Unix, Linux, Mac OS X and Windows workstations from the report of the inventory of *target systems* obtained in *C.1 Asset Accounting and Inventory*.
- b. Request from IT a dated anti-virus software report and document the number of installed workstations and the signature file in use on each system; the name of the

anti-virus software vendor; software product; date of installed signature files; and the date of information capture for each workstation in the sample.

- c. Using the vendor's web site, obtain the three latest available signature files for each virus protection product identified in step b.
- d. For each workstation sampled, compare the anti-virus software report obtained in step b to the vendor's latest available signature and report differences.

F.8 Control of Server Configuration

Objective:

Server configuration settings meet the Center for Internet Security (CIS) platform control standards.

Procedure:

- a. Using the sampling parameters in Section N, select a sample of servers from the report of the inventory of *target systems* obtained in *C.1 Asset Accounting and Inventory*.
- b. Using the report of inventory in step a, identify the operating system for each server.
- c. Request from IT the corresponding component template used to configure the selected operating systems.
- d. Obtain the current benchmark for each operating system identified in step b from the CIS web site (www.cisecurity.com) under Scoring Tools, in the Operating Systems section.
- e. Compare the settings for each server in the sample obtained in step c to the CIS benchmark obtained in step d and report differences.

F.9 Administrative Activity Logging

Objective:

The system audit log files contain the following *attributes*.

- 1) Account creation events
- 2) Timestamp of the account create event
- 3) Account name that created new account
- 4) Account created

Procedure:

- a. Haphazardly select a sample of operating systems from the report of the *inventory* of *target systems* obtained in *C.1 Asset Accounting and Inventory* that includes one of each type of operating system in use.
- b. Obtain a test user account on each system and report the date and time it was created.
- c. Using the Practitioners' Notes, observe the log for each system for the presence of following *attributes*.
 - 1) Event identifier
 - 2) Timestamp
 - 3) Creator's account name
 - 4) Account created

Practitioners' Notes

System administrator should delete or disable test account upon completion of procedure according to *security policy*.

Operating System	Audit Log Location
Windows NT, 2000, 2003	Event log → security log
Mandrake Linux	Var/log/syslog
RedHat Linux	Var/log/messages
SuSE	/var/log/messages
Mac OS X	/var/log/system
Free BSD	/var/log/messages
Solaris	/etc/security
HP-UX	/.secure/etc/auditfile1
AIX	/etc/security/audit/events
SCO	/var/adm/syslog
MVS, OS/390, z/OS - RACF	SMF, type 80
MVS, OS/390, z/OS – Top Secret	TSSUTIL REPORT DRC (PW) DATE(-07) END REPORT EVENT (AUDIT) DATE (-07) END
MVS, OS/390, z/OS – ACF2	SCFRPTPW

F.10 Log-on Activity Logging

Objective:

The *attributes* listed below are correctly reported in the system audit log files:

- 1) Successful and unsuccessful log-on attempts
- 2) Timestamp – both successful and unsuccessful log-on attempts
- 3) Terminal identity or location – both successful and unsuccessful log-on attempts

Procedure:

- a. Using the sampling parameters in Section N, select a sample of systems from the report of the *inventory* of *target systems* obtained in *C.1 Asset Accounting and Inventory*, including all operating systems in use.
- b. Obtain a test user account for each system selected in step a.
- c. Attempt to log on unsuccessfully to each system using the test user account and document the system date and time.
- d. Attempt to log on successfully to each system using the test user account and document the system date and time.
- e. Using the Practitioners' Notes, obtain the system audit log files for each system and report the presence of the following attributes for each of the log-on and log-off entries generated in steps c and d.
 - 1) Test user account
 - 2) Timestamp
 - 3) Terminal identity or location

Practitioners' Notes

System administrator should delete or disable test account upon completion of procedure according to *security policy*.

It is highly recommended that the practitioner utilize the *service provider's* staff to display the audit even codes while the practitioner views and compiles the results.

Operating System	Audit Log Location
Windows NT, 2000, 2003	Event log → security log
Mandrake Linux	Var/log/syslog
RedHat Linux	Var/log/messages
SuSE	/var/log/messages
Mac OS X	/var/log/system
Free BSD	/var/log/messages
Solaris	/etc/security
HP-UX	/.secure/etc/auditfile1
AIX	/etc/security/audit/events
SCO	/var/adm/syslog
MVS, OS/390, z/OS - RACF	SMF, type 80
MVS, OS/390, z/OS – Top Secret	TSSUTIL REPORT DRC (PW) DATE(-07) END REPORT EVENT (AUDIT) DATE (-07) END
MVS, OS/390, z/OS – ACF2	SCFRPTPW

F.11 Log Retention

Objective:

Audit logs are retained.

Procedure:

- a. Obtain an audit log file from each of the following day ranges: 85 to 95, 175 to 185; 265 to 275; and 360 to 370 for each of the systems sampled in *F.10 Log on Activity Logging*.
- b. Observe that each audit log contains log entries and report the day ranges of the selected log files.

F.12 Application Change Control

Objective:

A change management process is in place for documenting and executing operational changes in applications.

Procedure:

- a. Obtain from IT the most recent copy of the *master change log* for all *target systems*.

- b. Using the sampling parameters in Section N, select a sample of application changes from the *master change log* based on software reports in the report of the *inventory of target systems* obtained in *C.1 Asset Accounting and Inventory*.
- c. Inspect the *master change log* for presence of the following *attributes* for each selected application change:
 - 1) Reference/unique identifier
 - 2) Date submitted
 - 3) Date of the change
 - 4) Name of the affected system
 - 5) Approval status (approved / rejected)
- d. Obtain the *change initiation request (CIR)*, the *pre-deployment test document*, and the *post-deployment test document* for each selected application change.
- e. Inspect the documents for the existence of the following *attributes*.

Change Initiation Request:

 - 1) Name of the person initiating the change
 - 2) System(s) affected by the change
 - 3) Description of the change [including the file name(s) and file location(s)]
 - 4) Date the change will occur
 - 5) Approval signature by someone other than the person initiating the change
 - 6) Approval date

Pre-Deployment Test Document:

 - 1) Reference to a *CIR*
 - 2) Identified testing resource
 - 3) Test start date
 - 4) Test end date
 - 5) Expected test results
 - 6) Actual test results

Post-Deployment Test Document:

 - 1) Reference to a *CIR*
 - 2) Identified deployment resources
 - 3) Deployment's start date
 - 4) Deployment's end date
 - 5) Expected results
 - 6) Actual results
 - 7) Approval signature
 - 8) Approval date

F.13 Operating System Change Control

Objective:

A report for the installation of the most recent patch or maintenance level for operating systems exists in the *master change log*.

Procedure:

- a. Using the sampling parameters in Section N, select a sample of operating systems, which includes Unix, Windows and Linux operating systems, from the report of the *inventory of target systems* obtained in *C.1 Asset Accounting and Inventory*.

- b. For each operating system, use the Practitioners' Notes to identify the most recently installed patch or maintenance level.
- c. Compare the *master change log* obtained in *F.12 Application Change Control* to the most recently installed patch or maintenance level and report the presence of the most recent patch or maintenance level in the *master change log*.

Practitioners' Notes

Windows – Control Panel --> Add/Remove Programs or hfnetchk.exe
Unix: Solaris – showrev -p or patchadd -p
Unix: AIX – instfix -ia
Unix: FreeBSD – /usr/src/ patch -p
Unix: Mac OS X – /usr/bin/uname -v
Unix: HP/UX – swlist -l patch
Linux: Redhat – rpm -qa
Linux: Mandrake – rpm -qa
Linux: SuSe – rpm -qa

F.14 Web Site Privacy Policy

Objective:

A link to the *privacy policy* exists on the home page (main page) of each Internet-facing web server.

Procedure:

- a. Using the sampling parameters in Section N, select a sample of Internet facing web servers from the *target systems* report obtained in *C.1 Asset Accounting and Inventory*.
- b. Access each selected web server via a web browser.
- c. Observe whether a link to “*privacy policy*” exists on the home page (main page) directory.

F.15 Web Site - Client Encryption

Objective:

SSL is enabled and contains a valid *SSL* certificate for each web server.

Procedure:

- a. Using the sample of Internet facing web servers generated in *F.14 Web site Privacy Policy*, connect to each web site with Internet Explorer 5.0 or a later version and observe whether a golden lock appears on the bottom bar of the browser (depicting whether *SSL* is enabled).
- b. For each site with a golden lock present, document the digital certificate issuer, host it was issued to, expiration date, and encryption key length.

F.16 Email Relaying

Objective:

Email relaying by connecting to the *SMTP* port via Telnet is disabled.

Procedure:

- a. Select all *SMTP* servers from the *target systems* list obtained in *C.1 Asset Accounting and Inventory*.
- b. Telnet (without authenticating) into each identified *SMTP* port and attempt to send a message.
- c. Observe on the monitor whether the message failed (a “250 OK” reply from *DATA* command means attempt to send message was successful).

F.17 Physical Media Tracking

Objective:

Point-to-point monitoring and/or chain of custody tracking is in place for *physical media* used for transporting *sensitive information* between supplier locations or between the supplier and third parties from the time it is received until it is destroyed.

Procedure:

Pre-shipment

- a. During the *scoping meeting*, identify one media shipment scheduled to be made during the testing period.
- b. Haphazardly select a single item from the media shipment and inspect the selected item as it is being packaged for shipment for the following *attributes*.
 - 1) It is labeled with a unique *tracking* identifier.
 - 2) The company name or data classification does not appear on the outside of the container.
 - 3) There is a separate record identifying the information contents.
 - 4) If the media are packaged within a sealed outer container, the outer container also has the *attributes* listed in 1) and 2) above and there is a log showing which media are packaged within the sealed container.

Outbound Shipments

- a. Obtain the log used for tracking outbound media shipments.
- b. Per the sampling guidelines in Section N, select from the log a sample of shipments made during the past 90 days.
- c. For each shipment selected, inspect the log obtained in step a for the presence of the following *attributes*.
 - 1) Tracking identifier of the media or container shipped
 - 2) Date the shipment was picked up
 - 3) Company name and signature of the individual making the pickup
 - 4) Destination of the shipment
 - 5) Delivery confirmation report from the end recipient

Inbound Shipments

- a. Obtain the log used for tracking inbound media shipments.
- b. Per the sampling guidelines in Section N, select a sample of shipments received during the past 90 days.
- c. For each shipment selected, inspect the log obtained in step a for the presence of the following *attributes*.
 - 1) Tracking identifier of the media or container received
 - 2) Date the shipment was received
 - 3) Signature, name, and job title of the individual confirming receipt
 - 4) Source of the shipment

5) End destination of *physical media* following receipt

Internal Tracking

- a. Obtain the log used for tracking inbound media shipments.
- b. Per the sampling guidelines in Section N, select a sample of shipments received from financial institutions within the last 12 months.
- c. For each selected shipment, inspect the documentation received from the *service provider* identifying the current location of the media and a continuous chain of custody between initial receipt and its current location, and document the results.
- d. Observe that the location identified as the current location in step c.

Destruction

- a. Obtain the log used for tracking destruction of media containing *sensitive information*.
- b. Per the sampling guidelines in Section N, select a sample of destroyed media from the past year from the log used for tracking destruction of media containing *sensitive information*.
- c. For each selected media destruction event, inspect the log obtained in step a for the following *attributes*.
 - 1) Tracking identifier of the media destroyed
 - 2) Date of destruction
 - 3) For media destroyed in-house, the signature, name, and title of the person confirming destruction
 - 4) For media destroyed by a third party, obtain from the *service provider* the third party certificate of destruction that uniquely identifies the destroyed media and compare the third party certificate of destruction to attributes 1 and 2 and report the differences.

F.18 Security of Media in Transit

Objective:

Media in transit is secure (pickup and delivery is in a locked box).

Procedure:

- a. Obtain from IT a copy of the backup media off-site pickup and delivery schedule.
- b. Using the sampling parameters in Section N, select a sample of backup tapes from the *target systems*.
- c. Inspect the *service provider's* pickup and delivery records for the presence of the following *attributes*.
 - 1) Pickup and delivery date
 - 2) Lockbox identifier

F.19 Unapproved Wireless Networks

Objective:

Only vendor or *service provider*-approved wireless access points exist on the network.

Procedure:

- a. Obtain from IT the approved wireless access points list (802.11a/b/g).
- b. Inspect the *target systems' general perimeter* to identify any 802.11a, 802.11b, and

- 802.11g access points and document the respective service set identifier (*SSID*).
- c. Compare the *service provider's* approved wireless access points list (802.11a/b/g) to the access points identified in step b and report the differences.

F.20 Wireless Networks Encryption

Objective:

Encryption and authentication are required to connect to each access point on the approved wireless access points list (802.11a/b/g).

Procedure:

- a. Using the sampling parameters in Section N, select a sample of wireless access points from the vendor approved wireless access points list obtained in *F.19 Unapproved Wireless Networks*.
- b. Connect to each access point with a compatible client.
- c. Document both the authentication and encryption method as per the Practitioners' Notes.

Practitioners' Notes

It is highly recommended that the practitioner utilize the *service provider's* staff to observe the wireless access points from a client.

Wireless Networks Encryption

- 1) Under Network Connections, select Properties for the Wireless Network Connection.
- 2) Select Wireless Network Tab, and select from the list the specific access point to be viewed.
- 3) Select Properties, and Association.
 - **Authentication:**
Under Network Authentication note the method selected (e.g., Open, Shared, WPA, WPA-PSK, etc.)
 - **Encryption:**
Under Data Encryption note the method selected (e.g., Disabled, WEP, AES, TKIP, etc.)

F.21 Network Security –Firewalls

Objective:

At least one *firewall* exists, and is inspecting traffic between third parties, including the Internet, and the internal location where *target data* is stored.

Procedure:

- a. Obtain from the *service provider* the list of *firewalls*, which protect *target systems* from the Internet or third parties.
- b. Select a single *firewall* from the list obtained in step a.
- c. Request from the *service provider* a list of network connections that pass through the selected *firewall* and haphazardly select a single network connection.
- d. Request the *service provider* to provide the following for the connection selected in step c.

- 1) Source *IP* of the third party/Internet that passes through the *firewall* (include *NAT*'d source *IP* if *NAT* is utilized)
 - 2) Destination *IP* of the *target system* (include *NAT*'d Destination *IP* if *NAT* is utilized)
- e. Observe the *service provider* perform filtering of the logs from the *firewall* identified in step b for a period within the last 30 days, so that only network traffic between the third party *IP* address and the *target system IP* address obtained in step d are displayed; and report the existence of the *attributes* identified in step d for the following:
- 1) True or *NAT*'d source *IP*
 - 2) True or *NAT*'d destination *IP*

Practitioners' Notes

It is highly recommended that the practitioner utilize the *service provider's* staff to display the network logs while the practitioner views and compiles the results.

Network Security - Firewalls

The main *firewalls* that are typically deployed are Check Point, Cisco PIX and Juniper NetScreen.

Check Point

- 1) Select Start, Programs, Check Point Client, Log Viewer, Log in in.
- 2) Open logs.
- 3) To Filter: Select Column, right click, Selection, include target traffic under Selected Objects.
- 4) Repeat for all prescribed *attributes*.

Cisco

- 1) SSH to Cisco device
- 2) Execute the command: *Show log | grep <src IP> | grep <dst Ip>*
- 3) Repeat for all prescribed *attributes*.

Juniper NetScreen

- 1) Log in into the NSM.
- 2) Select Log Viewer.
- 3) To Filter: Select Column, right click, filter, set filter, enter target under "Add."
- 4) Repeat for all prescribed variables so as to match *IP* to *attributes*.

Other Network Devices

Have *Service Provider* staff execute and observe the output.

F.22 Network Security – Authorized Network Traffic

Objective:

Inbound and outbound network service traffic that accesses *target systems* are both documented and authorized within the information security program.

Procedure:

- a. Obtain from the approved network services list from the *service provider*.
- b. For the *firewall* selected in F.21 *Network Security –Firewalls.*, use the Practitioners' Notes to review the *firewall* rules and report rules that are not on the approved network services list obtained in step a.

Practitioners' Notes

It is highly recommended that the practitioner utilize the *service provider's* staff to display the network logs while the practitioner views and compiles the results.

Network Security – Authorized Network Traffic

The main *firewalls* that are typically deployed are Check Point, Cisco PIX and Juniper NetScreen.

Check Point

- 1) Select Start, Programs, Check Point Managed Client, Check Point Policy Editor, Log in.
- 2) View each rule that permits network services traffic and compare to documented authorized traffic obtained in step a.
- 3) Repeat for all permitted services.

Cisco PIX

- 1) SSH to Cisco PIX.
- 2) Execute the command: *PIX# show access-list*
View each rule that permits network services traffic and compare to documented authorized traffic obtained in step a.
- 4) Repeat for all permitted services.

Juniper NetScreen

- 1) Log in into the NSM.
- 2) Select Security Polices, and choose active policy.
- 3) View each rule that permits network services traffic and compare to documented authorized traffic obtained in step a.
- 4) Repeat for all permitted services.

Other Network Devices

Have *service provider* staff execute and observe the output.

F.23 Network Security – IDS Attributes**Objective:**

IDS/IPS alert events contain the following *attributes*.

- 1) Unique identifier
- 2) Date
- 3) Time
- 4) Priority level identifier
- 5) Event description
- 6) Notification sent to security team
- 7) Event status

Procedure:

- a. Using the sampling parameters in Section N, select a sample of *IDS/IPS* alerts generated in the last 90 days from the list of *IDS/IPS* sensors selected in *F.1 Network Security – IDS/IPS Signature Updates*.
- b. Inspect the alert event for the presence of the following seven attributes and report whether they are present.
 - 1) Unique identifier
 - 2) Date
 - 3) Time

	<p><i>Financial Institution Shared Assessments Program</i> <i>Agreed Upon Procedures</i> <i>Version 2.0</i></p>
--	---

- 4) Priority level identifier
- 5) Event description.
- 6) Notification sent to security team
- 7) Event status

G. Access Control

BITS Matrix Reference

High Level Expectation

Business Requirements for Access Control High-Level Expectation: Service providers should have and adhere to a documented policy to ensure that only properly approved users are granted access to financial institution information systems and assets. Users should be granted access on a need-to-know basis, according to job responsibilities. The access-control policy should employ methods designed to physically and logically restrict access to equipment, ensure the identification and authentication of individuals who access computing resources, and restrict an individual's access to information once the individual has accessed a system. Depending on the level of protection required (based on the asset classification), a combination of access-control techniques may need to be employed.

User Access Management High-Level Expectation: To protect the confidentiality and privacy of data and information, user access capabilities should be configured with least privilege. User access rights and privileges should be consistent with users' assigned job responsibilities for performing a particular function or transaction.

User Responsibilities High-Level Expectation: Users should be aware of their responsibilities for maintaining effective access controls, particularly as they relate to password security and user equipment. Service providers should have a written authorized user accountability policy that incorporates authentication standards and clearly articulates user responsibilities.

Network Access Control High-Level Expectation: The design of the service provider's internal and external networks should demonstrate a commitment to secure networking. The design must be documented, on paper or in an electronic chart, including notes. External connections should be managed carefully; connections to networks for third parties should only be created after security due diligence has been completed. Procedures should verify the authenticity of the counterparty providing electronic instructions or transactions through trusted exchange of passwords, tokens, or cryptographic keys.

Operating System Access Control High-Level Expectation: Service providers should implement operating system access controls that protect the systems from compromise. Protections should include but are not limited to appropriate system authorization and management.

The service provider should maintain and adhere to policies and processes that restrict user access to information and application functions, and prevent and detect unauthorized access to information systems.

Service providers should be able to monitor the use and administration of systems. The monitoring system should produce an audit trail that allows the service provider to respond quickly to high-risk events. The monitoring system should be based on current vulnerability and risk analysis, and should be integrated with an incident-response capability.

Service providers should maintain and adhere to policy, standards, procedures, and controls for governing the security of information and systems accessed from outside company facilities, as well as the security of information stored on mobile and telecommuting equipment.

ISO 17799 Matrix Reference

User Access Management (11.2)
User Password Management (11.2.3)
Review of User Access Rights (11.2.4)
Password Use (11.3.1)
Network Access Control (11.4)
Remote Diagnostic and Configuration Port Protection (11.4.4)
Network Connection Control (11.4.6)
Secure Log on Procedure (11.5.1)
User Identification and Authentication (11.5.2)
Password Management System (11.5.3)
Session Timeout (11.5.5)

Documentation that may be Requested

Security policy with access policy, user policy and network access controls, network architecture diagram (including placement of firewalls), application access control procedures, dataflow diagram

G.1 Password Controls**Objective:**

The password settings from the system configuration file on each system are implemented.

Procedure:

- a. Using the sampling parameters in Section N, select a sample of hardware systems from the report of the inventory of *target systems* obtained in *C.1 Asset Accounting and Inventory*.
- b. Using the report of inventory in step a, identify the operating system and version for each system.
- c. Observe and document the following password settings from the system configuration file on each system:
 - 1) Initial password change
 - 2) Minimum password length
 - 3) Password complexity
 - 4) Password history limit
 - 5) Lockout attempts
- d. Request creation of test accounts on the systems selected in step a.
- e. Observe the following password settings on each system using the test accounts:
 - 1) Initial password change – Log on successfully to the *target system* and report whether or not the user is forced to change his password.
 - 2) Minimum password length – Attempt to change the password to a character password. If the change is permitted, report the minimum length as one character. If the change is not permitted, conduct the same test for up to 10 characters and report the minimum length permitted.
 - 3) Password complexity – Attempt to change the password to a purely alphabetic password, using no numerals (0 1 2 3 4 5 6 7 8 9) or special characters (~`!@#\$\$%^&*()-+=\|}]][{}“”’;:/?.>,<). Based on the attempt to change the password, report whether *complex passwords* are required.
 - 4) Password history limit (prevention of recent password re-use) – Change the password one time and then attempt to change the password back to the original password. If the change is accepted, report the minimum password history as one. If the change is not accepted, repeat the test for

a history of at least five. Report the results.

- 5) Lockout attempts – Incorrectly enter the password one time. After entering the password incorrectly, attempt to log in using the test account. If the log-in is not permitted, report the number of failed lockout attempts as one. If the log-in is permitted, repeat the test for up to five attempts. Report the results.

Practitioners' Notes

System administrator should delete or disable test account upon completion of procedure according to *security policy*.

G.2 Revoke System Access

Objective:

User access is removed upon termination.

Procedure:

- a. Obtain from HR a list of *constituents* terminated in the past 12 months.
- b. Using the sampling parameters in Section N, select a sample of hardware systems from the report of the *inventory* of *target systems* obtained in *C.1 Asset Accounting and Inventory*.
- c. Inspect the user account listing for the selected systems for the presence of and report terminated *constituents* and report those that are present on the systems selected.

G.3 Access Authorization

Objective:

There is an approval process for access requests.

Procedure:

- a. Using the sampling parameters in Section N, select a sample of hardware systems from the report of the *inventory* of *target systems* obtained in *C.1 Asset Accounting and Inventory*.
- b. Using the sampling parameters in Section N, Select a sample of user IDs from the *target systems* selected in step a.
- c. Obtain the authorization (paper or electronic) to grant privileges to the selected user IDs.
- d. Inspect the authorization for the selected user IDs for an indication of authorization and report the name(s) of the approvers listed as authorizing access.

G.4 Inactive Accounts

Objective:

Inactive accounts are locked or disabled.

Procedure:

- a. Using the sampling parameters in Section N, select a sample of hardware systems from the report of the *inventory* of *target systems* obtained in *C.1 Asset Accounting and Inventory*.

- b. Using the sampling parameters in Section N, select a sample of user IDs from the selected *target systems*.
- c. Obtain from IT a list of the last log-on date for all selected users including accounts that have never signed on or have not signed on in the past 30 days.
- d. Obtain from IT a list of all accounts on each system that are disabled or locked out.
- e. Compare the two lists, obtained from steps c and d and report whether the inactive accounts were either disabled or locked out after a 30-day period of inactivity.

G.5 Controls for Unattended Systems

Objective:

Console/CPU is protected by one of the following controls if unattended for a period of inactivity:

- 1) Password protected screensaver
- 2) Session timeouts (forced logout)
- 3) Key lock (keyboard usage requires authentication)

Procedure:

- a. Haphazardly select one hardware system per operating system from the report of the *inventory of target systems* obtained in *C.1 Asset Accounting and Inventory*.
- b. Inspect the system configuration of each system to document control utilized for the timeout variable.
- c. Observe whether one of the following controls protects the system after the timeout period and report the results.
 - 1) Password protected screensaver
 - 2) Session timeouts (forced logout)
 - 3) Key lock (keyboard usage requires authentication)

H. Information Systems Acquisition, Development and Maintenance

BITS Matrix Reference

High Level Expectation

Service providers should have and adhere to an established process for developing secure infrastructure, systems, and/or applications. Programs written for and/or used by the receiver company should be certified as free from malicious code and patent-infringement issues and appropriate for use by the receiver company. The programs should also be protected from unauthorized copy, use, duplication, and storage, with asset-management requirements specified.

Appropriate controls and audit trails or activity logs should be incorporated into the application system's design. These controls should include the validation of input data, internal processing and output data. Application systems should also provide controls to allow the receiver company to segregate the duties of employees using the applications.

Service providers should use internationally or nationally accepted cryptographic methods and key-management techniques to protect information when other controls do not provide adequate protection or if the receiver company's information-classification policy dictates.

Service providers should document, control and maintain system files.

Service providers should ensure all proposed system changes are reviewed and tested to be sure they do not compromise the security of either the system or the operating environment.

ISO 17799 Matrix Reference

Control of Operational Software (12.4.1)

Technical Vulnerability Management (12.6)

Control of Technical Vulnerabilities (12.6.1)

Documentation that may be Requested

Application security policy, network configuration diagrams, dataflow diagrams, change control policy, programming standard and guidelines, certifications of encryption algorithms, documentation of security reviews of application code, vulnerability assessments of application and environment

H.1 Patch Levels of Vulnerable Systems

Objective:

Patch levels of the "SANS Top 20" most vulnerable operating systems are current.

Procedure:

- a.** Using the sampling parameters in Section N, select a sample of Windows, Unix, and Linux and Mac OS X systems from the *target systems*.
- b.** Obtain from the operating system vendor the most current patch level.
- c.** For each operating system, use the appropriate method per the Practitioners' Notes to identify the most recently installed patch or maintenance level and report the operating system, the vendor's most current patch level, the patch level resident on the operating system, and the date of capture.

Practitioners' Notes

Windows: Open "My Computer" select "About Windows" from the "Help" menu.
Unix: Solaris - showrev -p or patchadd -p
Unix: AIX - instfix -ia
Unix: HP/UX - swlist -l patch
Linux: Redhat - rpm -qa
Linux: Mandrake - rpm -qa
Linux: FreeBSD - /usr/src/ patch -p
Linux: SuSe - rpm -qa
Mac OS X: /usr/bin/uname -v
IPSO: ver

H.2 Router Vulnerabilities**Objective:**

Router configuration and maintenance includes the following *attributes*.

- 1) Known vulnerabilities in routers are addressed.
- 2) Default router passwords are not in use.
- 3) Default SNMP community strings are not in use, and devices are set to SNMP read-only mode.
- 4) Router operating system patch levels are current.
- 5) IP source routing is disabled.

Procedure:

- a. Using the sampling parameters in Section N, select a sample of hardware systems from the report of the *inventory of target systems* obtained in *C.1 Asset Accounting and Inventory*.
- b. For each *target system*, run the command "traceroute 64.38.0.126."
- c. From the traceroute response, obtain from IT the addresses that are *service provider*-controlled routers and the respective vendors.
- d. For the routers selected in step c, obtain from the router vendors a list of default user IDs and passwords.
- e. Observe the *service provider's* staff attempt to log on to the target routers using the default user ID and password.
- f. Record instances of successful log on attempts using the default user ID and password.

Practitioners' Notes

Vendor	Command
CISCO	show run; show version
Juniper	show config ; show version
Other	Record vendor only

H.3 Firewall Patch Levels

Objective:

Firewalls contain the most current patch level.

Procedure:

- a. Using the *firewall* selected in F.21 *Network Security – Firewalls*, observe the *service provider's* staff extract the current operating system patch level from the selected *firewall* using the Practitioners' Notes under H.1 *Patch Levels of Vulnerable Systems*.
- b. Obtain from the vendor web site for the current patch level for the *firewall* operating system.
- c. Report the operating system name, *firewall* operating system patch level, latest operating system patch level from the vendor site, and the date of capture.

I. Information Security Incident Management

BITS Matrix Reference

N/A

ISO 17799 Matrix Reference

Responsibilities and Procedures (13.2.1)

Documentation that may be Requested

N/A

Note: Version 2.0 of the Shared Assessments Program AUP does not include objectives and procedures under this ISO 17799:2005 control area.

J. Business Continuity Management

BITS Matrix Reference

High Level Expectation

Service providers are expected to have comprehensive business continuity plans, including having technology solutions that ensure recovery of services to receiver company during a time of business interruption. These plans should be tested at least annually and results of the tests should be made available to the receiver company. These plans also must be approved by service provider management annually in order to comply with FFIEC regulations. The service provider is responsible for ensuring its suppliers have business continuity programs and that those plans are included in recovery testing.

ISO 17799 Matrix Reference

N/A

Documentation that may be Requested

Business continuity plan, technology recovery plan(s), testing schedule, latest test results or generic test results, contract, copy of insurance declaration pages

J.1 Business Impact Analysis

Objective:

The *service provider* conducted a business impact analysis.

Procedure:

- a. Obtain a copy of the *service provider's* business continuity plan (BCP).
- b. Obtain a copy of the most recent business impact analysis (BIA).
- c. Inspect the BCP for the presence of the following *attributes* for each business process identified in the BIA.
 - 1) Business process priority (i.e., high, medium or low; numerical rating)
 - 2) Maximum allowable downtime
 - 3) Costs associated with downtime

J.2 Threat Assessment

Objective:

The BIA addresses the threats identified by the FFIEC for business continuity planning.

Procedure:

- a. Using the sampling parameters in Section N, select a sample of business processes from the BIA obtained in *J.1 Business Impact Analysis*.
- b. Inspect the BIA for each of the threats listed below and document whether the threat has been categorized based on impact and the probability of occurrence for each business process.
 - 1) Fraud
 - 2) Theft
 - 3) Blackmail
 - 4) Sabotage
 - 5) Terrorism
 - 6) Fire

- 7) Floods or water damage
- 8) Severe weather
- 9) Air contaminants
- 10) Hazardous chemical spills
- 11) Communications failure
- 12) Power failure
- 13) Equipment failure
- 14) Software failure
- 15) Transportation system disruptions
- 16) Telecommunication system disruptions

K. Compliance

BITS Matrix Reference

High Level Expectation

Service providers should establish and adhere to policies to ensure compliance with applicable legal and regulatory requirements, including agency legal opinions and guidelines. These regulatory requirements should reflect any international environments that must be accommodated based on processing locations.

Information systems should be audited regularly for compliance with the service provider's security policies and standards.

Based on the risk assessment of the services outsourced, an annual assessment of the service provider by an independent auditor or assessor, including testing of controls and onsite testing and validation, may be required. The scope of the report should include the environment used to process the receiver company's applications and data and a follow-up review to confirm that recommendations have been implemented. The receiver company should retain the right to audit in order to ensure that controls are verified as deemed necessary by the results of the receiver company's risk assessment.

ISO 17799 Matrix Reference

Technical Compliance Checking (15.2.2)

Documentation that may be Requested

Vulnerability test reports, list of administrators, audit log files third-party assessment reports

K.1 Presence of Log-on Banners

Objective:

Log-on banners are present that indicate the system is private and that unauthorized access is not permitted.

Procedure:

- a.** Using the sampling parameters in Section N, select a sample of systems from the report of the *inventory of target systems* obtained in *C.1 Asset Accounting and Inventory*.
- b.** Observe a user log on to each system and document whether a log-on banner is present that indicates the system being entered is private and unauthorized access is not permitted.

K.2 Technical Compliance Checking - Vulnerability Testing and Remediation

Objective:

Vulnerability assessments of *target systems* are performed and vulnerabilities identified in vulnerability assessments are remediated.

Procedure:

- a.** Using the sampling parameters in Section N, select a sample comprised of no less than one *target system* for each operating system from the report of the *inventory of target systems* obtained in *C.1 Asset Accounting and Inventory*. Note: Exclude any systems running operating systems that are not listed in the OS column of the table appearing in Section M.

- b.** For each system sampled in step a, obtain from the *server provider* at least two vulnerability assessment reports produced using one of the automated testing tools listed in the table in Section M: one within the past twelve months and the second within the past one month.
- c.** Document the name of the report for each system selected, the date of the most recent assessment, and the testing tool and version that was used to produce the most recent report.
- d.** For each system tested, report the number of vulnerabilities that are common to both reports.

L. Glossary of Terms

Anti-Tailgating / Piggybacking Mechanism – Two sets of doors whereby access to the second is not granted until the person has passed through (and closed) the first, often referred to as a “man trap.”

Asset Control Tag – A unique identification number assigned to all inventoried assets.

Attribute - A property or field of a particular object.

Change Initiation Request (CIR) – A document (physical or electronic) used to track change requests, including new features, enhancement requests, defects, and changed requirements. The change initiation request document must contain the following items:

- Name of the person initiating the change
- System(s) affected by the change
- A description of the change which includes the file name(s) and file location(s)
- The date the change will occur
- An approval signature by someone other than the person initiating the change
- An approval date

Complex Password – A password that is a combination of alphabetic and non-alphabetic characters such as special or numeric characters.

Confidentiality – The protection of *sensitive information* from unauthorized disclosure and sensitive facilities from physical, technical, or electronic penetration or exploitation.

Constituent – An active employee or contractor.

Facility – A structure, building or multiple structures or buildings in which the operations are conducted for the services provided. These operations include handling, processing and storage of information, data or systems as well as personnel that support the operations.

Firewall – A set of related programs, located at a network *gateway* server that protects the resources of private networks from other networks. Firewalls can be application/proxy, packet filtering, or stateful based. Examples of firewalls are Cisco PIX, Check Point Firewall, Juniper NetScreen & Cyberguard. Though they contain some firewall functionality, routers are not included in this definition.

Gateway – A *node* on a network that facilitates the communication of information between two or more *nodes*.

General Perimeter – The area with fully enclosed walls that extend from floor to ceiling (beyond raised floors and ceilings) surrounding the *secure perimeter*. This may be the same floor as the *secure perimeter*, if shared by other tenants in the *facility*, or the *facility* itself.

IDS – An Intrusion Detection Systems (IDS) is a security inspection system for computers and networks that can allow for the inspection of systems activity and inbound/outbound network activity. The IDS key function identifies suspicious activity or patterns that may indicate a network or system attack. Examples of IDS systems and vendors are ISS, SNORT, Dragon and Cisco.

Immediate Perimeter – A rack or cage housing the *target systems*.

Inventory – An itemized list of current assets.

IP – Internet Protocol (IP) is the networking standard that allows messages to be sent back and forth over the Internet or other IP networks.

IPS – An Intrusion Protection System (IPS) is a more sophisticated Intrusion Detection System (IDS) that allows administrators to configure predefined actions that should be taken if suspicious activity is detected.

Master Change Log – A document or database that contains a report of each *change initiation request* (CIR) (approved or rejected). The document or database must contain the following items:

- A reference to a CIR
- Date submitted
- Date of change
- Name of affected system
- Approval status (approved or rejected)

NAT – Network Address Translation (NAT) involves re-writing the source and/or destination addresses of IP packets as they pass through a network device.

NPI – Non-Public Personal Information (NPI) is “any personally identifiable financial information that is not publicly available,” according to Federal Trade Commission document 16 CFR 313.3(n). Non-Public Information includes but is not limited to name, address, city, state, Zip code, telephone number, Social Security number, credit card number, bank account number and financial history.

Node – Any physical device with a unique network address on the network.

Ownership – A formally assigned responsibility over a given asset.

Physical Media – Any portable device or substance (e.g., paper) used to store data for specific and legitimate purposes. The following types of devices are examples of physical media:

- Magnetic tapes and disks
- Cartridges, including 9-track, DAT, and VHS
- Optical disks in CD and DVD format
- Microfilm/fiche
- Paper (e.g., computer-generated reports and other printouts)
- Static memory devices, such as USB “memory sticks”

PIN – Personal Identification Number (PIN) is a secret shared between a user and a system that can be used to authenticate the user to the system.

Post-Deployment Test Document – A document that provides evidence that the change was tested and approved in the production environment. The document must contain the following items:

- Reference to a CIR
- Identified deployment resources
- Deployment start date
- Deployment end date
- Expected results
- Actual results
- Approval signature
- Approval date

Pre-Deployment Test Document – A document (electronic or paper) that provides evidence that the requested changes were tested prior to deployment in the production environment. The document will be inspected for the following items:

- Reference to a CIR
- Identified testing resources
- Testing start date
- Testing end date
- Expected test results
- Actual test results

Privacy Policy – A *service provider’s* official statement (on a web site or by other means) addressing the type of information collected, how the information will be used, how the individual may access this data and the steps for having the data removed. A privacy

statement will usually include information regarding systems in place to protect the information of web site visitors, consumers or other persons whose data is being collected and used.

Receiver Company – The financial institution that has contracted with a *service provider* to have a specific service performed.

Scoping Meeting – Meeting held prior to commencement of the Shared Assessments AUP engagement during which the financial institutions and *service providers* determine the *service providers’ target systems*.

Secure Perimeter – A space fully enclosed by walls that surround the *immediate perimeter*, extend from floor to ceiling (beyond raised floors and ceilings), is contained, and the points of entry of which are secured.

Security Policy – A document or set of documents that a *service provider* has published defining requirements for one or more aspects of information security.

Sensitive Information – Also known as “*Target Data*.” Any customer data stored at the *service provider’s facility*. This data may be stored in the form of *physical media*, digital media, or any other storage medium.

Service Provider – An organization that provides outsourced services such as data processing, applications or systems to a financial institution.

SMTP – Simple Mail Transfer Protocol (SMTP) is the de facto standard for email transmissions across the Internet.

SSID – Service Set Identifier (SSID) is a 32-character unique identifier attached to the header of packets sent over a wide area network so as to identify each packet as part of that network.

SSL – Secure Socket Layer (SSL) is a protocol developed by Netscape for transmitting private documents via the Internet. SSL uses a cryptographic system that uses two keys to encrypt data: a public key known to everyone and a private or secret key known only to the recipient of the message.

Target Data – A financial institution’s Non-Public Personal Information (NPI) that is stored, transmitted, or processed by the *service provider*.

Target System – Computer hardware and software in scope for the engagement and containing *target data*.

True ceiling – The permanent overhead interior surface of a room constructed of solid building materials offering resistance to and evidence of unauthorized entry.

True floor – The permanent bottom interior surface of a room constructed of solid building materials offering resistance to and evidence of unauthorized entry.

Unapproved – Operating without consent.

Vibration Alarm Sensor – An alarm that responds to vibrations in the surface onto which it is mounted. A normally closed switch momentarily opens when the sensor is subjected to a vibration of sufficiently large amplitude.

VPN – Virtual Private Network (VPN) is a communication tunnel running through a shared network such as the Internet, which uses encryption and other security mechanisms to ensure the data cannot be intercepted and that the data senders and receivers are authenticated.

M. Approved Scanning Tools

Practitioners' Notes

The following table illustrates acceptable scanning tools (minimum version).

Also acceptable are scanning tools that have been approved for use in the Payment Card Industry (PCI) Data Security Standard.

Vendor	Operating System	Version
<u>ShadowSecurityScanner</u>	Unix, Linux, FreeBSD, OpenBSD, NetBSD, Solaris and, of course, Windows 95/98/ME/NT/2000/XP/.NET	Version: 7.55
GFI LANguard Network Security Scanner	98/NT/2000/XP/2003 Basic Linux	Version: 7.0
NetworkActiv Scanner	98/ME/NT/2000/XP	Version: 4.0
Retina		Version 5.4.17
Advanced Administrative Tools	9x/Me/NT4/2000/XP	Version: 5.92
FoundStone Enterprise FoundScan	NT/Win2K/Win9x/WinME/WinXP/Linux/Solaris	Version: 4.0
<u>SuperScan</u>	Windows 2000 and XP only	Version: 4.0
ISS Internet Scan	Windows, Unix	Version: 7.0
Cisco Secure Scanner	Unix, Linux, Windows, and NetWare	Version: 2.0.2.3
Core Impact	Unix, Linux, Windows, and NetWare	Version: 6.0
NetRecon	Unix, Linux, Windows, and NetWare	Version: 3.6
Nessus	Unix, Linux, Windows, and NetWare	Version: 3.0
SAINT	Unix, Linux, Windows, and NetWare	Version: 6.2.4
ETrust Vulnerability Manager	Unix, Linux, Windows, and NetWare	Version: 8.3
QualysGuard	Unix, Linux, Windows, and NetWare	Version: 4.2.26-1
NetIQ Vulnerability Manager	Windows, Unix, Linux, NetWare	Version: 5.5

N. Sampling Parameters

The table below reflects the sample size for a population using the haphazard sampling selection technique.

Population	Sample Size
X > 300	30
60 < X < 300	10%
10 < X < 60	6
X < 10	Lesser of 5 or All

Sample of *constituents* must represent both employees and contractors.