The Shared Assessments Program

Agreed Upon Procedures

Version 5.0 Assessment Guide

BITS
1001 Pennsylvania Avenue, NW
Suite 500 South
Washington, DC 20004
www.bits.org

The Santa Fe Group
3 Chamisa Drive N., Suite 2
Santa Fe, NM 87501
(505) 466-6434
www.santa-fe-group.com
www.sharedassessments.org

The Shared Assessments Program is administered by The Santa Fe Group (www.santa-fe-group.com). Questions about this document and the program should be directed to:

Michele Edson
Senior Vice President
The Santa Fe Group
505-466-6434
sharedassessments@santa-fe-group.com

Table of Contents

Introduction to the Shared Assessments Program and the Agreed Upon Procedures

More and more, companies of all sizes are outsourcing applications, systems and services to service providers around the globe. While a virtually unlimited number of business functions can be moved outside the walls of any business, responsibility for reputation, transaction, regulatory and other risks remain with the outsourcing organization. To manage these risks, companies must carefully evaluate the controls their service providers have in place for security, privacy and business continuity.

The Shared Assessments Program (www.sharedassessments.org) was originally developed by Bank of America Corporation, The Bank of New York Mellon, Citi, JPMorgan Chase & Company, U.S. Bank, and Wells Fargo & Company in collaboration with leading service providers and the Big 4 accounting firms. These founding organizations saw the need for a standardized and objective vendor management assessment methodology that would help outsourcers meet regulatory and risk management requirements while significantly reducing costs for all stakeholders.

The Shared Assessments Program pilot was completed in 2005, and Version 1 of the Program's tools was published in February 2006. Today, the Shared Assessments Program membership has grown to nearly 60 participating companies. Under the management of strategic consultancy The Santa Fe Group (www.santa-fe-group.com), this community of outsourcers, service providers and assessment firms work together to foster adoption of the Shared Assessments standards around the globe.

Now entering its fifth year, Shared Assessments offers a one-stop shop for industry-standard tools for evaluating service provider controls for security, privacy and business continuity. The Shared Assessments Program's goals are to:

- **Standardize the collection of information about security, privacy, and business continuity controls** through a consistent and repeatable evaluation process
- **Reduce costs and increase efficiencies** for outsourcers and their service providers
- **Raise the bar on security** in industries that outsource critical information services through more rigorous assessments for security, privacy and business continuity

A Global Community

Shared Assessments Program members are national and international organizations of all sizes that understand the importance of comprehensive standards for managing risk. They are financial institutions, healthcare organizations, retailers and telecommunications companies. They are service providers of all sizes and types, including business process outsourcers, technology management outsourcers, application service providers, partners/suppliers, application software and hosting providers, and assessment firms of all sizes. They are the best in their class, members of a global community of risk management experts who understand the value of implementing efficient and effective industry-standard practices.

In addition to its members, the Shared Assessments Program maintains strategic alliances with global associations including the National Association of Software and Services Companies

(NASSCOM) and the Securities Industry and Financial Markets Association (SIFMA). Additionally, the Program licenses the Shared Assessments standards to software providers who wish to integrate the tools into their products. Shared Assessments also continues its affiliation with industry association BITS (www.bits.org), whose financial institution members originally founded the Program. The Santa Fe Group manages the Shared Assessments Program. Together, Shared Assessments' diverse community members work to increase awareness and adoption of the Program tools across industry sectors and around the globe.

Using the Agreed Upon Procedures

Together with the Shared Assessments Standardized Information Gathering Questionnaire (SIG), the Shared Assessments AUP is used by outsourcers to evaluate the controls their service providers have in place for security, privacy and business continuity. Both the AUP and the SIG are aligned with ISO 27002:2005, PCI DSS, COBIT, and NIST as well as FFIEC Guidance, the AICPA/CICA Privacy Framework, and a host of privacy regulatory guidance.

The AUP was created for use by independent accounting and assessment firms that conduct on-site audits of service provider controls. The AUP provides objective and consistent procedures that evaluate key controls in the following domains of risk management:

- Information 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
- Compliance
- Privacy

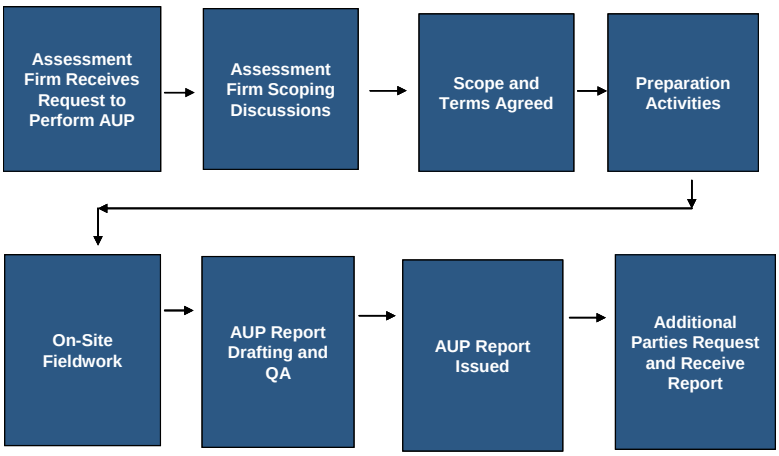
The AUP procedures follow the American Institute of Certified Public Accountants (AICPA) professional standards Attestation Standard (AT) Section 201, which sets forth attestation standards and provides guidance to practitioners on performance and reporting in AUP engagements.

Objective results of the AUP are provided directly to the service provider by the audit or assessment firm. The service provider may then share the report with a virtually unlimited number of clients, who evaluate the report in the context of their engagement(s) with the service provider and industry risk management and regulatory requirements.

AUP reports typically consist of population, sample size and number of failures within the sample. No subjective opinions are formed, allowing the outsourcing organization to form its own opinions of the results in the context of its own risk appetite. Depending on the recipient, AUP reports may be used in place of a costly onsite assessment, reducing assessment costs for both the service provider and the outsourcer. *Anecdotal evidence indicates that medium-sized organizations can expect an AUP assessment to be completed in approximately five days onsite.*

Agreed Upon Procedures Engagement

Typical AUP engagements proceed as diagrammed below.



As indicated, the scope of an AUP engagement must be determined before any procedures are executed. The scope must take into account the type of service provider, its business, the type of Target Data, Protected Target Data, Privacy Target Data and Protected Privacy Target Data it collects, stores, uses, shares, transports, retains, secures and/or deletes. Given this information, the target systems or processes are defined along with their supporting hardware, software and procedures to be tested. The applicability of each procedure should be determined during scoping discussions, assisting the practitioner in:

- Understanding the service provider's environment
- Identifying the documentation the service provider will need to provide
- Determining the order in which the procedures will be executed

The majority of procedures in this document have been determined by the Shared Assessments Technical Development Committee's AUP team to be core to the scope of a typical engagement. Testing those procedures provides the depth of inspection outsourcing clients typically expect, potentially saving time and effort for both the client and the service provider when clients are willing to accept the AUP report in lieu of their own on-site examination.

Procedures marked with an asterisk (*) may be used depending on the industry verticals a service provider serves and/or the specific services it offers to demonstrate a higher level of control(s) in certain areas.

Examples of non-core procedures intended for use according to verticals served and/or services offered are:

- Application security procedures (ASP, SaaS, Cloud)
- Business process outsourcing procedures (contact centers)
- Business continuity procedures (telecommunications or other critical infrastructure organizations)
- Privacy procedures

When all applicable procedures are completed, the audit or assessment firm provides the service provider with a report of its findings. *This report does not express an opinion and covers only those procedures performed under the scope of the agreement.*

After reviewing the report and providing it to clients, service providers are strongly encouraged to communicate with clients about the content of their report. Specifically, the service provider should:

- Identify any mitigating and compensating controls that were not tested during the AUP assessment. (This information may need to be tailored according to the services subscribed to by the client or in accordance with relevant contracts.)
- Describe any remediation plans, including how and when issues will be addressed and plans for testing to demonstrate that the required changes have been implemented. (Service providers should understand that most clients will require remediation plans.)

Agreed Upon Procedures Format

Each AUP control area contains:

- **Objective(s):** Statement(s) describing the business interest behind assessing the domain
- **Control(s):** Statement(s) about the controls service providers should have in place
- **Procedure(s):** The action or actions a practitioner will perform to test each control area
- **Industry Relevance:** Reference(s) to other standards that apply to the same objective and control as the procedure

Certain terms and phrases in this document are italicized. These terms and phrases are defined in the glossary (Section X).

Sampling Methodology

Some procedures rely on sampling, which falls into four types:

- **Random sampling of an entire population**. In these cases, a population of items gathered as a part of an AUP will subsequently require a random sample to be taken from the entire population. Refer to Section Y to determine the number of items to be sampled based on population size.
- **Random sampling of a population subset.** A population gathered as a part of an AUP may include items with many characteristics, but require only certain characteristics of that population be sampled. For example, G.1 requires the sampling of IDS/IPS sensors from the Asset Accounting and *Inventory* list. The list contains more items than IDS/IPS sensors. The list should first be reduced to include only those specific items; then a random sample can be taken. Refer to Section Y to determine the exact number of items to be sampled based upon the resulting population size.
- **Reuse of samples.** Certain procedures reuse samples from other procedures. In these cases, no further sampling is needed. For example, H.2 relies on a hardware sample taken in H.1.
- **Judgmental sampling.** Certain procedures require a specific type or number of characteristics from the population to be included in the sample. For example, G.7 requires that at least “one of each type of operating system in use for workstations, servers and network devices” be a part of the sample. The sampling methodology is

described in the AUP. Refer to Section Y to determine the exact number of total items to be sampled based on the resulting population size.

Target Data Tracker

The Target Data Tracker tool, available for download at the Shared Assessments site (www.sharedassessments.org), was created to help outsourcers determine where their Critical Data resides, both at the Service Provider and Dependent Service Provider levels. Because outsourcers cannot examine their controls without first examining their data, the Target Data Tracker provides the outsourcer with critical information about the location of data at up to 40 service provider and dependent service provider locations. The Target Data Tracker can be completed in a relatively short time and used either as a standalone document or prior to completing the SIG tool or an AUP assessment.

Other Shared Assessments Program Resources

The Shared Assessments Technical Development Committee has published a number of white papers designed to assist organizations that are evaluating adoption and integration of the Shared Assessments Program:

- *An Integrated Approach – ISO 27001 and the Shared Assessments Program: A Perspective of BSI Management Systems and the Shared Assessments Program*
- *Shared Assessments Program AUP and SAS70 Frequently Asked Questions*
- *Shared Assessments – Getting Started: A Step by Step Guide to Integrating Shared Assessments into Your Vendor Management Program*

These and other papers are available for free download at:
http://sharedassessments.org/value/resources.html.

Shared Assessments Program Evolution

Technology, threats and regulations change. The Shared Assessments Program's revision process ensures the AUP evolves with industry risk management priorities and the regulatory environment.

All comments and suggestions for improving version 4.0 of the AUP were reviewed by the Shared Assessments Working Group and Technical Development Committee. Those contributions were then used to create Version 5.0.

All users of the Shared Assessments tools are encouraged to provide feedback, including suggesting modifications to the AUP document and SIG questionnaire, to the Technical Development Committee for consideration in subsequent versions of the tools. Forms may be submitted online at www.sharedassessments.org. *Please do not submit confidential or proprietary information in your feedback form.*

Learn More About Shared Assessments

The Shared Assessments website (www.sharedassessments.org) offers a wealth of information about the Shared Assessments tools, our global community of members, and Shared Assessments events. Visit us online to access free downloads of the Program tools and other documents, Shared Assessments FAQs, a member listing, and information about membership and licensing opportunities. To learn more about how your organization can benefit from Shared Assessments membership, please contact Michele Edson directly at michele@santa-fe-group.com.

A. Risk Management

Domain Objective:
Organizations should create and maintain a continuous process for IT and Infrastructure risk management to identify, quantify, and prioritize risks against defined risk acceptance levels and objectives relevant to the organization.

A.1 IT and Infrastructure Risk Governance

Objective:
An organization's risk management program should include a formal program which documents the organization's assets and threats and evaluates associated risks.

Control:
A formal risk governance program is implemented.

Procedure:

a. Obtain from the *service provider* the document(s) that are part of the risk assessment program.
b. Inspect the document(s) for evidence of the following *attributes*:
    1. Risk governance plan
    2. Risk policy and procedures
    3. Range of business assets to be evaluated
    4. Range of threats
    5. Risk scoping
    6. Risk context
    7. Risk training plan
    8. Risk scenarios
    9. Risk evaluation criteria
c. Report the *attributes* listed in step b not found in the risk program, the date of the last update, the business and technical owner of the risk program, or if the risk program documentation does not exist.

Industry Relevance:
ISO 27002: 4.1 Assessing Security Risks, 4.2 Treating Security Risks
SIG 5.0: A.1, A.1.2, A.1.2.2, A.1.2.3, A.1.2.4, A.1.2.5, A.1.2.6, A.1.2.7, A.1.2.8, A.1.2.9, A.1.2.10, A.1.3

A.2 IT and Infrastructure Risk Assessment Life Cycle

Objective:
An organization's risk management program should move beyond detailing the threats, vulnerabilities and assets to where it examines and evaluates risk within the context of the overall workings of the business and its environment.

Control:
A formal risk governance program is aligned with the business environment.

Procedure:

a. Using the risk management documents obtained in **A.1 IT and Infrastructure Risk Governance**, inspect the document for evidence of the following *attributes*:

Range of *Threats* includes:

1. Malicious
2. Natural
3. Accidental
4. Business changes (e.g., transaction volume)

Range of *Assets* includes:

1. People
2. Process (business or IT service management)
3. Information (physical and electronic)
4. Technology (applications, middleware, *servers*, storage, network)
5. Physical (buildings, energy)

Vulnerabilities Assessment:

1. Vulnerability assessment exists for each threat-asset combination

Dependency Analysis includes:

1. Business processes linked to IT processes
2. IT processes linked physical infrastructure

Scenario Analysis includes:

1. List of threat sources and assets impacted
2. For each threat-asset combination
3. Probability of threat occurring
4. Impact

Control determination exists for each risk:

1. Preventive
2. Detective
3. Corrective
4. Predictive

Formal designation exists for each risk:

1. Accept (in whole or managed to reduce)
2. Avoid
3. Transfer (fully or shared)
4. Insure

Risk Response process includes:

1. Assignment of ownership
2. Action plan
3. Status of response action items to closure
4. Status updates to management

**Denotes non-core procedure to be used when appropriate according to the industry verticals a service provider serves and/or the specific services offered.*

Risk Monitoring process includes:

1. Monitoring plan
2. Monitoring data reviewed by management
3. Action triggers where conditions are outside of defined controls

Risk Program process includes:

1. Feedback and update plan triggered by internal and external environment changes
2. Report if the risk management documents do not exist, if a list of the risks is not available, whether the *attributes* listed in step b are not found in the IT and Infrastructure Risk Governance and Context Program, and the date the threats and assets were last updated

Industry Relevance:
ISO 27002: 4.1 Assessing Security Risks, 4.2 Treating Security Risks
SIG 5.0: A.1.2.1, A.1.2.4.1, A.1.4, A.1.5, A.1.5.2, A.1.5.3, A.1.5.3.1, A.1.6, A.1.2.3.1

**Denotes non-core procedure to be used when appropriate according to the industry verticals a service provider serves and/or the specific services offered.*

B. Information Security Policy

Domain Objective:
Organizations should provide management direction and support for information security in accordance with business requirements and relevant laws and regulations. They should set a clear policy direction in line with business objectives and demonstrate support for, and commitment to, information security through the issue, acceptance and maintenance of an information *security policy* across the organization.

B.1 Information *Security Policy* Content

Objective:
An organization should establish a strong *security policy* that sets the security tone for the whole company. This security program should incorporate the key areas of security.

Control:
An information *security policy* is maintained which includes the key relevant domains of security.

Procedure:

a. Obtain from the *service provider* a copy of the most current, approved *security policy*.
b. Inspect the *security policy* for evidence of the following *attributes*:
    1. Policy maintenance
    2. Asset management, including information handling
    3. Human resources
    4. Physical and environmental security
    5. Communications and operations management
    6. Access control
    7. Information systems acquisition, development and maintenance, including vulnerability management
    8. Information security *incident* management
    9. Business continuity management
    10. Compliance with legal requirements
c. Report the *attributes* listed in step b not found in the *security policy.*

Industry Relevance:
ISO 27002: 5.1.1 Information *security policy* document
SIG 5.0: B.1.3, B.1.5, D.1.1, E.1, F.1.1, H.1.1, K.1.1

B.2 Information *Security Policy* Maintenance

Objective:
An organization should review the information *security policy* at planned intervals, at least annually (or if significant changes occur), to ensure its continuing suitability, adequacy, and effectiveness.

**Denotes non-core procedure to be used when appropriate according to the industry verticals a service provider serves and/or the specific services offered.*

Control:
An information *security policy* has been approved, reviewed within the last 12 months, and contains a revision history.

Procedure:
a. Using the information *security policy* obtained in **B.1 Information *Security Policy* Content,** inspect the document for evidence of the following *attributes:*
   1. Approval, including the most recent approver's title and date of approval
   2. Date of last review
   3. Revision history
b. Report approver's title, date of approval, date of last review and existence or nonexistence of a revision history.

Industry Relevance:
ISO 27002: 5.1.2 Review of Information *Security Policy*
SIG 5.0: B.1.1, B.1.6, B.1.7.2

B.3 Employee Acknowledgment of Acceptable Use

Objective:
An organization's acceptable use of information and assets should be identified, documented, and implemented. Additionally, employees of the organization should signify acceptance of the policy at least annually.

Control:
Employees signify their acceptance of the company's *acceptable use policy* at least annually.

Procedure:
a. Obtain a current *employee* list from the *service provider.*
b. Using the sampling parameters in Section Y, select a sample of employees.
c. For each sample item, obtain the *employee's* physical or electronic acknowledgment of the company's *acceptable use policy.*
d. Inspect the physical or electronic acknowledgment of the company's *acceptable use policy* for a date that is within the last 12 months from the date of testing.
e. Report the number of *employees* sampled, and number of employees who have not accepted the company's *acceptable use policy in the past 12 months.*

Industry Relevance:
ISO 27002: 6.1.1 Management commitment to information security, 7.1.3 Acceptable use of assets, 8.1.3 Terms and conditions of employment
SIG 5.0: B.2.2, E.3.2, E.3.8.2

**Denotes non-core procedure to be used when appropriate according to the industry verticals a service provider serves and/or the specific services offered.*

C. Organization of Information Security

Domain Objective:
Organizations should establish a management framework to control and manage the information security organization. This should include the protection of organizational information through the use of employee *confidentiality* agreements and the addition of clauses in dependent *service provider* contracts or agreements.

C.1 Employee Acceptance of *Confidentiality*

Objective:
An organization should communicate, get acknowledgement from, and periodically review employees' responsibility to protect confidential information. Employees must acknowledge this communication by signing a *confidentiality* agreement.

Control:
Employees acknowledge at least annually their obligation to maintain *confidentiality*.

Procedure:

a. Using the sampling parameters in Section Y, select a sample from the *employee* list obtained in **B.3 Employee Acknowledgment of Acceptable Use.**
b. For each sample item, obtain from the *service provider* the most recent physical or electronic acknowledgment of the individual's responsibility for maintaining the *confidentiality* of information and information assets.
c. Inspect the most recent physical or electronic acknowledgment for a signature evidencing that the employee has acknowledged his or her obligation to maintain *confidentiality.*
d. Report the number of employees sampled and the number of employees who have not accepted the *confidentiality* agreement in the past 12 months.

Industry Relevance:
ISO 27002: 6.1.1 Management commitment to information security, 6.1.5 *Confidentiality* agreements, 8.1.3 Terms and conditions of employment
SIG 5.0: E.3.5

C.2 Dependent *Service Provider* Agreements

Objective:
An organization should ensure that all agreements or contracts with the dependent *service provider* contain specific clauses to ensure *target data* is protected when accessed, processed or stored by a dependent *service provider*.

Control:
Dependent *service provider* agreements detail security requirements between the *service provider* and the dependent *service provider.*

**Denotes non-core procedure to be used when appropriate according to the industry verticals a service provider serves and/or the specific services offered.*

Procedure:

a. Obtain from the *service provider* a list of *dependent service providers* that handle *target data.*
b. Using the sampling parameters in Section Y, select a sample of *dependent service providers.*
c. For each sample item, obtain from the *service provider* the agreement in place for providing services.
d. Inspect each agreement for evidence of the following *attributes:*
    1. *Dependent service provider* acknowledgment of responsibility for the security of *target data*
    2. *Dependent service provider* acknowledgment of responsibility for the *confidentiality* of information and information assets
    3. Requirement to notify the *service provider* in the event of an information security *incident* affecting *target data*
e. Report the total number of *dependent service providers* with access to *target data,* the number of *dependent service providers* sampled, and the number of *dependent service providers* where the agreement does not address the *attributes* listed in step d.

Industry Relevance:

ISO 27002: 6.2.3 Addressing security in third party agreements
SIG 5.0: C.2.4.1

**Denotes non-core procedure to be used when appropriate according to the industry verticals a service provider serves and/or the specific services offered.*

D. Asset Management

Domain Objective:
Organizations should document and maintain a detailed list of hardware and software assets. These assets should include an organizational owner who is responsible for these assets.

D.1 Asset Accounting and *Inventory*

Objective:
An organization should ensure assets are clearly identified and an *inventory* of all assets documented and maintained.

Control:
An *inventory* of all assets is maintained with required information.

Procedure:

a. Obtain from the *service provider* a hardware and software *inventory* report for all *target systems.*
b. Using the sampling parameters in Section Y, select a sample of hardware items and a sample of software items.
c. For each sampled item of hardware, inspect the hardware *inventory* report for evidence of the following *attributes.*
    1. *Asset Control Tag*
    2. Physical location (e.g., room, building, city, state)
    3. *System owner*
    4. Operating system
    5. Environment (e.g., development, test, production)
    6. *Asset classification*
d. For each sampled item of software, inspect the software *inventory* report for evidence of the following *attributes.*
    1. Environment (e.g., development, test, production)
    2. Software version
e. Report the number of items sampled, and the hardware and software items included in the samples for which the *attributes* listed in step c and d were nonexistent, along with the names of the *attributes.*

Industry Relevance:
ISO 27002: 7.1.1 *Inventory* of Assets, 7.1.2 Ownership of assets, 7.2.2 Information labeling and handling
SIG 5.0: D.1.2, D.1.3

**Denotes non-core procedure to be used when appropriate according to the industry verticals a service provider serves and/or the specific services offered.*

E. Human Resources Security

Domain Objective:
Organizations should establish a formal Security Awareness program for all employees that makes the employees aware of security best practices, and requires that they attend formal security training at least once annually to ensure that they are aware of the latest policies and security threats.

E.1 Security Awareness Training Attendance

Objective:
An organization should provide security awareness training at least annually and maintain employee attendance reports. Training ensures that employees are aware of information security threats, as well as their responsibilities.

Control:
Security awareness training occurs at least annually and attendance reports for *employees* are maintained.

Procedure:

a. Using the sampling parameters in Section Y, select a sample from the *employee* list obtained in **B.3 Employee Acknowledgment of Acceptable Use.**
b. For each sample item, obtain from the *service provider* the most recent physical or electronic record evidencing the *employee's* completion of the company's security awareness training.
c. Inspect the most recent physical or electronic record for a signature evidencing that the *employee* has received security awareness training within the last year.
d. Report the number of *employees* sampled, the number of *employees* sampled where evidence of security training is greater than the last year, or where evidence of security training is nonexistent.

Industry Relevance:
ISO 27002: 8.2.2 Information security awareness, education, and training
SIG 5.0: E.4

E.2 Background Investigation Policy Content

Objective:
An organization should establish a strong background investigation policy that includes which background verification checks should be carried out in accordance with industry best practices and relevant laws and international restrictions.

Control:
Background investigation policy includes relevant industry security examination requirements.

Procedure:

a. Obtain from the *service provider* a copy of the current *background investigation policy*.

**Denotes non-core procedure to be used when appropriate according to the industry verticals a service provider serves and/or the specific services offered.*

b. Inspect the *background investigation policy* for evidence of the following *attributes*:
    1. Policy maintenance
    2. Name, address, and date of birth verification
    3. Official identification/SSN verification
    4. Employment verification
    5. Educational verification
    6. Credit check requirement
    7. Federal or State criminal record check
    8. Reference Checks
    9. Positive verification of individual against official photo ID
c. Report the *attributes* listed in step b not found in the *background investigation policy,* and if an attribute is nonexistent report the country to which it applies.

Industry Relevance:
ISO 27002: 8.1.2 Screening
SIG 5.0: E.2

**Denotes non-core procedure to be used when appropriate according to the industry verticals a service provider serves and/or the specific services offered.*

F. Physical and Environmental Security

Domain Objective:
Organizations should take appropriate steps to prevent unauthorized physical access, as well as accidental and intentional damage to the organizations' physical premises, systems and information. Organizations should also take appropriate steps to protect against environmental and systems malfunctions or failures.

F.1 Environmental Controls – Computing Hardware

Objective:
An organization should ensure that critical supporting utilities, such as climate control, fire suppressants and backup power supplies needed to support the business are in place.

Control:
Target data, target systems, and physical media are protected with environmental controls.

Procedure:

a. Using the sampling parameters in Section Y, select a sample of *hardware systems* from the *inventory of target systems* obtained in **D.1 Asset Accounting and *Inventory*.**
b. For each sample item, observe the *secure* and *general perimeter* for evidence of the following *attributes:*

Secure Perimeter:

1. *Climate control system*
2. Thermostat sensor
3. *Raised floor*
4. *Smoke detector*
5. *Heat detector*
6. *Fluid or water sensor*
7. *Fire suppression system*
8. *Uninterruptible Power Supply (UPS)*
9. *Battery*

General Perimeter:

1. *Climate control system*
2. Thermostat sensor
3. *Raised floor*
4. *Smoke detector*
5. *Heat detector*
6. *Fluid or water sensor*
7. *Fire suppression system*
8. *Uninterruptible Power Supply (UPS)*
9. *Battery*
10. *Generator*

**Denotes non-core procedure to be used when appropriate according to the industry verticals a service provider serves and/or the specific services offered.*

c. Report the number of *hardware systems* sampled and the number of sampled *hardware systems* where the *attributes* listed in step b were nonexistent.

Industry Relevance:
ISO 27002: 9.1.4 Protecting against external and environmental threats, 9.2.1 Equipment sitting and protection, 9.2.2 Supporting utilities
SIG 5.0: F.1.10.2.1, F.1.10.2.3, F.1.11, F.1.11.1.4, F.1.11.1.5, F.1.11.1.6, F.1.11.1.8, F.1.11.1.10, F.1.11.1.11, F.1.11.1.12, F.1.13, F.1.15.1.3, F.1.15.1.5, F.1.15.1.6, F.1.15.1.7, F.1.16.1.6, F.1.16.1.7, F.1.16.1.8, F.1.16.1.10, F.1.16.1.11, F.1.16.1.13, F.1.16.1.14, F.1.16.1.15, F.1.19.1.6, F.1.19.1.7, F.1.19.1.8, F.1.19.1.10, F.1.19.1.11, F.1.19.1.13, F.1.19.1.14, F.1.19.1.15, F.2, F.2.2.1, F.2.2.2, F.2.2.3, F.2.2.5, F.2.2.6, F.2.2.10, F.2.2.11, F.2.2.12, F.2.2.18, F.2.2.19

F.2 Physical Security Controls – Target Data

Objective:
An organization should ensure that physical access to data or systems is appropriately restricted by layered security controls and that only authorized personnel are allowed access to restricted areas.

Control:
Target data, target systems, and physical media are protected with physical security controls.

Procedure:
a. Using the sampling parameters in Section Y, select a sample of *hardware systems* from the *inventory of target systems* obtained in **D.1 Asset Accounting and *Inventory*.**
b. For each sample item, observe the *immediate, secure, general* and *external perimeter* for evidence of the following *attributes:*

Immediate Perimeter
1. Camera to monitor physical access to *immediate perimeter*
2. Badge, *biometric readers* or locked doors requiring a key or *PIN* on all points of entry
3. Access logs
4. Alarm system (motion or infrared or other detection mechanism for unauthorized entry)
5. Cage or walls that completely enclose the *immediate perimeter*

Secure Perimeter
1. Alarm system (motion, infrared or other detection mechanism for unauthorized entry)
2. Mounted camera at points of entry
3. *Anti-tailgating (anti-piggybacking)* mechanisms at each point 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
7. Access logs

**Denotes non-core procedure to be used when appropriate according to the industry verticals a service provider serves and/or the specific services offered.*

General Perimeter

1. Mounted camera at points of entry
2. *Anti-tailgating (anti-piggybacking)* mechanisms at each point 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, including roof access if applicable
5. Access logs

External Perimeter

1. Defined boundary or property line
2. Signage identifying the *facility* as a data center
3. Entry point(s)
   a) Mounted camera at each point of entry
   b) *Anti-tailgating (anti-piggybacking)* mechanisms at points of entry
   c) Security guards at each unlocked point of entry
   d) Badge or *biometric readers* or locked doors requiring a key or *PIN* on all points of entry
   e) Access logs

c. Report the number of *hardware systems* sampled and the number of sampled *hardware systems* where *attributes* listed in step b were nonexistent.

Industry Relevance:
ISO 27002: 9.1.1 Physical security perimeter, 9.1.2 Physical entry controls, 9.1.3 Securing offices, rooms, and facilities, 9.1.5 Working in secure areas, 9.1.6 Public access, delivery, and loading areas, 9.2.1 Equipment sitting and protection
SIG 5.0: F.1.4.1, F.1.4.3, F.1.9.7, F.1.9.15, F.1.9.16, F.1.9.18, F.1.9.20.1, F.1.9.20.2, F.1.9.20.3, F.1.9.21, F.1.9.22.4, F.1.10.2.5, F.1.10.2.6, F.1.10.3.2, F.1.11.1.3, F.1.11.1.14, F.1.11.2.1, F.1.11.2.3, F.1.11.2.5, F.1.13.5.1, F.1.13.5.3, F.1.13.5.5, F.1.13.6, F.1.14.1.1, F.1.14.1.3, F.1.14.1.5, F.1.15.1.2, F.1.15.2.1, F.1.15.2.3, F.1.15.2.5, F.1.16.1.2, F.1.16.1.3, F.1.16.1.4.1, F.1.16.1.5, F.1.16.2.1, F.1.16.2.3, F.1.16.2.5, F.1.17.1.3, F.1.17.1.4, F.1.17.2.1, F.1.17.2.3, F.1.17.2.5, F.1.18.1.2, F.1.18.1.3, F.1.18.1.4.1, F.1.18.2.1, F.1.18.2.3, F.1.18.2.5, F.1.19.1.2, F.1.19.1.3, F.1.19.1.4.1, F.1.19.1.5, F.1.19.2.1, F.1.19.2.3, F.1.19.2.5, F.2.2.20.1, F.2.2.20.5, F.2.2.21, F.2.2.22, F.2.2.24, F.2.2.24.1, F.2.2.24.2, F.2.2.26, F.2.2.27, F.2.3.1, F.2.3.1.2, F.2.3.5, F.2.4.2.2

F.3 Secure Workspace Security Program*

Objective:
An organization should ensure that protecting the *Secure Workspace* environment is part of the Security and Risk Management Program.

Control:
The controls in the *Secure Workspace* are commensurate with the risk and are part of the organization's security and risk management program.

**Denotes non-core procedure to be used when appropriate according to the industry verticals a service provider serves and/or the specific services offered.*

Procedure:

a. Obtain from the *service provider* the document(s) that are part of the *Secure Workspace* security and risk management program.
b. Inspect the program for evidence of the following *attributes*:
    1. Writing instruments
    2. Cell phones, PDAs or smartphones
    3. Cameras
    4. External storage devices
    5. Recording devices
    6. Printing privileges limited to persons with a role-based need to print
    7. *Internet* access limited for business
    8. Anti-spyware software
    9. Anti-malware software
    10. Personal *firewall*
    11. Automatic updates
    12. System access limited for business requirements
    13. Applications restricted to those required to perform work
    14. Administrative rights limited to persons with a role-based need
    15. Limited external email
    16. IM, VoIP and other external communications applications
    17. Peer-to-peer user networking
    18. Password-enabled screensavers with automatic logout of unattended *workstations*
    19. Secure disposal of *Target Data*
    20. Secure storage of *Target Data*
    21. Monitoring of traffic for anomalies
    22. Monitoring of systems for anomalies
    23. Security awareness completed at least annually by staff
    24. Process to escalate security issues
c. Report the *attributes* listed in step b not found in the, program documents, r, the names of the policies and documents where this information was found, and the date(s) of the last policy and procedure updates, or the nonexistence of a Secure Workspace or documents.

Industry Relevance:

ISO 27002: 5.1.1 Information security policy document
SIG 5.0: B.1.3, B.1.5, D.1.1, E.1, F.1.1, H.1.1, K.1.1

F.4 Secure Workspace Perimeter*

Objective:

An organization should control ingress and egress into the secure workspace. The level of controls should be commensurate with the level of risk.

Control:

Organizations should control ingress and egress into the secure workspace

**Denotes non-core procedure to be used when appropriate according to the industry verticals a service provider serves and/or the specific services offered.*

Procedure:

a. Observe the *Secure Workspace Perimeter* at the points of entry and exit for evidence of the following *attributes*:

1. Entry Points:
   a) Mounted camera
   b) *Anti-tailgating (anti-piggybacking)* mechanisms
   c) Security guards
   d) Locked door
   e) Badge, *biometric reader*, key or PIN required for access
   f) Walls that completely enclose the *Secure Workspace*
   g) Physical inspection of bags upon entrance

2. Exit Points:
   a) Mounted camera
   b) *Anti-tailgating (anti-piggybacking)* mechanisms
   c) Security guards
   d) Badge, or PIN required for exit
   e) Exit log (physical or electronic)
   f) Walls that completely enclose the *Secure Workspace*
   g) Physical inspection of bags upon exit

3. Emergency Exit Points:
   a) Mounted camera
   b) Signage identifying alarm (signage)
   c) Locked to prevent access from outside in
   d) Walls that completely enclose the *Secure Workspace*

b. Report the *attributes* listed in step a as present or absent for each point of entry and exit as defined in the *Secure Workplace* Perimeter.

Industry Relevance:

ISO 27002: 9.1.1 Physical security perimeter, 9.1.2 Physical entry controls, 9.1.3 Securing offices, rooms, and facilities, 9.1.5 Working in secure areas, 9.1.6 Public access, delivery, and loading areas, 9.2.1 Equipment sitting and protection

SIG 5.0: F.1.4.1, F.1.4.3, F.1.9.7, F.1.9.15, F.1.9.16, F.1.9.18, F.1.9.20.1, F.1.9.20.2, F.1.9.20.3, F.1.9.21, F.1.9.22.4, F.1.10.2.5, F.1.10.2.6, F.1.10.3.2, F.1.11.1.3, F.1.11.1.14, F.1.11.2.1, F.1.11.2.3, F.1.11.2.5, F.1.13.5.1, F.1.13.5.3, F.1.13.5.5, F.1.13.6, F.1.14.1.1, F.1.14.1.3, F.1.14.1.5, F.1.15.1.2, F.1.15.2.1, F.1.15.2.3, F.1.15.2.5, F.1.16.1.2, F.1.16.1.3, F.1.16.1.4.1, F.1.16.1.5, F.1.16.2.1, F.1.16.2.3, F.1.16.2.5, F.1.17.1.3, F.1.17.1.4, F.1.17.2.1, F.1.17.2.3, F.1.17.2.5, F.1.18.1.2, F.1.18.1.3, F.1.18.1.4.1, F.1.18.2.1, F.1.18.2.3, F.1.18.2.5, F.1.19.1.2, F.1.19.1.3, F.1.19.1.4.1, F.1.19.1.5, F.1.19.2.1, F.1.19.2.3, F.1.19.2.5, F.2.2.20.1, F.2.2.20.5, F.2.2.21, F.2.2.22, F.2.2.24, F.2.2.24.1, F.2.2.24.2, F.2.2.26, F.2.2.27, F.2.3.1, F.2.3.1.2, F.2.3.5, F.2.4.2.2

**Denotes non-core procedure to be used when appropriate according to the industry verticals a service provider serves and/or the specific services offered.*

F.5 Secure Workspace Access Reporting*

Objective:
An organization should maintain access and incident reports.

Control:
Access to *Secure Workplace* is logged and incident reports are maintained.

Procedure:

a. Obtain the access and incident logs (physical or electronic) from the *service provider* for the *Secure Workspace Perimeter*, and inspect for evidence of the following *attributes*:

Access Logs (Staff):
1. Name
2. Date and time
3. Point of access
4. Date of last update

Access Logs (Visitor):
1. Name
2. Date and time
3. Point of access
4. Company name
5. Visiting
6. Equipment
7. Sign out and return of badge
8. Date of last update

Incident Logs:
1. Name
2. Date and time
3. Company name
4. Incident type
5. Date of last update

b. Report the attributes listed in step a not in evidence, the date the access logs and incident log was last updated, or the nonexistence of the access log or incident log.

Industry Relevance:
ISO 27002**:** 9.1.1 Physical security perimeter, 9.1.2 Physical entry controls, 9.1.3 Securing offices, rooms, and facilities, 9.1.5 Working in secure areas, 9.1.6 Public access, delivery, and loading areas, 9.2.1 Equipment sitting and protection
10.10.1 Audit Logging, 10.10.4 Administrator and operator logs
SIG 5.0: G.14.1.25, G.15.1.20, G.16.1.25, G.17.1.22, G.18.1.21

**Denotes non-core procedure to be used when appropriate according to the industry verticals a service provider serves and/or the specific services offered.*

F.6 Secure Workspace Compliance Audits*

Objective:
An organization should complete periodic compliance audits of the Secure Workspace desktop environment.

Control:
Periodic compliance audits of the *Secure Workspace* environment are conducted.

Procedure:

a. Obtain from the *service provider* a copy of the *audit program* which encompasses the *Secure Workspace,* and the resulting *audit reports.*
b. Inspect the *audit program documentation* and resulting *audit reports f*or evidence of the following *attributes:*

Audit Program:

1. Requirement to audit the *Secure Workspace* environment
2. Role(s) responsible for audits
3. Audit reports created and maintained
4. Remediation action required on audit findings
5. Frequency of audits
6. Audit results are reviewed as part of the organizations security and risk management program
7. Audit against a list of compliance checks which includes:
   a) Clean desk review
   b) External storage devices
   c) Cell phones, PDAs or Smartphones
   d) Cameras
   e) Screen lock on unattended desktops
   f) *Target Data* in common areas
   g) *Target Data* on or near printers

Audit Logs:

1. Title of auditor
2. Date of audit
3. Audit notes or findings

c. Report the *attributes* listed in step b not found in the *audit program* and *logs*, the title of the auditor, the frequency of the audits, the date of the last audit, of if the *Secure Workspace* audit program or logs do not exist

Industry Relevance:
ISO 27002: 5.1.1 Information security policy document, 6.1.2 Information security co-ordination, 6.1.8 Independent review of information security, 10.10.1 Audit logging, 15.2.1 Compliance with security policies and standards, 15.2.2 Technical compliance checking, 15.3 Information systems audit considerations
SIG 5.0: L.8, L.8.3, L.9.2, L.10, L.11, L.12

**Denotes non-core procedure to be used when appropriate according to the industry verticals a service provider serves and/or the specific services offered.*

G. Communications and Operations Management

Domain Objective:
Organizations should maintain documented operating procedures and technological controls to ensure the effective management, operation, integrity and security of their information systems and data.

G.1 Network Security – IDS/IPS Signature Updates

Objective:
An organization should ensure that IDS/IPS systems have the latest signatures applied in order to effectively monitor for the most recent threats and vulnerabilities.

Control:
Signatures are up to date on *Network Intrusion Detection Systems (IDS)/Intrusion Prevention Sensors (IPS)).*

Procedure:

a. Using the sampling parameters in Section Y, select a sample of *IDS/IPS sensors* from the *inventory* of *target systems* obtained in obtained in **D.1 Asset Accounting and *Inventory*.**
b. For each sample item, obtain from the *service provider* a list of the five most recently released signatures, or rules, from the vendor website.
c. Obtain from the *service provider* a report or screen shot of the signatures, or rules, resident on each selected *IDS/IPS sensor.*
d. Compare the list obtained in step b with the report or screen shot obtained in step c.
e. Report the number of *IDS/IPS sensors* sampled, and the number of *IDS/IPS sensors* where the list obtained in step did not agree with the report or screen shot obtained in step c.

Industry Relevance:
ISO 27002: 10.4.1 Controls against Malicious Code, 10.6.1 Network controls
SIG 5.0: G.9.21.1.3, G.9.21.2.3

G.2 Network Management – Encrypted Authentication Credentials

Objective:
An organization should protect credentials as they travel throughout the network. To prevent possible exposure of credentials, an organization should ensure that network devices have encryption enabled for network authentication.

Control:
Authentication credentials transmitted to *network devices* are encrypted in transit.

Procedure:

a. Using the sampling parameters in Section Y, select a sample of *network devices* from the *inventory of target systems* obtained in **D.1 Asset Accounting and *Inventory*.**

**Denotes non-core procedure to be used when appropriate according to the industry verticals a service provider serves and/or the specific services offered.*

b. For each sample item, execute the prescribed commands and obtain the authentication parameters using the Practitioners' Notes in Section Z.
c. Report the number of devices sampled, and the devices that use either HTTP or Telnet as an authentication method.

Industry Relevance:
ISO 27002: 10.6.1 Network controls, 10.6.2 Security of network services, 11.4.1 Policy on use of network services
SIG 5.0: G.9.17

G.3 *Externally Facing* Open Administrative Ports

Objective:
An organization should manage open ports accessible from the *Internet* that are not specifically required for business functionality. These should be disabled or removed to decrease the likelihood of being exploited. This is particularly relevant for administrative ports that can be used to remotely manage a system.

Control:
High-risk administrative ports on *externally facing target systems* are not accessible from the *Internet*.

Procedure:
a. Using the sampling parameters in Section Y, select a sample of *externally facing* systems from the *inventory of target systems* obtained in **D.1 Asset Accounting and *Inventory*.**
b. For each sample item, obtain from the *service provider* the *IP* addresses that correspond to the selected systems.
c. For each sample item, obtain from the *service provider* a *port scan* report for the selected systems generated within the past thirty days that shows the open ports between 0 - 1024.
d. For each sample item, compare the *IP* addresses obtained in step b to the *port scan* report obtained in step c.
e. Report the number of *externally facing* systems sampled, and whether SSH, telnet, RDP or VNC access is listed as open in the *port scan*.

Industry Relevance:
ISO 27002: 10.6.1 Network controls, 10.6.2 Security of network services, 11.4.4 Remote Diagnostic and Configuration Port Protection
SIG 5.0: G.9.18, G.9.19.4

G.4 Network Logging

Objective:
An organization should comply with relevant security best practices for the monitoring and logging activities of its networks, and should ensure that appropriate logging and monitoring should be applied to enable recording of relevant actions

**Denotes non-core procedure to be used when appropriate according to the industry verticals a service provider serves and/or the specific services offered.*

Control:
Network connections are logged and the log files are retained for examination

Procedure:

a. Using the sampling parameters in Section Y, select a sample of *network devices* from the *inventory of target systems* obtained in **D.1 Asset Accounting and *Inventory*.**
b. For each sample item, obtain logs using the Practitioners' Notes in Section Z and observe whether logs are available for the two date ranges defined: one within 30 days and the second between 30 to 60 days.
c. For both date ranges, inspect the logs for the evidence of the following *attributes.*
    1. Source *IP*
    2. Destination *IP*
    3. Destination port
    4. *Protocol* type (e.g., TCP, UDP, ICMP)
    5. Timestamp
d. Report the number of *network devices* sampled, the absence of any of the *attributes* listed in step c, or the number of sampled devices where the logs are not available for one or both of the time periods in step b.

Industry Relevance:
ISO 27002: 10.6.1 Network Controls, 10.10.1 Audit logging
SIG 5.0: G.9.7, G.9.7.1

G.5 Virus Protection (*Servers*)

Objective:
An organization should ensure virus protection software is deployed on target *servers*, and that these have the latest signatures applied.

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

Procedure:

a. Using the sampling parameters in Section Y, select a sample of Mac OS and Windows *servers* from the *inventory of target systems* obtained in **D.1 Asset Accounting and *Inventory*.**
b. For each sample item, obtain from the *service provider* the current antivirus software report.
c. Using the antivirus vendor's website, obtain the dates of the latest available signature files for each virus protection product sampled in step b.
d. For each sample item, compare the antivirus software report obtained in step b to the vendor's latest available signature obtained in step c.
e. Report the number of *servers* and the operating system sampled, the number of *servers* from step d where the latest virus definitions were not installed, or the number of *servers* that do not have antivirus software installed.

**Denotes non-core procedure to be used when appropriate according to the industry verticals a service provider serves and/or the specific services offered.*

Industry Relevance:
ISO 27002: 10.4.1 Controls against malicious code, 10.4.2 Controls against *mobile code*
SIG 5.0: G.7.2.3

G.6 Virus Protection (*Workstations*)

Objective:
An organization should ensure virus protection software is deployed on *workstations* which access target systems, and that these have the latest signatures applied.

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

Procedure:

a. Using the sampling parameters in Section Y, select a sample of Mac OS and Windows *workstations* from the *inventory of target systems* obtained in **D.1 Asset Accounting and *Inventory*.**
b. For each sample item, obtain a current antivirus software report.
c. Using the antivirus vendor's website, obtain the dates of the latest available signature files for each antivirus product sampled in step b.
d. For each sample item, compare the antivirus software report obtained in step b to the vendor's latest available signature obtained in step c.
e. Report the number of *workstations,* the operating system of each *workstation* sampled, the number of *workstations* from step d where the latest virus definitions were not installed, or the number of *workstations* that do not have antivirus software installed.

Industry Relevance:
ISO 27002: 10.4.1 Controls against malicious code, 10.4.2 Controls against *mobile code*
SIG 5.0: G.7.2.1

G.7 Administrative Activity Logging

Objective:
An organization should comply with all relevant security requirements applicable to its monitoring and logging activities, and should ensure that appropriate logging and monitoring is in place to capture administrative activity for accountability and audit purposes.

Control:
Systems and network logging is enabled and system audit log files are retained.

Procedure:

a. Using the sampling parameters in Section Y, select a sample of systems from the *inventory of target systems* obtained in **D.1 Asset Accounting and *Inventory*.** In selecting the sample, select one of each type of operating system in use for *workstations, servers* and *network devices.*
b. For each sample item, based on the *service provider* policies, either create a test user account or obtain a user account that has been created in the last 12 months.

**Denotes non-core procedure to be used when appropriate according to the industry verticals a service provider serves and/or the specific services offered.*

c. Using the Practitioners' Notes in Section Z, inspect the log for each system for evidence of the following *attributes:*
    1. Event identifier
    2. Timestamp
    3. Creator's account name
    4. Account created
d. Report the number of systems sampled, the type of system, the absence of *attributes* listed in step c, and the number of systems where audit logs are nonexistent.

Industry Relevance:
ISO 27002: 10.10.1 Audit Logging, 10.10.2 Monitoring system use, 10.10.4 Administrator and operator logs
SIG 5.0: G.14.1.25, G.15.1.20, G.16.1.25, G.17.1.22, G.18.1.21

G.8 Log-On Activity Logging

Objective:
An organization should ensure that log-on attempts are captured and stored for accountability and audits requirements.

Control:
Key log *attributes* are logged and reported in the system audit log files.

Procedure:
a. Using the user account and sample systems selected in **G.7 Administrative Activity Logging** and the sampling parameters in Section Y, attempt to log on, both successfully and unsuccessfully, to each system.
b. For each sample item, obtain from the *service provider* the system audit log files using the Practitioners' Notes in Section Z.
c. Inspect the logs obtained in step b for evidence of the following *attributes* for each log-on attempt generated in steps a:
    1. User Account
    2. Timestamp
    3. Terminal identity or location and compare the time of the attempt in step a. with the timestamp of the log entry Report the number of systems sampled, the nonexistence of *attributes* listed in step c, and/or if the compared timestamps do not match, or the number of systems where audit logs are nonexistent.

Industry Relevance:
ISO 27002: 10.10.1 Audit Logging, 10.10.2 Monitoring system use, 10.10.4 Administrator and operator logs
SIG 5.0: G.14.1.25, G.15.1.20, G.16.1.25, G.17.1.22, G.18.1.21

**Denotes non-core procedure to be used when appropriate according to the industry verticals a service provider serves and/or the specific services offered.*

G.9 Log Retention

Objective:
An organization should ensure that system and network logs are retained for a sufficient period of time to allow for the successful auditing of historical events, to meet legal requirements, and also, if needed, for forensic purposes.

Control:
Audit logs are retained for the required duration.

Procedure:
a. Using the sampling parameters in Section Y, select a sample of systems from the *inventory of target systems* obtained in **D.1 Asset Accounting and *Inventory*.** In selecting the sample, select one of each type of operating system in use for *workstations, servers* and *network devices*.
b. For each sample item, obtain from the *service provider* the audit logs, using the Practitioners' Notes in Section Z, and observe whether the audit log files are available for each of the following day ranges: 1 to 30, 31 to 60, and 61 to 90.
c. Observe whether each audit log obtained in step b contains log entries for all date ranges.
d. Report the number of systems sampled, the number of systems where audit logs are nonexistent or if the audit logs do not contain entries, and the day ranges of the selected log files that are not available.

Industry Relevance:
ISO 27002: 10.10.1 Audit logging, 10.10.3 Protection of Log Information
SIG 5.0: G.14.1.26, G.15.1.21, G.16.1.26, G.17.1.23, G.18.1.22

G.10 Website Privacy Policy

Objective:
An organization should have a *Privacy Policy* developed, published, and clearly communicated. This policy should be accessible to all end users who access the organization's *Internet*-facing end-user websites that have access to *target data*.

Control:
Privacy Policy exists on *Internet*-facing websites from the point where end users access *target data*.

Procedure:
a. Using the sampling parameters in Section Y, select a sample of *Internet*-facing, *publicly accessible* end-user websites where *target data* is accessible from the *inventory of target systems* obtained in **D.1 Asset Accounting and *Inventory*.**
b. For each sample item, access each selected website via a web browser.
c. Observe whether a link to the *Privacy Policy* exists.
d. Report the number of websites sampled, the sites that do not provide a link to the *Privacy Policy* and the number of websites that do not have a privacy statement.

**Denotes non-core procedure to be used when appropriate according to the industry verticals a service provider serves and/or the specific services offered.*

Industry Relevance:
ISO 27002: 10.9.2 On-Line Transactions, 15.1.4 Data Protection and Privacy of Personal Information
SIG 5.0: L.6.2

G.11 Website – Client Encryption

Objective:
An organization should ensure that sensitive information sent through on-line transactions remains confidential and protected from unauthorized disclosure as well as message alteration while in transit through the *Internet*.

Control:
SSL authentication and encryption is enabled

Procedure:
a. Using the sampling parameters in Section Y, select a sample of *Internet*-facing, *publicly accessible* end-user websites where *target data* is accessible from the *inventory of target systems* obtained in **D.1 Asset Accounting and *Inventory*.**
b. For each sample item, access each website using the Practitioners' Notes in Section Z and observe whether *SSL* is enabled.
c. Report the number of websites sampled, the digital certificate issuer, and the number of websites that did not have *SSL* enabled or where the certificate has expired.

Industry Relevance:
ISO 27002: 10.9.1 Electronic Commerce, 10.9.2 On-Line Transactions
SIG 5.0: G.19.1.1

G.12 Email Relaying

Objective:
An organization should ensure that sufficient steps are taken to secure privileged access and prevent misuse of the company's email resources.

Control:
Email relaying is disabled.

Procedure:
a. Using the *inventory of target systems* obtained in **D.1 Asset Accounting and *Inventory*,** select all *SMTP servers.*
b. Telnet (without authenticating) into each *SMTP* port and attempt to send a message.
c. Observe whether the message failed. (A "250 OK" reply from DATA command means attempt to send message was successful.)
d. Report the number of *SMTP servers* selected and the number of instances where email relaying is enabled.

**Denotes non-core procedure to be used when appropriate according to the industry verticals a service provider serves and/or the specific services offered.*

Industry Relevance:
ISO 27002: 10.8.4 Electronic messaging
SIG 5.0: G.13.4.4

G.13 *Physical Media* Tracking

Objective:
An organization should ensure that effective processes and procedures are in place for the destruction of media. Processes and procedures should be in place for the handling, storage and transport of external media to protect *target data* from unauthorized access and/or disclosure. Sensitive information can also be obtained from media that is not properly destroyed.

Control:
Tracking is in place for *physical media* used for transporting *target data* from *pre-shipment* until *destruction*.

Procedure:

Pre-shipment

a. Through inquiry with the *service provider,* select one media shipment scheduled to be made during the testing period.
b. From step a above, randomly 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. Labeled with a unique *tracking* identifier
    2. Company name or data classification does not appear on the outside of the container
    3. 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 a log shows which media are packaged within the sealed container.
c. Report the absence of *attributes* listed in step b, or the absence of the identified media.

Outbound Shipments

a. Obtain from the *service provider* the log used for tracking outbound media shipments.
b. Using the sampling parameters in Section Y, select a sample of shipments made during the past 90 days from the log obtained in step a.
c. For each sample item, inspect the shipment log for evidence 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 or barcode track of the individual making the pickup
    4. Destination of the shipment
    5. Delivery confirmation report from the end recipient
d. Report the number of shipments sampled, the absence of *attributes* listed in step c, or the absence of shipping logs.

Inbound Shipments

a. Obtain from the *service provider* the log used for tracking inbound media shipments.

b. Using the sampling parameters in Section Y, select a sample of shipments received during the past 90 days.
c. For each sample item, inspect the log for evidence of the following *attributes:*
    1. Tracking identifier of the media or container received
    2. Date the shipment was received
    3. Signature or barcode track and name, and job title of the individual confirming receipt
    4. Source of the shipment
    5. End destination of *physical media* following receipt
d. Report the number of shipments sampled, the absence of *attributes* listed in step c, or the absence of shipping logs.

Internal Tracking

a. Obtain from the *service provider* the log used for tracking inbound media shipments.
b. Using the sampling parameters in Section Y, select a sample of shipments containing *target data* that were received by the assessed *facility* within the last 90 days from the log obtained in step a.
c. For each sample item, obtain and inspect the documentation received from the *service provider* that identifies the current location of the media and a continuous chain of custody between initial receipt of the media and its current location.
d. Observe whether the location documented as the current location in step c is accurate.
e. Report the number of media sampled, the number of sample items that are not in their current location per step d, or any media not found in step d.

Destruction

a. Obtain the log used for tracking destruction of media containing *target data*.
b. Using the sampling parameters in Section Y, select a sample of destroyed media containing *target data* that was destroyed within the past 12 months from the log obtained in step a.
c. For each sample item, inspect the log obtained in step a for evidence of the following *attributes:*
    1. Tracking identifier of the media destroyed
    2. Date of destruction
    3. For media destroyed in-house, the name and title of the person confirming destruction
d. For media destroyed by a third party included in the sample selected in step b, 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 in step c above.
e. Report the number of destruction events sampled, the absence of *attributes* listed in step c, or the absence of the destruction logs. If a third party is used for destruction, report the absence of a media destruction certificate.

Industry Relevance:

ISO 27002: 10.5.1 Information back-up, 10.7.1 Management of removable media, 10.7.2 Disposal of media, 10.7.3 Information handling procedures, 10.8.3 *Physical media* in transit, 7.2.2, Information Labeling and Handling
SIG 5.0: D.2.2, D.2.3

**Denotes non-core procedure to be used when appropriate according to the industry verticals a service provider serves and/or the specific services offered.*

G.14 Security of Media in Transit

Objective:
An organization should have processes and procedures in place for the transport of media to protect the information from unauthorized access and/or disclosure.

Control:
Backup media containing *target data* from *target systems* is transported off-site in a lockbox.

Procedure:
a. Obtain from the *service provider* a copy of the backup media off-site pickup and delivery schedule.
b. Using the sampling parameters in Section Y, select a sample of backup media containing *target data* from the *target systems* from the schedule obtained in step a.
c. Using the sample selected, obtain from the *service provider* and inspect the pickup and delivery records for evidence of the following *attributes.*
    1. Pickup and delivery date
    2. Lock box identifier
d. Report the number of backup media selected, if the record does not include any of the *attributes* listed in step c, the media type, the name of the company that transports the media, or where there is no record of the schedule.

Industry Relevance:
ISO 27002: 10.7.1 Management of removable media, 10.7.3 Information handling procedures, 10.8.3 *Physical media* in transit, 7.2.2 Information labeling and handling
SIG 5.0: D.2.2.1.6

G.15 *Unapproved* Wireless Networks

Objective:
An organization should have all network connections and devices adequately tracked, managed and controlled to protect against threats and to maintain security for the systems and applications using the network.

Control:
Only prior approved wireless access points are present on the network.

Procedure:
a. Obtain from the *service provider* the following:
    1. The process document the *service provider* uses to locate, scan for or detect *unapproved* wireless access points
    2. Documentation indicating the last time the process was executed
    3. A list of approved wireless access points
    4. A list of all known wireless access points visible from the *facility,* but not associated with the organization
b. *War walk* the *facility* with a wireless scanning tool to observe any wireless access points and document their respective Service Set Identifiers *(SSIDs)*.

**Denotes non-core procedure to be used when appropriate according to the industry verticals a service provider serves and/or the specific services offered.*

c. Remove the wireless access points identified in step a3 and a4 from the list of access points in step b.
d. If access points remain after step c, randomly select up to three wireless access points from the list.
e. Using a wireless scanning tool, attempt to determine the location of the access points sampled in step d.
f. If the documentation in steps a1 and a2 was not available, report the date of last execution in a2, the number of wireless access points remaining in step d, the number of wireless access points sampled in step d, the wireless access points that were able to be located in step e, and whether they were connected to the *service provider's* network or a third party, and the number of wireless access points in step e whose location could not be determined, along with the reason.

Industry Relevance:
ISO 27002: 10.6.1 Network Controls, 10.6.2 Security of network services, 10.8.1 Information exchange policies and procedures
SIG 5.0: G.10

G.16 Wireless Networks Encryption

Objective:
An organization should ensure that wireless encryption for authorized wireless access points is implemented to protect from threats, and to maintain security for the systems and applications using the network.

Control:
Encryption and authentication are required prior to connecting to internal wireless access points.

Procedure:
a. Using the sampling parameters in Section Y, select a sample of wireless access points from the list of approved wireless points obtained in **G.15 *Unapproved* Wireless Networks.**
b. For each sample item, connect to the access point using the Practitioners' Notes in Section Z.
c. Report the number of wireless access points sampled and the number of wireless access points where authentication is not required and/or encryption is nonexistent.

Industry Relevance:
ISO 27002: 10.6.1 Network Controls, 10.6.2 Security of network services, 10.8.1 Information exchange policies and procedures
SIG 5.0: G.10.8

G.17 Network Security – *Firewall*(s)

Objective:
Networks should be segregated to ensure systems and applications are protected from threats outside of their connected network. This should include utilizing *firewalls* to segment and protect

the organization's internal network from the *Internet*, and also from other less restricted internal networks.

Control:
Firewall(s) protect and are inspecting traffic between defined network zones that posses different levels of trust.

Procedure:
a. Obtain the source and destination *IP* address ranges for the location of *target systems* (True or *NAT*'d *IP*) for the following scenarios:
   1. Source *IP* on the *Internet* or third party to *DMZ IP* address ranges
   2. *DMZ IP* address ranges to internal *IP* ranges
   3. Wireless *IP* address ranges to internal *IP* address ranges
b. Obtain from the *service provider* a list of frequently recurring network connections for each of the scenarios in step a, and randomly select one that contains a single source and destination *IP* address (True or *NAT*'d *IP*) for each of the above scenarios.
c. For the network connection selected in step b, obtain from the *service provider* the logical location of the *firewall* that protects the network connection.
d. Log into the *firewall*(s) identified in step c and filter the logs using the Practitioners' Notes in Section Z for a period within the last 30 days.
e. Observe whether the logs contain the network connection details for each of the scenarios listed in step a.
f. Report the network connections selected in step b and whether the network connections selected in step b can be found in the *firewall*(s) obtained in step c for each of the scenarios in step a. Also report where only a single *firewall* is used to protect more than one of the scenarios in step a and the scenarios to which it applies.

Industry Relevance:
ISO 27002: 10.6.1 Network controls, 10.6.2 Security of network services, 11.4.5 Segregation in Networks
SIG 5.0: G.9.2, G.9.3, G.9.13

G.18 Network Security – Authorized Network Traffic

Objective:
An organization should ensure strong rules are implemented by ensuring that each network service that is permitted has been formally approved and authorized.

Control:
Network rules are authorized.

Procedure:
a. Obtain from the *service provider* the approved network services list from G.3 *Externally Facing* open ports.
b. For the *firewall* selected in **G.17 Network Security – *Firewalls*,** compare the *firewall rules* found with the list obtained in step a using the Practitioners' Notes in Section Z.

**Denotes non-core procedure to be used when appropriate according to the industry verticals a service provider serves and/or the specific services offered.*

c. Report the number of network services reviewed and the number of network services found in step b that do not match the list obtained in step a, or if an approved network services list is nonexistent.

Industry Relevance:
ISO 27002: 10.6.1 Network controls, 10.6.2 Security of Network Services, 10.8.1 Information exchange policies and procedures
SIG 5.0: G.9.11

G.19 Network Security – IDS/IPS *Attributes*

Objective:
An organization should ensure that *IDS/IPS* systems have been deployed, that the alerts contain sufficient information to evaluate a potential *incident*, and that they are generating active alerts.

Control:
IDS/IPS alert events contain required security information.

Procedure:
a. Using the report of the *inventory of target systems* obtained in **D.1 Asset Accounting and *Inventory*,** randomly select one *IDS/IPS sensor.*
b. Using the sampling parameters in Section Y, select a sample of *IDS/IPS* alerts generated in the last 90 days from the sample item selected in step a.
c. Inspect the alert event for evidence of the following *attributes:*
    1. Unique identifier
    2. Date
    3. Time
    4. Priority level identifier
    5. Source *IP* address
    6. Destination *IP* address
    7. Event description
    8. Notification sent to security team
    9. Event status
d. Report the number of alerts sampled, the absence of *attributes* listed in step c, or if alerts were nonexistent.

Industry Relevance:
ISO 27002: 10.4.1 Controls against Malicious Code, 10.6.1 Network controls, 10.10.1 Audit logging, 10.10.2
Monitoring system use, 10.10.3 Protection of log information
SIG 5.0: G.9.21

**Denotes non-core procedure to be used when appropriate according to the industry verticals a service provider serves and/or the specific services offered.*

G.20 Backup Media Restoration

Objective:
An organization should have systems, applications and data available in the event of a disaster. Backups of these systems and data should be available, and they should contain valid information.

Control:
Backups occur and are restored successfully.

Procedure:
a. Obtain from the *service provider* a list of backup media generated within the last six months, excluding mainframe data. See Practitioners' Notes in Section Z.
b. From the list in step a, randomly select one item of media on-site.
c. For the sample item in step b, randomly select a single readable file, such as a text file, document or spreadsheet, which is greater than 0k in size.
d. Restore the selected file.
e. Report if the file could not be restored, or if the contents of the file were corrupt.

Industry Relevance:
ISO 27002: 10.1.1 Documented operating procedures, 10.5.1 Information back-up, 10.7.1 Management of removable media
SIG 5.0: G.8.5

G.21 Change Control

Objective:
An organization should ensure that changes are made within a formal change control program.

Control:
Formal change request process is in place and change requests are documented, tested, and approved prior to implementation.

Procedure:
a. Obtain the most recent copy of the *master change log* for all *target systems* for the past six months.
b. Using the sampling parameters in Section Y, select a sample of changes from the *master change log* obtained in step a. In selecting the sample, ensure it contains the following types of changes: application, operating system and network infrastructure, including *firewalls.*
c. For the sample items, obtain from the *service provider* the detailed change request and supporting documentation.
d. Inspect the change request and supporting documentation obtained in step c for evidence of the following *attributes:*
    1. Clearly identified roles and responsibilities
    2. Impact or risk analysis of the change request
    3. Testing prior to implementation of change

**Denotes non-core procedure to be used when appropriate according to the industry verticals a service provider serves and/or the specific services offered.*

4. Authorization and approval
5. Post-installation validation
6. Backout or recovery plans

e. Report the number of change requests sampled, the type of change (application, operating system and/or network device) and the presence of the *attributes* listed in step d, or if a change request log was nonexistent.

Industry Relevance:
ISO 27002: 10.1.1 Documented operating procedures, 10.1.2 Change Management, 12.4.1 Control of operational software, 12.5.1 Change control procedures, 12.5.2 Technical review of applications after operating system changes, 12.5.3 Restrictions on changes to software packages
SIG 5.0: G.2

**Denotes non-core procedure to be used when appropriate according to the industry verticals a service provider serves and/or the specific services offered.*

H. Access Control

Domain Objective:
Organizations should ensure sufficient control over access to information, including controlled access to *target data* and information processing systems and facilities. These controls should be based on security and business requirements, and should follow both industry best practices and internal policies.

H.1 Password Controls

Objective:
An organization should ensure that its password controls meet industry best practices and follow internal policies.

Control:
Password security settings on each system are implemented.

Procedure:

a. Using the sampling parameters in Section Y, select a sample of systems from the *inventory of target systems* obtained in **D.1 Asset Accounting and *Inventory*.** In selecting the sample, select one of each type of operating system in use for *workstations, servers* and *network devices.*
b. Use one of the following techniques to perform procedure c below:
    1. Request creation of test accounts on the systems selected in step a.
    2. Use an existing account.
c. For each sample item, observe the following password settings using the Practitioners' Notes in Section Z and report accordingly.
    1. Forced or initial password change – Log on successfully to each system sampled. Report the number of systems sampled, and which of those do not require the user to change the password for each operating system.
    2. Minimum password length – Observe the minimum password length from the configuration file, and attempt to change the password to one character less than the minimum password length. Report the number of systems sampled and number of instances per operating system where this change is 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 (~`!@#$%^&*()-+=\|]}[{'";:/?.>,<).
d. Report the number of systems sampled and number of instances per operating system where this change is permitted.

Industry Relevance:
ISO 27002: 11.3.1 Password use, 11.5.1 Secure log-on procedures, 11.5.3 Password management system
SIG 5.0: G.9.1.1.2, G.14.1.31, G.14.1.32, G.14.1.36, G.15.1.26, G.15.1.27, G.15.1.31, G.16.1.31, G.16.1.32, G.16.1.36, G.17.1.28, G.17.1.29, G.17.1.33, G.18.1.29, G.18.1.30, G.18.1.34, H.3.6, H.3.12.5

**Denotes non-core procedure to be used when appropriate according to the industry verticals a service provider serves and/or the specific services offered.*

H.2 Revoke System Access

Objective:
An organization should review and revoke user access rights from all systems upon *constituent* termination. Formal procedures should be in place to manage the controlled revocation of logical access rights to an organization's systems.

Control:
User system access is removed upon termination.

Procedure:
a. Obtain from the *service provider* a list of *constituents* terminated in the past 12 months.
b. Obtain from the *service provider* a user account listing for the hardware sample generated in H.1 Password Control using the Practitioners' Notes in Section Z.
c. Inspect the user account listing obtained in step b for evidence of terminated *constituents* from step a.
d. Report the number of systems sampled, the number of accounts on the selected systems and the number of instances where terminated *constituents* observed in step c are found on the list obtained in step b.

Industry Relevance:
ISO 27002: 8.3.3 Removal of access rights, 11.1.1 Access control policy, 11.2.1 User registration, 11.2.4 Review of user access rights
SIG 5.0: E.6.2, E.6.3

H.3 Logical Access Authorization

Objective:
An organization should ensure that a formal user registration and approval procedure to which employees consistently adhere is in place for granting access to all systems. Formal procedures should be in place to control the allocation of logical access rights to systems.

Control:
Approval process exists for logical access requests.

Procedure:
a. Using the sampling parameters in Section Y, select a sample of users from the list of the user accounts obtained in **H.2 Revoke System Access** step b.
b. For each sample item, obtain from the *service provider* the physical or electronic authorization used to grant privileges to the selected user IDs.
c. For each sample item, inspect the physical or electronic authorization obtained in step b for evidence of approval for logical access requests.
d. Report the number of users sampled and the users sampled where no approval was found.

**Denotes non-core procedure to be used when appropriate according to the industry verticals a service provider serves and/or the specific services offered.*

Industry Relevance:
ISO 27002: 11.1.1 Access control policy, 11.2.1 User registration, 11.2.3 User password management
SIG 5.0: H.2.5.1

H.4 Inactive Accounts

Objective:
An organization should ensure that only active users who actually require access at the present time have system access. Management should review and revoke or disable user logical access rights of inactive *constituents* at regular, predefined intervals.

Control:
Inactive accounts are locked or disabled.

Procedure:
a. Obtain the user ID reports from the hardware sample generated in **H.1 Password Controls** that includes the last log-on date and the account status (active, suspended or locked).
b. Inspect the user ID reports obtained in step a for evidence that users that have not logged on in the past 90 days have had their accounts locked or disabled.
c. For each sample, report the operating system, the total number of accounts on the sampled system, and the number of accounts of users who have not logged on in the past 90 days but have not been locked or disabled.

Industry Relevance:
ISO 27002: 11.5.5 Session time-out
SIG 5.0: H.2.3

H.5 Controls for Unattended Systems

Objective:
An organization should ensure that sufficient preventative controls such as screen or session timeouts are in place to prevent unauthorized log-on access to unattended systems.

Control:
Unattended systems are locked.

Procedure:
a. Using the *inventory of target systems* obtained in **D.1 Asset Accounting and *Inventory***, randomly select one system for each type of operating system in use for *workstations, servers* and *network devices.*
b. For each sample item, obtain from the *service provider* and inspect the system configuration for the timeout variable.
c. Log on to the system and observe whether one of the following controls protects the system after the timeout period:
    1. Password protected screensaver

**Denotes non-core procedure to be used when appropriate according to the industry verticals a service provider serves and/or the specific services offered.*

2. Session timeouts (forced logout)

d. Report the systems sampled and the presence of one or both of the *attributes* listed in step c, or the number of systems that do not have any of the *attributes* listed in step c.

Industry Relevance:
ISO 27002: 11.3.2 Unattended user equipment, 11.5.5 Session time-out
SIG 5.0: H.2.14, H.2.15

H.6 Revoke Physical Access

Objective:
An organization should review and revoke user physical access rights from all information processing facilities upon *constituent* termination. Formal procedures should be in place to manage the controlled revocation of physical access rights to the organization's facilities.

Control:
User access to facilities where *target systems* reside is removed upon termination.

Procedure:

a. Using the sampling parameters in Section Y, select a sample of *constituents* from the list of *constituents* terminated in the past 12 months obtained in **H.2 Revoke System Access.**
b. Obtain from the *service provider* a list of active accounts with physical access to the *target systems.*
c. Inspect the user account listing obtained in step b for the presence of terminated *constituents* from step a.
d. Report the sample of *constituents*, the number of accounts on the selected systems, and the number of instances in which terminated *constituents* observed in step c are found on the list obtained in step b.

Industry Relevance:
ISO 27002: 8.3.3 Removal of access rights, 9.1.2 Physical entry controls, 11.1.1 Access control policy
SIG 5.0: F.1.9.20.4.3, F.2.3.3

H.7 Physical Access Authorization

Objective:
An organization should ensure that a formal user registration and approval procedure to which employees consistently adhere is in place for granting access to all information processing facilities. Formal procedures should be in place to control the allocation of physical access rights to the organization's facilities.

Control:
Physical access is authorized.

**Denotes non-core procedure to be used when appropriate according to the industry verticals a service provider serves and/or the specific services offered.*

Procedure:

a. Using the sampling parameters in Section Y, select a sample of active accounts from the list of active accounts with physical access to the *target systems* obtained in **H.6 Revoke Physical Access.**
b. For each sample item, obtain from the *service provider* the physical or electronic authorization used to grant privileges to the selected user IDs.
c. For each sample item, inspect the physical or electronic authorization obtained in step b for evidence of approval of physical access requests.
d. Report the number of users sampled, and the number of users sampled where no approval was found.

Industry Relevance:
ISO 27002: 8.3.3 Removal of access rights, 9.1.2 Physical entry controls, 11.1.1 Access control policy
SIG 5.0: F.1.10.3.5, F.1.11.2.6, F.1.13.5.6, F.1.14.1.6, F.1.15.2.6, F.1.16.2.6, F.1.17.2.6, F.1.18.2.6, F.1.19.2.6, F.2.2.20.2

H.8 Multifactor Authentication for Remote Access

Objective:
An organization should consider utilizing multifactor authentication to provide an additional level of security for staff with remote access to high-risk systems, including systems that store *target data*.

Control:
Multifactor authentication is required for staff administrator remote access.

Procedure:

a. Using the sampling parameters in Section Y, select a sample of systems from the *inventory* of target systems obtained in **D.1 Asset Accounting and *Inventory*,** which are accessible remotely by staff through client-to-site *VPN* access.
b. Obtain from the *service provider* the user account listing of staff with administrator access for the sample selected in step a, and from this select a user account that is available physically on-site for testing for each sample.
c. Observe the users selected in step b log into the sample systems selected in step a using remote access.
d. Report the number of systems sampled, the type of multifactor authentication used for each access, and whether any of the samples selected did not require multifactor authentication for staff administrator remote access.

Industry Relevance:
ISO 27002: 10.6.2 Security of network services, 11.2.3 user password management, 11.4.2 user authentication for external connections, 11.5.2 User identification and authentication 11.7.1 Mobile Computing and Communications
SIG 5.0: H.4.1.4.3

**Denotes non-core procedure to be used when appropriate according to the industry verticals a service provider serves and/or the specific services offered.*

I. Information Systems Acquisition, Development and Maintenance

Domain Objective:
Organizations should utilize a comprehensive application security program to help ensure that external high-risk applications are consistent with industry security requirements. This should include full application compliance testing and software development reviews.

I.1 Application Vulnerability Assessments/Ethical Hacking

Objective:
An organization should perform application penetration tests or ethical hacking of proprietary web-facing applications. Industry standards such as OWASP should be utilized as a foundation for detecting vulnerabilities in the applications, and measuring the effectiveness of the application security controls in place.

Control:
Vulnerability assessments performed on *externally facing* proprietary website applications that process, store or transmit *target data.*

Procedure:

a. Obtain from the *service provider* the list of proprietary applications that are *externally facing.*
b. From the list obtained in step a, select one application.
c. For the application selected in step b, obtain the most recent ethical hack or application penetration test and inspect for evidence of the following *attributes:*
    1. Cross Site Scripting (XSS)
    2. Injection Flaws
    3. Malicious File Execution
    4. Insecure Direct Object Reference
    5. Cross Site Request Forgery (CSRF)
    6. Information Leakage and Improper Error Handling
    7. Broken Authentication and Session Management
    8. Insecure Cryptographic Storage
    9. Insecure Communications
    10. Failure to Restrict URL Access
d. Report the sample application name, the name of the company that carried out the application evaluation as well as the date, the absence of the *attributes* in step c, or if an ethical hack or application penetration test was not conducted.

Industry Relevance:
ISO 27002: 12.2.1 Input data validation, 12.2.2 Control of internal processing, 12.2.3 Message integrity, 12.2.4 Output data validation, 12.3.1 Policy on the use of cryptographic controls, 12.3.2 Key management, 12.5.4 Information leakage, 12.6.1 Control of technical vulnerabilities, 15.2.2 Technical Compliance Checking
SIG 5.0: I.4.1, I.5

**Denotes non-core procedure to be used when appropriate according to the industry verticals a service provider serves and/or the specific services offered.*

I.2 Secure Systems Development Life Cycle (SDLC) Code Reviews

Objective:
An organization's Systems Development Life Cycle (SDLC) should include security best practices within the key development phases of the application. This should include code reviews of proprietary web-facing applications using industry standards such as OWASP.

Control:
Secure SDLC code reviews are performed on *externally facing* proprietary website applications that process, store or transmit *target data.*

Procedure:

a. Utilize the application selected in I.1 from the *service provider* list of proprietary applications that are *externally facing*.
b. Obtain the SDLC documentation that was generated for the SDLC code review of the application, and inspect for evidence of the following attributes:
    1. Cross Site Scripting (XSS)
    2. Injection Flaws
    3. Malicious File Execution
    4. Insecure Direct Object Reference
    5. Cross Site Request Forgery (CSRF)
    6. Information Leakage and Improper Error Handling
    7. Broken Authentication and Session Management
    8. Insecure Cryptographic Storage
    9. Insecure Communications
    10. Failure to Restrict URL Access
    11. Signoff from Security
c. Report the sample application name, the absence of the *attributes* in step b, or if a SDLC code review was not documented.

Industry Relevance:
ISO 27002: 12.2.1 Input data validation, 12.2.2 Control of internal processing, 12.2.3 Message integrity, 12.2.4 Output data validation, 12.3.1 Policy on the use of cryptographic controls, 12.3.2 Key management, 12.4.1 Control of operational software, 12.5.4 Information leakage, 12.6.1 Control of technical vulnerabilities, 15.2.2 Technical Compliance Checking
SIG 5.0: I.2.9.2.10, I.2.9.2.11, I.2.28.1.6

I.3 Secure System Hardening Standards

Objective:
An organization should ensure that a formal, documented configuration standard exists for building and managing target systems. This should include key configuration and hardening requirements in accordance with industry security best practices, to reduce the risk of compromise.

**Denotes non-core procedure to be used when appropriate according to the industry verticals a service provider serves and/or the specific services offered.*

Control:
Secure systems configuration standards include required industry best practices.

Procedure:

a. Obtain from the *service provider* a copy of the most current, approved *system configuration standard* for each type of operating system in use for *workstations*, *servers* and *network devices*.
b. Inspect the *system configuration and deployment standards* for evidence of the following *attributes*:
    1. Policy maintenance
    2. Removal or renaming of default user accounts and administrator accounts (e.g., guest, administrator, etc.)
    3. Change of default user and system passwords
    4. Restrictions for access to system logs
    5. Increase of default log file size
    6. Local logs are stored or copied to a secure centralized location
    7. Access limits to system files and directories
    8. Application of the most recently available systems software (firmware and patches)
    9. Unnecessary services disabled or removed
    10. Non-secure protocols such as anonymous FTP disabled or removed
    11. Unencrypted administrative remote access protocols such as telnet disabled or removed
    12. Unnecessary physical access ports disabled or removed
    13. Display of warning messages upon access to the device
    14. Modifying configuration settings in accordance with security standards
    15. Unnecessary features including functionality and scripts disabled or removed
    16. One primary function per *server* type
    17. The principle of *least privilege* is applied to user, administrator, and system accounts
    18. Security scan of system is completed prior to storing or processing *target data*
    19. Antivirus software is installed (where applicable)
c. Report the absence of a *system configuration standard* for each operating system, and report any *attributes* listed in step b not found in the *system configuration standard* for each operating system.

Industry Relevance:
ISO 27002: 12.4.1 Control of operational software, 15.2.2 Technical compliance checking, 5.3.2 Protection of information systems audit tools
SIG 5.0: G.14.1, G.15.1

I.4 System Patching

Objective:
An organization should implement an effective software update management process to ensure the most relevant, up-to-date, approved patches are installed for all authorized software. This process should also include weighing the benefit associated with installing a patch to resolve vulnerability against other factors, including the potential impact to system stability.

**Denotes non-core procedure to be used when appropriate according to the industry verticals a service provider serves and/or the specific services offered.*

Control:
System patches are applied.

Procedure:

a. Using the sampling parameters in Section Y, select a sample comprised of *servers*, which includes UNIX, Windows and Linux operating systems from the *inventory* of target systems obtained in **D.1 Asset Accounting and *Inventory*.**
b. Using the operating system vendor's website, obtain the operating system patch list. The list should be current (within 3 months of issue).
c. Using the Practitioners' Notes in Section Z, identify the most recently installed patch or maintenance level for each operating system.
d. Report the number of *servers* and the operating system sampled, and the number of *servers* from step a where any of the patches from step b were not found in the patch list generated in step c. For systems whose patches were not installed, obtain and inspect documentation to determine the existence of management's analysis and approval for not installing the respective patch(es).
e. Document those patches identified in step d for which documentation is not available.

Industry Relevance:
ISO 27002: 12.4.1 Control of operational software, 12.5.3 Restrictions on changes to software packages, 12.6.1,
Control of Technical Vulnerabilities
SIG 5.0: G.15.1.3, I.3

I.5 Application Security Program Governance*

Objective:
An organization should manage the application development activities, methodologies and application security risk. Application security should be part of an organization's overall risk governance framework.

Control: A formal application security risk governance program is implemented.

Procedure:

a. Obtain from the *service provider* the document(s) that are part of the *application security risk governance program*
b. Inspect the document(s) for evidence of the following *attributes*:
    1. Application security policy and procedures
    2. Application security threat assessment program
    3. Application security risk assessment and remediation
    4. Application security risk reporting
    5. Responsibilities of application security risk governance program
    6. Application security training program
    7. Application remediation items from the latest meeting
    8. Date of the last program update
    9. Date of the last program meeting
    10. The business and the technical owner(s) of the program

**Denotes non-core procedure to be used when appropriate according to the industry verticals a service provider serves and/or the specific services offered.*

11. Job titles of the application security risk governance program members

c. Report the *attributes* listed in step b not part of the *application security risk governance program*, the date of the last update, the date of the last meeting, the business and the technical owner(s) of the application risk governance program, the job titles of the Application Security Risk governance program members, or if the *application security risk governance program* does not exist.

Industry Relevance:
ISO 27002: 12.4.1 Control of operational software, 13.1.2 Reporting security weaknesses, 13.2.1 Responsibilities and procedures, 15.2.2 Technical compliance checking, 5.3.2 Protection of information systems audit tools, SIG 5.0: A.1.1, A.1.2, A.1.2.4, I.1.1

I.6 Application Security Vulnerability Assessment and Remediation*

Objective:
An organization should ensure that application security vulnerabilities are assessed for business risk and impact, and have a vulnerability remediation plan.

Control:
Application risks are assessed as part of a formal application security vulnerability assessment and remediation program.

Procedure:

a. Obtain from the *service provider* the list of active application security risks which are documented as part of the application security program.
b. From the list obtained in step a, select one risk.
c. For the risk selected in step b, obtain from the *service provider* the most recent application security assessment documentation and inspect for evidence of the following *attributes*:
    1. Risk prioritization
    2. Business impact
    3. Vulnerability remediation plan
    4. Application risk decision: accept, reject, reduce or transfer
    5. Job title(s) that made the application risk decision
    6. Timeline to resolve
d. Report the *attributes* listed in step c not found in the application security documentation, and the job title(s) that made the application risk decision, or if a list of active application security risks does not exist.

Industry Relevance:
ISO 27002: 4.1 Assessing security risks, 4.2 Treating security risks, 15.2.2 Technical Compliance Checking
SIG 5.0: A.1.1, A.1.2, A.1.2.4, I.1.1

**Denotes non-core procedure to be used when appropriate according to the industry verticals a service provider serves and/or the specific services offered.*

I.7 Application Security SDLC Phases*

Objective:
An organization should ensure that security requirements are part of the key phases of their internal SDLC program. This process should ensure that security reviews, security scans and security signoff occurs at applicable phases.

Control:
Security reviews are completed within the organization's SDLC program.

Procedure:
a. Obtain from the *service provider* the document(s) that are part of SDLC.
b. Inspect the document(s) for evidence of the following *attributes*:
    1. The SDLC phases where security participation is required
    2. The SDLC phases where security signoff is required
    3. Security evaluation of third party libraries
    4. Security signoff prior to application release
    5. Ongoing security maintenance post software release
    6. Job title of the individual providing a security signoff
    7. Date of the last program update
    8. Assigned business and the technical owner(s) of the SDLC process
c. Report the *service provider* SDLC phases, the phases where security participation is required, the phases where security signoff is required, the job title of the individual providing a security signoff, the *attributes* not found in step b, the date of the last program update, the assigned business and the technical owner(s) of the SDLC process, and if the SDLC documentation does not exist.

Industry Relevance:
ISO 27002**:** 12.2.1 Input data validation, 12.2.2 Control of internal processing, 12.2.3 Message integrity, 12.2.4, Output data validation, 12.3.1 Policy on the use of cryptographic controls, 12.3.2 Key management, 12.4.1 Control of operational software,12.5.4 Information leakage, 12.6.1 Control of technical vulnerabilities, 15.2.2 Technical, Compliance Checking
SIG 5.0**:** I.2.9.2.10, I.2.9.2.11, I.2.28.1.6

I.8 Security Review of Internal and External Applications*

Objective:
An organization should perform security reviews of applications developed internally, as well as third party applications that process, store or transmit *target data.*

Control:
Security reviews are performed on internally developed applications, and third party applications that process, store or *transmit target data.*

Procedure:
a. Obtain from the *service provider* the list of both the internally developed applications and the third party applications that process, store or transmit *target data*.

**Denotes non-core procedure to be used when appropriate according to the industry verticals a service provider serves and/or the specific services offered.*

b. From the two lists obtained in step a, select one application from each.
c. For each of the applications selected in step b, obtain from the service provider the applicable SDLC and security review documentation, and inspect for evidence of the following *attributes:*

Application Developed Internally:

1. Security review in the functional design phase
2. Security review in the technical design phase
3. Source code review of application
4. Security scan or penetration test of application
5. Risk assessment and remediation process
6. Security review of third party libraries
7. Documented list of security requirements and status
8. Documented list of security requirements not implemented
9. Electronic or written signoff signifying security acceptance of risk for any documented security requirements not implemented
10. Electronic or written signoff signifying security acceptance

Third Party Application:

1. Security evaluation during the procurement process
2. Security scan or penetration test of application
3. Security configuration recommendations
4. Electronic or written signoff signifying security acceptance
5. Job title of the individual(s) providing a security signoff

d. Report the name of the application selected and the release dates, the absence of the *attributes* in step c, the job title of the individual(s) providing security signoff, and if the SDLC review documentation does not exist for the sampled internally developed application or if the security review documentation does not exist for the sampled third party application.

Industry Relevance:
ISO 27002: 12.2.1 Input data validation, 12.2.2 Control of internal processing, 12.2.3 Message integrity, 12.2.4 Output data validation, 12.3.1 Policy on the use of cryptographic controls, 12.3.2 Key management, 12.5.4 Information leakage, 12.6.1 Control of technical vulnerabilities, 15.2.2 Technical Compliance Checking
SIG 5.0: I.4.1, I.5

I.9 Application Security Awareness Training Content*

Objective:
An organization should ensure that the content of its application security program incorporates current and relevant security attacks and vulnerabilities mitigation, and that the course content is applicable to the organization and its environment.

**Denotes non-core procedure to be used when appropriate according to the industry verticals a service provider serves and/or the specific services offered.*

Control:
Application security awareness course content deals with security vulnerabilities and is applicable to the organization and its environment.

Procedure:

a. Obtain from the *service provider* the document(s) that are part of the Application Security Training Program.
b. Inspect the document(s) for evidence of the following *attributes*:
    1. Current *OWASP Top 10* application security vulnerabilities
    2. *Secure Coding Standards*
    3. High-risk vulnerabilities applicable to organization
    4. Application security best practices relevant to the organization
    5. Vulnerability remediation process
    6. Requirement to successfully pass the organization's application security exam upon completion of course
    7. Date of the last update
c. Report the *attributes* listed in step b not found in the application security training program, the date of last update, and if an application security training program does not exist.

Industry Relevance:
ISO 27002: 8.2.2 Information security awareness, education, and training
SIG 5.0: E.4

I.10 Application Security Awareness Training Attendance and Certification*

Objective:
An organization should ensure that its software developers are aware of application security and secure coding best practices, that they attend a formal application security training program at least annually and that they pass an application security exam upon course completion.

Control:
Developers attend application security awareness training annually, and pass an application security exam upon course completion.

Procedure:

a. Using the sampling parameters in Section Y, select a sample of software developers from the employee list obtained in B.3.
b. For each sample item, obtain from the *service provider* the most recent physical or electronic record evidencing the employee's completion of the company's application security training program obtained in *I.9 Application Security Awareness Training Content*, and evidence of successfully passing an exam post course completion.
c. Inspect the application security program documentation and the most recent physical or electronic record for a signature evidencing that the employee has received application security training within the last year, that he or she has successfully passed the organization's application security exam post course completion, and the job title(s) of the individual(s) instructing.

**Denotes non-core procedure to be used when appropriate according to the industry verticals a service provider serves and/or the specific services offered.*

d. Report the number of employees sampled, the number of employees sampled where there is no evidence of application security training occurring within the last year, the number of employees sampled that have not passed the organization's application security exam post course completion, the job title(s) of the individual(s) instructing, or where evidence of application security training or an application security exam requirement do not exist.

Industry Relevance:
ISO 27002: 8.2.2 Information security awareness, education, and training
SIG 5.0**:** E.4

**Denotes non-core procedure to be used when appropriate according to the industry verticals a service provider serves and/or the specific services offered.*

J. Information Security *Incident* Management

Domain Objective:
Organizations' *incident* response programs should include formal event reporting and escalation procedures that should be clearly communicated throughout the organizations, and should include the active participation of *incident* response members with clearly defined roles and responsibilities.

J.1 Information Security *Incident* Management Policy and Procedures Content

Objective:
An organization should establish a formal information security event reporting procedure, together with an *incident* response and escalation procedure to be executed in the event of a potential *incident*.

Control:
Information security *incident* management policy and procedures incorporate key relevant *attributes*.

Procedure:

a. Obtain from the *service provider* a copy of the information security *incident* management policy and procedures.
b. Inspect the document(s) obtained in step a for evidence of the following *attributes*:
    1. Organizational structure is defined
    2. Response team is identified
    3. Response team availability is documented
    4. Timelines for *incident* detection and disclosure are documented
    5. *Incident* process lifecycle is defined including the following discrete steps:
        a) Identification
        b) Assignment of severity to each *incident*
        c) Communication
        d) Resolution
        e) Training
        f) Testing
        g) Reporting
c. Report the *attributes* listed in step b not found in the *information security incident management policy and procedures*, or the nonexistence of *information security incident management policy and procedures.*

Industry Relevance:
ISO 27002: 13.1.2 Reporting security weaknesses, 13.2.1 Responsibilities and procedures, 13.2.2 learning from
information security *incidents*, 13.2.3 Collection of evidence
SIG 5.0: J.1.1, J.2.1

**Denotes non-core procedure to be used when appropriate according to the industry verticals a service provider serves and/or the specific services offered.*

K. Business Continuity Management

Domain Objective:
Organizations should incorporate business continuity considerations into the overall design of their business model to mitigate the risk of service disruptions and the impacts of those within the supply chain. This should include an enterprise-wide, process-oriented approach that considers technology, business operations, testing, and communication strategies that are critical to *business continuity planning* for the entire business.

K.1 Business Impact Analysis

Objective:
An organization should conduct an assessment and prioritize all business functions and processes, including their interdependencies, as part of a workflow analysis. This assessment should also evaluate the potential impact of business disruptions resulting from uncontrolled, non-specific events on the organization's business functions and processes.

Control:
Business impact analysis is implemented.

Procedure:
a. Obtain from the *service provider* a copy of the *business continuity plan (BCP)* and a copy of the most recent *business impact analysis (BIA).*
b. Inspect the BCP for evidence 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
c. Report the nonexistence of the *attributes* listed in step b, or the nonexistence of a *BCP* and a *BIA*

Industry Relevance:
ISO 27002: 14.1.2 Business continuity and risk assessment, 14.1.3 Developing and implementing continuity plans including information security
SIG 5.0: K.1.15.1

K.2 Threat Assessment

Objective:
An organization should create and maintain an in-depth business threat assessment that includes realistic threat scenarios such as malicious activity, natural and technical disasters, and pandemic *incidents*. The magnitude of the business disruption should consider a wide variety of threat scenarios, including capacity.

Control:
BIA is aligned with existing assets and the key industry threats to these are identified.

**Denotes non-core procedure to be used when appropriate according to the industry verticals a service provider serves and/or the specific services offered.*

Procedure:

a. Using the sampling parameters in Section Y, select a sample of *business processes* from the BIA obtained in **K.1 Risk (Threat and Impact) Analysis.**
b. Inspect the BIA for the following quantitative and qualitative *attributes*:
   Asset types:
   1. People (health and safety)
   2. Processes (business and IT)
   3. Information (electronic and paper)
   4. Software
   5. Hardware
   6. Communications
   7. Power/energy
   8. Transportation system disruptions

   Malicious Threats:
   1. Fraud
   2. Theft
   3. Blackmail
   4. Sabotage
   5. Terrorism

   Natural Threats:
   1. Floods or water damage
   2. Severe weather

   Accidental Threats:
   1. Fire
   2. Air contaminants
   3. Hazardous chemical spills
   4. Business or IT process error (process existed, but was not used properly when event occurred)
   5. Business or IT non-process error (process didn't exist to avoid accident)

   Business environment:
   1. IT capacity impact due to business opportunities
   2. Legal, regulatory, industry standard or customer contract changes impacting IT

   Threat variables
   1. Internal or external source
   2. Probability of occurrence
   3. Impact

c. Report the *attributes* listed in step b not found in the *BIA*, or if a *BIA* was not conducted or documented.

Industry Relevance:
ISO 27002: 14.1.2 Business continuity and risk assessment, 14.1.3 Developing and implementing continuity plans including information security
SIG 5.0: A.1.2.3.1

K.3 Business Continuity Governance*

Objective:
An organization should create and maintain an in-depth *business continuity governance plan* that documents the program details, the decision making and communication process, and defines who is responsible for which components of governance.

Control:
A *business continuity governance plan* is implemented and maintained.

Procedure:

a. Obtain from the *service provider* a copy of the *Business Continuity Governance Plan* and the *resulting working documents* of the business continuity governance body.
b. Inspect the *Business Continuity Governance Plan* and *working documents* for evidence of the following *attributes:*
    1. Mission/Objective statement
    2. Membership structure and responsibilities, including roles
    3. *Decision making process flows*
    4. *Communications plan*
    5. Schedule for governance board meetings
    6. Agendas of meetings
    7. Meeting minutes
    8. Communications on business continuity decision-making are shared with the executive management team and/or board of directors
c. Report the *attributes* listed in step b not found in the *Business Continuity Governance Plan* and resulting *working documents*, the titles of the Business Continuity Governance body members, the titles of those that were present at the last meeting, the defined governance body meeting frequency, the dates of the last two meetings, or the nonexistence of a *business continuity governance statement/plan.*

Industry Relevance:
ISO 27002: 14.1.2 Business continuity and risk assessment, 14.1.3 Developing and implementing continuity plans including information security
SIG 5.0: K.1

K.4 *Business Process* Level Readiness*

Objective:
An organization should create and conduct *business continuity planning* and analysis to be able to evaluate the business continuity readiness of end-to-end *business processes*.

**Denotes non-core procedure to be used when appropriate according to the industry verticals a service provider serves and/or the specific services offered.*

Control:
A *business process level analysis and plan* is implemented and maintained.

Procedure:

a. Obtain from the *service provider* the list of critical *business processes.*
b. From the list obtained in step a, select one critical *business processes.*
c. For the *business process* selected in step b, obtain from the *service provider* the most recent *business continuity analysis plan* and inspect for evidence of the following *attributes*:
    1. End-to-end workflow description or diagram of the business process
    2. *Map of dependencies*
    3. List of *incidents* that could occur that could degrade the delivery of the business process
    4. Action plans to reduce the likelihood and impact of potential *incidents* degrading the delivery of the business process.
    5. Statement of to whom action plans have been communicated and who has approved within the enterprise
    6. Creation of controls to monitor the likelihood and impact of potential *incidents*
    7. Project or other work records demonstrating progress on the action plans
    8. Statement of maximum allowable downtime
    9. Response plans includes:
        a) Alternative resources (back-up power, consultants on call, *warm sites*, *hot sites*).
        b) Explicit level-of-service provision in accordance with contractual and/or regulatory requirements.
d. Report the name of the *business process* selected and, the nonexistence of the *attributes* listed in step c*,* the date of the last update, or if the *business continuity analysis plan* does not exist.

Industry Relevance:
ISO 27002: 14.1.1 Including information security in the business continuity management process, 14.1.2 Business continuity and risk assessment, 14.1.3 Developing and implementing continuity plans including information security, 14.1.4 Business continuity planning framework, 14.1.5 Testing, maintaining and re-assessing *business continuity plans*,
SIG 5.0: K.1

K.5 Business Continuity Threat Assessments*

Objective:
An organization should create and maintain realistic threat scenarios which consider internal, business partners, and customers. These threat scenarios should focus both on the impact of the threat as well as the nature of the threat.

Control:
A *threat assessment* is conducted based on the actual threat environment, the nature of the service provided and the service provision environment

**Denotes non-core procedure to be used when appropriate according to the industry verticals a service provider serves and/or the specific services offered.*

Procedure:

a. Obtain from the *service provider* a copy of the most recent *threat assessment*
b. Inspect the threat assessment for evidence of the following *attributes*:
    1. Description of services provided
    2. Inclusion of Service provider environment types including software, hardware, facilities and location.
    3. Dependencies list involved in the provision of the business process
    4. Types of threats (natural, malicious, accidental and business activity) to which services are exposed
    5. Action plans to reduce the likelihood and impact of potential *incident*s degrading the delivery of the business processes
    6. Statement of to whom action plans have been communicated and who has approved within the enterprise.
    7. Creation of controls to monitor the likelihood and impact of potential *incidents*
    8. Project or other work records showing the present status of the action plans
c. Report the *attributes* obtained in step b not found in the *threat assessment*, the date of the last update, or the nonexistence of a *threat assessment.*

Industry Relevance:

ISO 27002: 14.1.1 Including information security in the business continuity management process, 14.1.2 Business continuity and risk assessment, 14.1.3 Developing and implementing continuity plans including information security, 14.1.4 *Business continuity planning* framework, 14.1.5 Testing, maintaining and re-assessing *business continuity plans*,
SIG 5.0: A.1.2.3.1, K.1

K.6 Business Continuity Process Testing*

Objective:

An organization should create and maintain detailed *business continuity test plans*. These should include scoping the business process and identifying the dependencies, as well as detailed testing to complete a realistic and thorough test.

Control:

Business continuity test plans for business processes are scoped and the problems identified are made visible, and have an associated remediation action.

Procedure:

a. *Obtain from the service provider the most recent business continuity test plan and results* for the critical business process sample obtained in ***K.4 Business Process Level Readiness****.*
b. *Inspect the business plan and results* for evidence of the following *attributes*:
    1. Business scope and structure of the test:
        a) Defined business scope for the test (such as an entire business, a business process(es), *facility*(*ies)*, geographic area, *server*, or other construct)
        b) Roles involved in developing the test and participating in the test (such as Board, CEO, CRO, CIO, business line leaders, crisis management, facilities

**Denotes non-core procedure to be used when appropriate according to the industry verticals a service provider serves and/or the specific services offered.*

management, internal audit, IT systems mangers, security managers)
c) Input to the test plan includes:
1) Formal statement of changes in business operations (external and internal)

2. Prior audit and/or regulatory examination recommendations, and prior test results. Business process dependencies:
a) Internal and external dependencies listed
b) Related to people
c) Related to processes
d) Related to information systems "stack":
1) IT management processes
2) Applications
3) Middleware
4) Server
5) Storage
6) Networking
7) Physical facilities

3. Test Plan Metrics:
a) Related to RTO
b) Related to RPO
c) Related to business metrics
d) Related to the maximum allowable downtime (MAD) for the business process in scope

4. Test Plan Scenarios:
a) List of scenarios that would require the recovery of the *business process*
b) List of threats
c) List of event types
d) Crisis management situations
e) Scenarios analysis includes:
1) Examination for single points of failure within both the infrastructure and the vendors
2) Single points of failure evaluation of vendors for:
a) Equipment relocation
b) Alternative staff work locations
c) Back-up fuel
3) Preferential supply relationships availability
4) Adverse events in geographic areas include:
a) Loss of access to an office location
b) Loss of power or communications
c) Public safety limitation on access to roadways or geographic areas
d) Regional weather or civil unrest event
e) Pandemic
5) Ability to support customers with higher than normal service levels

**Denotes non-core procedure to be used when appropriate according to the industry verticals a service provider serves and/or the specific services offered.*

during times of public disaster (such as extra cash in automated teller machines and computer equipment in stock)

5. Test Types such as:
   a) Tabletop exercise/structured walk-through test
   b) Walk-through drill/simulation test
   c) Functional drill/parallel test
   d) Full-interruption/full-scale test

6. Test Results and Actions:
   a) Outcomes linked to top-level objectives
   b) Root cause and lessons learned documented
   c) Feedback from the board of directors and/or senior executive management on their evaluation of test results
   d) Action/Remediation plans have been communicated within the enterprise

c. Report the name of the *business process* sampled, the *attributes* listed in step c not found in the *business continuity test plan and results,* the date the test plan was last executed, whether a test plan review was completed by a third party and/or an internal auditor, the titles of those involved in executing the test, or the nonexistence of a *business continuity test plan and results* for the sampled *business process.*

Industry Relevance:
ISO 27002: 14.1.1 Including information security in the business continuity management process, 14.1.2 Business continuity and risk assessment, 14.1.3 Developing and implementing continuity plans including information security, 14.1.4 *Business continuity planning* framework, 14.1.5 Testing, maintaining and re-assessing *business continuity plans*,
SIG 5.0: A.1, K.1

**Denotes non-core procedure to be used when appropriate according to the industry verticals a service provider serves and/or the specific services offered.*

L. Compliance

Domain Objective:
Organizations should ensure compliance of information systems with the organizational security policies and standards to include checking systems regularly against compliance with security implementation standards and regulatory requirements.

L.1 Presence of Log-On Banners

Objective:
An organization should ensure that at log on all users accessing target systems are made explicitly aware of the company's legal and internal terms of use. This should include a message indicating the right and restrictions that apply.

Control:
Log-on banners are presented at log on, informing users of restrictions.

Procedure:

a. Using the sample systems generated in **H.1 Password Controls,** observe a user log on to each system and observe whether a log-on banner is present and contains the following *attributes:*
    1. The system being entered is private
    2. Unauthorized access is not permitted
b. Report the systems sampled and the absence of *attributes* listed in a, or the instances for each system sampled where log-on banners are nonexistent.

Industry Relevance:
ISO 27002: 11.5.1 Secure log-on procedures, 15.1.5 Prevention of misuse of information processing facilities
SIG 5.0: H.2.8.5

L.2 Technical Compliance Checking – Vulnerability Testing and Remediation

Objective:
An organization should ensure that externally facing systems are regularly scanned for compliance against industry security standards including SANS 20, and that any applicable detected vulnerabilities are remediated.

Control:
Target systems are scanned for vulnerabilities and identified vulnerabilities are remediated.

Procedure:

a. Using the sample systems generated in **H.1 Password Controls,** obtain from the *service provider:*
    1. One *external* SANS 20 *vulnerability scan* report dated within the preceding two to six months
    2. One *external* SANS 20 *vulnerability scan* report dated within the past month

**Denotes non-core procedure to be used when appropriate according to the industry verticals a service provider serves and/or the specific services offered.*

b. Report the name and version of the scanner, the report's generation date, the number of vulnerabilities detected in the reports obtained in step a1 and a2 and the number of vulnerabilities that are common to the reports obtained in step a1 and a2, or nonexistence of vulnerability scans.

Industry Relevance:
ISO 27002: 15.2.2 Technical compliance checking
SIG 5.0: L.11, L.11.1

**Denotes non-core procedure to be used when appropriate according to the industry verticals a service provider serves and/or the specific services offered.*

P. Management of Privacy Program

Domain Objective:
Organizations should establish a management framework to control and manage their privacy program. This should include the overall management of the privacy program within the organization and with all *third parties* that have access to *target privacy data*. The privacy program should include: individuals responsible for the creation, oversight and maintenance of the program; all *third parties* meeting their commitments under the organization's business requirements, *privacy applicable law*, policy and industry best practices; and the protection and privacy of *target privacy data* through its life cycle of collection, storage, usage, sharing, transferring, securing, retention and destruction.

P.1 Target Privacy Data *Inventory* and Flows*

Objective:
An organization should *inventory*, define by *data subject category* and assign ownership for *target privacy data* and document its flow through the data life cycle of collection, storage, use, sharing, trans-border flows, retention and retirement though the organization and its *third parties*.

Control:
An *inventory* of all *target privacy data*, defined by *data subject category*, its ownership and its flow is maintained and updated annually with all required information in the *privacy inventory/flow*. It has been approved and reviewed within the last 12 months and contains a revision history.

Procedure:

a. Obtain from *service provider* a list of current *third parties* that access *target privacy data.* Using the sampling parameters in Section Y, select a sample from the *third party* list.
b. Obtain from the *service provider* and the selected *third parties*, via the *service provider,* a copy of their *privacy inventory/flow*; a copy of the *privacy policy*; *privacy notice*s; and procedures for jurisdictions determined to be in scope.
c. For the *service provider* and each *third party* in the sample chosen, inspect the *privacy inventory/flow* documents obtained in b for evidence of the following *attributes:*
    1. Classifications for security for each *data subject category*
    2. *Privacy inventory/flow* for each jurisdiction or group of jurisdictions
    3. *Privacy inventory/flow* for sources/origin (including detailing from whom (entity) and from where collected (country))
    4. *Target privacy data* owner and *target privacy data* "*data controller*," if applicable
    5. Media types used for storage, access, processing, transport, retention, reporting, archiving and destruction
    6. Location (entity and country) for storage
    7. Retention and destruction schedules
    8. Purpose(s) for collection and use
    9. List of who (role and location (entity and country)) uses *target privacy data* for what purposes

**Denotes non-core procedure to be used when appropriate according to the industry verticals a service provider serves and/or the specific services offered.*

10. List of who (role and location (entity and country)) receives *target privacy data* within the *service provider*, the selected *third parties* and outside the *service provider* to the client
11. List of what *target privacy data* is transferred (including on media, in processing or on display) across borders (state or international)
12. List of *third parties* that access the *target privacy data*
13. The organizational owner(s) and approval(s) of *privacy inventory/flow* documents
14. Evidence of approval, including the most recent approver's title and date of approval
15. Date of last review
16. Revision history
17. Compare the flow of *target privacy data* in the *privacy policy, privacy notices* and procedures to that found in the *privacy inventory/flow* documents:
    a) Sources/origins and where collected
    b) Purpose(s) for collection and use
    c) Location for storage
    d) Retention and destruction schedules
    e) Role and location of the individual that uses *target privacy data*
    f) Role and location of the individual that receives *target privacy data*

d. For the *service provider* and each third party in the sample chosen, report the applicable *attributes* listed in step b that were not found.

Industry Relevance:
MA Information Security Regulation; EU Directive
SIG 5.0**:** P.9, P.10, P.11, P.12.1-10

P.2 *Privacy Policy* and *Privacy Notices**

Objective:
An organization should provide management policy, direction and support for information privacy in accordance with privacy business requirements and *privacy applicable law*. It should demonstrate support for, and commitment to, information privacy through the issue, acceptance and maintenance of a *privacy policy* across the organization. It should, where required, communicate that commitment to *data subjects* via *privacy notices* and where applicable gain their consent and seek their *permission* for certain uses of *target privacy data*. It should ensure that *third parties' privacy policies* and *privacy notices* are consistent with its *privacy policy* and *privacy notices*. The *privacy policy* and *privacy notice*s should incorporate the key areas of privacy and should be reviewed at planned intervals (at least annually), or if significant changes occur, to ensure continuing suitability, adequacy and effectiveness.

Control:
Privacy policy and privacy notices of service provider and third parties have been developed, maintained, and include the Privacy Principles developed by the OECD or the Generally Accepted Privacy Principles developed by the AICPA/CICA and have been approved and reviewed within the last 12 months and contain a revision history.

**Denotes non-core procedure to be used when appropriate according to the industry verticals a service provider serves and/or the specific services offered.*

Procedure:

a. Obtain from *service provider* a copy of its privacy business requirements and the requirements of privacy *applicable law*, both of which *service provider* has confirmed are current and complete.
b. Using the sample of *third parties* from the list obtained in **A. Target Privacy Data *Inventory* and Flows**, obtain from *service provider* and selected *third parties*, via the *service provider,* a copy of their current applicable *privacy policy* and *privacy notices.*
c. For the *service provider* and each *third party* in the sample chosen, inspect the *privacy policy and the privacy notices* obtained in b for evidence of the following *attributes:*
    1. The privacy business requirements and the requirements of *privacy applicable law*.
    2. Categories of *target privacy data* collected and the purposes (or restrictions) for which this information is used
    3. Categories of *protected target privacy data* and requirement to protect this information
    4. Categories of affiliates and other *third parties* to whom *service provider* discloses *target privacy data*
    5. Transfer and share of *target privacy data* with requirement to comply with *applicable privacy law* on cross-border transfers
    6. Restrictions for transfers in the *privacy notice* that prevent a flow to or from a jurisdiction
    7. Security section that states the commitment to protect the *target privacy data*
    8. *Data subject* access and corrections section that informs the *data subject* on how to gain access to *target privacy data* for review, correction and/or deletion
    9. *Data subject* contact section for questions and complaints
    10. Collection of personal information of children
    11. Reference to the law of the jurisdiction, where required
    12. Changes to *privacy notic*e
    13. Effective date
    14. Cookies and cookie policy, for online notices
    15. Use of IP address and other online technology information, for online notices
    16. A consent to the *privacy notice* section, which varies from jurisdiction to jurisdiction
    17. Promotional communications and the right to opt out from those communications
    18. Evidence of approval, including the most recent approver's title and date of approval
    19. Date of last review
    20. Revision history

    Compare the content of each of the following *attributes* of the *third parties' privacy policy and privacy notices* to the *service provider's privacy policy* and *privacy notices* to confirm they are the same:

    a) Categories of *target privacy data* collected and the purposes (or restrictions) for which this information is used
    b) Categories of *protected target privacy data* and requirement to protect the information
    c) Categories of affiliates and other *third parties* to whom *service provider* discloses *target privacy data*
    d) Transfer and share of *target privacy data* with requirement to comply with *applicable privacy law* on cross-border transfers

**Denotes non-core procedure to be used when appropriate according to the industry verticals a service provider serves and/or the specific services offered.*

e) Restrictions for transfers in the *privacy notice* that prevent a flow to or from a jurisdiction
f) Security section
g) *Data subject* access and corrections section that informs the *data subject* on how to gain access to *target privacy data* for review, correction and/or deletion
h) *Data subject* contact section for questions and complaints
i) Collection of personal information of children
j) Reference to the law of the jurisdiction, where required
k) Changes to *privacy notice*
l) Effective date
m) Cookies and cookie policy, for online notices
n) Use of IP address and other online technology information, for online notices
o) A consent to the *privacy notice* section, which varies from jurisdiction to jurisdiction
p) Any promotional communications and the right to opt out of those communications

d. For the *service provider* and each *third party* in the sample chosen, report the applicable *attributes* listed in step b that were not found.

Industry Relevance:
AICPA/CICA; APEC; EU Data Protection Directive; FFIEC Handbook Guidelines re Privacy; FCC Privacy Guidelines and Regulations; FTC Privacy Guidelines and Regulations; GLBA; HIPAA; HITECH/ARRA; Japanese Privacy Seal; PIPEDA;
SIG 5.0**:** P.1, P.4, P.14.2-5, P.42

P.3 Privacy Organization and Program Maintenance*

Objective:
An organization should ensure that the organization and *third parties* each have a designated privacy individual responsible for its *privacy policy* and program. The privacy program should contain enforcement and monitoring procedures, and a change management procedure to remain current with privacy changes in business requirements, *privacy applicable law*, policy and industry best practices.

Control:
An individual has been assigned as accountable for the privacy program at *service provider* and *third parties*. Accountability includes creation, review, enforcement and a change management process for the *privacy policy* and program. This responsibility is documented as part of the organization chart and roles and responsibilities for the privacy program. Key procedures have been written for due diligence, review and compliance, enforcement and monitoring, and change management.

Procedure:
a. Using the sample of *third parties* from the list obtained in **P.1 Target Privacy Data *Inventory* and Flows**, obtain from *service provider* and from the selected *third parties,* via the *service provider*, a copy of the most current, approved organization chart and

**Denotes non-core procedure to be used when appropriate according to the industry verticals a service provider serves and/or the specific services offered.*

responsibilities for the privacy program, the privacy program responsibilities procedures, the most recent reviews, due diligence, compliance and enforcement events, on-site audits, security program audits, change management procedures, remediation plans and changes implemented during the past 12 months, and any privacy regulator finding or court ruling concerning *target privacy data* each confirmed by third parties as current and complete.

b. For each *third party* in the sample chosen, inspect the documents to confirm the *service provider* and *third parties* have documents regarding their responsibilities for managing their privacy program and supporting the privacy programs of their clients by looking for evidence of the following *attributes:*
    1. There is an individual responsible for their privacy program
    2. Due diligence procedures for third parties on compliance with privacy applicable law prior to contracting with a third party
    3. Review of company target privacy data practices for compliance with privacy program and enforcement procedures for non compliance
    4. On-site audits of third parties accessing target privacy data
    5. Security program audits
    6. Change management procedures
    7. Records of the most recent reviews, remediation plans, and changes implemented during the past 12 months as a result of due diligence, review, compliance and enforcement procedures, on-site audits, security program audits and change management procedures
    8. Records of any privacy regulator finding or court ruling concerning *target privacy data* within the last 12 months
    9. For *third parties*, there is an assigned individual responsible for the applicable elements of the *service provider*'s *privacy policy*
c. For the *service provider* and each *third party* in the sample chosen, report the applicable *attributes* listed in step b that were not found.

Industry Relevance:
AICPA/CICA; APEC; EU Data Protection Directive; FFIEC Handbook Guidelines re Privacy; FCC Privacy Guidelines and Regulations; FTC Privacy Guidelines and Regulations; GLBA; HIPAA; HITECH/ARRA; Japanese Privacy Seal; PIPEDA;
SIG 5.0**:** P.3, P.6, P.14.7, P.43-P.45, P.47-P.50, P.60

P.4 Privacy Third Party Agreements*

Objective:
All entities that access, process, or store *target privacy data* can be a risk to an organization or its clients. Management should ensure that all agreements with *third parties* contain specific clauses to ensure *target privacy data* is protected and that certain other privacy requirements are included.

Control:
Privacy agreements detail privacy and protection requirements between the *service provider* and its *third parties* that have access to *target privacy data*.

**Denotes non-core procedure to be used when appropriate according to the industry verticals a service provider serves and/or the specific services offered.*

Procedure:

a. Using the sample of *third parties* from the list obtained in **P.1 Target Privacy Data *Inventory* and Flows***,* obtain from the *service provider* and selected *third parties*, via the *service provider,* the privacy and security portions of the agreement with the *service provider* in place for providing services and a representative sample of *third party* privacy and security sections of the agreements from each *third party*.

b. Inspect each agreement chosen in the sample for evidence of the following *attributes:*
   1. *Third party* requirement to protect all *target privacy data* and *protected target privacy data*
   2. *Third party* requirement to document the flow of *target privacy data* within its organization and to those *third parties* with whom it shares *target privacy data*
   3. *Third party* requirement to process *target privacy data* in accordance with agreement
   4. *Third party* requirement to collect only the minimum *target privacy data* necessary to achieve the purposes for which it is collected
   5. *Third party* requirement to collect *target privacy data* by legal means only
   6. *Third party* requirement to implement policies, procedures and safeguards consistent with the agreement's specified privacy requirements, *privacy applicable law*, policy and industry best practices when managing *target privacy data*
   7. Requirement to notify *service provider* of potential event affecting *target privacy data*
   8. *Third party* requirement to notify *service provider* if a *data subject* requests access, correction, or deletion of his/her *target privacy data*, or asks a question or makes a complaint
   9. *Third party* requirement to comply with *privacy applicable law*, including countries with privacy laws that transcend the borders of their country or region (EU/EEA, e.g., by entering into the model clauses for international data transfers,Canadian, AR, AU, NZ, HK, JP and other onward transfer requirements for privacy of *target privacy data*, such as APEC or various seal programs)
   10. Retain or delete *target privacy data* according to a schedule
   11. Retain *target privacy data* within certain country/region boundaries
   12. Protect *service provider* employee *target privacy data*
   13. Contractually pass on "at least as stringent" privacy obligations under this agreement to any *third parties* that access or handle in any way the *target privacy data* and all further levels/chains of *third parties*
   14. Prohibition on the sale of *target privacy data, where required*

c. For the *service provider* and each *third party* in the sample chosen, report the applicable *attributes* listed in step b *exceptions* found**.**

Industry Relevance:

AICPA/CICA; APEC; EU Data Protection Directive; FFIEC Handbook Guidelines re Privacy; FCC Privacy Guidelines and Regulations; FTC Privacy Guidelines and Regulations; GLBA; HIPAA; HITECH/ARRA; Japanese Privacy Seal; PIPEDA;
SIG 5.0**:** P.2, P.4, P.5, P.5.1-P.5.15

**Denotes non-core procedure to be used when appropriate according to the industry verticals a service provider serves and/or the specific services offered.*

P.5 Legal Authorizations*

Objective:
An organization and *its third parties* should have completed the applicable notifications, registrations, permit, approvals and/or adequacy derogations as required by *privacy applicable law*.

Control:
A record is maintained of all required notifications, registrations, permits, approvals, adequacy mechanisms, and reviews/approvals from any mandated entities (such as employee-related bodies, councils or unions) of the *privacy policy*.

Procedure

a. Using the sample of *third parties* from the list obtained in **P.1 Target Privacy Data *Inventory* and Flows,** obtain from *service provider* and the selected *third parties*, via the *service provider,* copies of all records of legal authorizations and any related documentation required under *privacy applicable law* and their *privacy inventory/flow.* This includes registrations and permits from authorities in each jurisdiction receiving *target privacy data* identified in the *privacy inventory/flow,* requiring such by *privacy applicable law*, *privacy notices* for each applicable jurisdiction and the adequacy of mechanisms such as individual consents, Safe Harbor filings, model contracts and binding corporate rules, and other derogations. This would also include the most recent reviews, due diligence, compliance and enforcement events, on-site audits, security program audits, change management procedures, remediation plans, and changes implemented during the past 12 months and any privacy regulator finding or court ruling concerning *target privacy data.*
b. For each item in the sample, inspect for the following *attributes:*
    1. Notifications, registrations, permits and approvals and adequacy mechanisms (such as EU model clauses, safe harbor, binding corporate rules, and any approval required by data protection authorities)
    2. Mandated reviews and/or approvals of privacy material required under *privacy applicable law*s
    3. Outstanding requests from data protection authorities or any other entity that regulates *target privacy data*
    4. Outstanding remedial steps for any disputes or legal authorizations not granted by any data protection authority or any other entity that regulates *target privacy data*
c. For each item in the sample, report the *service provider* and *third parties* with access to *target privacy data* who do not have documentation of the approvals required by the data protection authorities and mandated reviews required under *privacy applicable laws.* For each item in the sample, report records of outstanding requests from b3; records from outstanding remedial steps from b.4.

Industry Relevance:
EU Data Protection Directive
SIG 5.0**:** P.4, P.7, P.8

**Denotes non-core procedure to be used when appropriate according to the industry verticals a service provider serves and/or the specific services offered.*

P.6 Management of Target Privacy Data*

Objective:
An organization should ensure that collection, storage, use, access, sharing, transport, retention and deletion of *Target Privacy Data* is in accordance with *privacy applicable law*, *privacy policy*, *privacy notice*s and industry best practice, and is represented in their documented procedures, and that these procedures are maintained.

Control:
Privacy procedures, which include the key relevant domains of privacy are enforced and maintained.

Procedure:

a. Using the sample from the *third party* list obtained in **P.1 Target Privacy Data *Inventory* and Flows**, obtain from *service provider* and the selected *third parties*, via the *service provider,* a copy of the most current approved privacy procedures.
b. Using the *privacy policy* and *privacy notices* and procedures obtained from *service provider* in **P.2 *Privacy Policy* and *Privacy Notices***, inspect the written privacy procedures for the following *attributes:*
    1. Procedure*s for* delivery collection, storage, use, access, and sharing of *privacy notices,* consents and *permissions*
    2. Procedures for collection, storage, use, access, sharing, transport, retention and deletion of *target privacy data*
    3. Proc*edures to en*sure *target privacy data* is only collected, stored and used for the purposes for which it was collected
    4. Access to *target privacy data* by *service provider* employees, *third parties* and any other individuals is on a need-to-know basis only
    5. If applicable, the conduct of background, criminal, health or various types of screening of individuals who have access to *target privacy data* (including credit, drug, medical or psychological tests)
    6. Procedures to ensure *data subject* screening and testing complies with *privacy applicable law* and that any resulting *target privacy data* is protected to a higher standard or is not received or stored at all
    7. Procedures to ensure *service provider* employees and *third party employees* take special care and protect *protected target privacy data* at a higher level
    8. Procedures to ensure compliance with *privacy applicable law* for retention of *target privacy data*
    9. Procedures for the secure deletion of *target privacy data* according to the *security policy*
    10. Procedures for managing compliance with *privacy applicable law* or policy that are in conflict from a retention and deletion perspective, e.g., pending request of discovery of documents in litigation vs. document deletion regulation of *target privacy data*
    11. If applicable, procedures for handling *target privacy data* outside of the country in which it was collected, including appropriate safeguards for compliance with *privacy applicable law*, such as cross-border transfers (including permitting access to or viewing) of *target privacy data* and countries where transfer of certain *target privacy data* is prohibited

**Denotes non-core procedure to be used when appropriate according to the industry verticals a service provider serves and/or the specific services offered.*

12. Procedures to deliver instructions for *service provider* employees and *third parties* on sharing and cross-border transfers of *target privacy data*
13. Procedures for sharing *target privacy data* with affiliates for their use
14. Procedures to maintain accuracy and currency of *target privacy data*
15. Evidence of approval, including the most recent approver's title and date of approval
16. Date of last review
17. Revision history

c. For each item in the sample, report: the total number of *service provider* and *third parties* with access to *target privacy data;* the number *third parties* sampled; and the details of *service provider* and *third parties* sampled where the privacy procedures do not address the *attributes* listed in (b). Also report the approver's title, date of approval, date of last review and existence or nonexistence of a revision history by *service provider* and *third party*.

Industry Relevance: AICPA/CICA; APEC; EU Data Protection Directive; FFIEC Handbook Guidelines re Privacy; FCC Privacy Guidelines and Regulations; FTC Privacy Guidelines and Regulations; GLBA; HIPAA; HITECH/ARRA; Japanese Privacy Seal; PIPEDA

SIG 5.0**:** P.6, P.13, PP.15.1, P.16.1, P.21-P.32, P.36-P37.1, P.41

P.7 Privacy Awareness*

Objective:
An organization and its *third parties* should ensure that privacy awareness training occurs at least annually and attendance reports for their employees are maintained. This ensures employees are aware of information privacy key requirements and their privacy responsibilities.

Control:
Privacy awareness training occurs at least annually and during on-boarding of new employees, addressing a broad set of privacy topics with comprehension testing included. Attendance reports for *service provider* employees and *third party* employees are maintained.

Procedure:

a. Using the sample from the *third party* list obtained in **P.1 Target Privacy Data *Inventory* and Flows**, obtain from *service provider* and the selected *third parties*, via the *service provider,* a current list of the employees who access the *target privacy data*; records setting out details and content of the privacy awareness training for the past year for these employees; and for each sample item, the most recent physical or electronic record evidencing each *employee's* completion of the applicable privacy awareness training, each of which the *service provider* and third party indicate are complete and the most current version.
b. For each item in the sample, inspect the privacy training program and attendance record (as appropriate) for the following *attributes:*
    1. Confirmation in the attendance record that the *employee* has received privacy awareness training within the last year
    2. Privacy information classification and flow guidelines

**Denotes non-core procedure to be used when appropriate according to the industry verticals a service provider serves and/or the specific services offered.*

3. Management of *target privacy data* and company proprietary information regarding privacy, including collection, storage, use, sharing, transfer, retention, protection and deletion
4. Information on the commitment made to each *data subject*, directing those as required to the supporting policies and procedures
5. Information on legal, regulatory, and contractual responsibilities for privacy
6. Employee comprehension testing of privacy awareness program
7. Information on consequences (including penalties) for violations of *privacy applicable law*, contractual obligations or company privacy program
8. Information on email and *Internet* usage guidelines regarding privacy and monitoring
9. Information on employee and *service provider* equipment monitoring policies for privacy
10. Process to identify content for the development of privacy awareness training for all employees
11. On-boarding privacy training for all employees
12. Records maintained that document participation in training to target metrics and dates

c. For each item in the sample, report the number of *service provider employees* and the number of *third parties'* employees sampled, the number of *service provider employees* and the number of *third parties' employees* sampled where evidence of privacy training is greater than the previous year's. Where evidence of privacy training does not exist, report this as a finding.

Industry Relevance:
AICPA/CICA; APEC; EU Data Protection Directive; FFIEC Handbook Guidelines re Privacy; FCC Privacy Guidelines and Regulations; FTC Privacy Guidelines and Regulations; GLBA; HIPAA; HITECH/ARRA; Japanese Privacy Seal; PIPEDA; Trustee SH Seal; ISO 27000's
SIG 5.0: P.51, P.51.1-13

P.8 Privacy Event Notification and Response Management*

Objective:
An organization should establish a formal privacy communication procedure, integrated with the security incident response and escalation procedure to be executed in the event of a potential breach or other required privacy communication requirement to *data subjects* or other entities, including government agencies.

Control:
Privacy communication procedures incorporate key relevant *attributes* of current communications regarding privacy communications, suspected issues, breach management laws, regulation and policy.

Procedure:
a. Using the sampling parameters in Section Y, select a sample of *third parties* from the list obtained in **P.1 Target Privacy Data *Inventory* and Flows.** Obtain from *service provider* and the selected *third parties*, via the *service provider,* the privacy and security event communication procedures.

**Denotes non-core procedure to be used when appropriate according to the industry verticals a service provider serves and/or the specific services offered.*

b. For each item in the sample, inspect the document(s) obtained in step a. for evidence of the following *attributes*:
    1. Privacy communications team, security incident response procedure, and escalation procedures, in each case with defined roles and responsibilities
    2. Procedures for notifying and supporting subsequent follow up for *data subjects*, *third parties*, *service provider*, organizations or government regulatory bodies, the media, in each case in accordance with an applicable agreement, *privacy applicable law* or *security applicable law*
    3. Requirement to meet appropriate deadlines required by *privacy applicable law* or *security applicable law*
    4. The third parties' privacy and security event communications procedures contain the requirements specified in the *service provider's* privacy and security event communications procedures
c. For each item in the sample, report the *attributes* listed in step a not found in the privacy and security event communication procedures and where privacy and security event communication procedures do not exist.

Industry Relevance:
US State Breach Laws, US Red Flags Rules, HITECH/ARRA
SIG 5.0: P.40, P.46

**Denotes non-core procedure to be used when appropriate according to the industry verticals a service provider serves and/or the specific services offered.*

X. Glossary

Term	Definition
Acceptable Use Policy	Part of the information security framework that defines what users are and are not allowed to do with the IT systems of the organization. It should contain a subset of the information security policy and refer users to the full security policy when relevant. It should also clearly define the sanctions applied if a user violates the policy.
Acknowledgement of Acceptable Use	A written attestation from a user of an information system indicating the user's acceptance and willingness to comply with the relevant information systems control policies.
Anti-Tailgating / Anti-Piggybacking Mechanism	Two sets of doors whereby access to the second is not granted until the individual has passed through (and closed) the first, often referred to as a "man trap." A controlled turnstile is also considered an anti-tailgating/piggybacking mechanism.
Asset Classification	The category or type assigned to an asset, derived from the asset classification policy. Asset classifications frequently vary from company to company.
Asset Control Tag	A unique identification number assigned to all inventoried assets.
Attribute	A property or field of a particular object.
Baseline	A benchmark by which subsequent items are measured.
Battery	An electrochemical cell (or enclosed and protected material) that can be charged electrically to provide a static potential for power or released electrical charge when needed.
Biometric Reader	A device that uses measurable biological characteristics such as fingerprints or iris patterns to assist in authenticating a person to an electronic system.
Business Continuity Plan (BCP)	A process that defines exactly how, for which applications, and for how long a business plans to continue functioning after a disruptive event. The business continuity plan is usually an overarching plan that includes both operational and technology-related tasks.
Business Impact Analysis (BIA)	This term is applicable across Technology Risk Management, in both information security and business continuity planning domains. An impact analysis results in the differentiation between critical and non-critical business functions. A function may be considered critical if there is an unacceptable impact to stakeholders from damage to the function. The perception of the acceptability of disruption may be modified by the cost of establishing and maintaining appropriate business or technical recovery solutions. A function may also be considered critical if dictated by law.
Business Process	An end-to-end service made available to internal or external parties that usually corresponds to standard service products that the Service Provider offers to clients.

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 name of the person initiating the change - The system affected by the change - A description of the change, including 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
Climate Control System	A combination of sensors and equipment that monitors the temperature and humidity in a sensitive environment (such as a data center) and that automatically heats/cools/dehumidifies as needed to keep the atmosphere within acceptable tolerances.
Cold Site	A remote facility that provides the equipment necessary for data and process restoration.
Communications Plan	A tool for communicating information on the considerations and implications of business continuity within the organization used to improve decision making.
Complex Password	A password that combines alphabetic and non-alphabetic characters, such as special or numeric characters.
Confidentiality	The protection of sensitive information from unauthorized disclosure and sensitive facilities due to physical, technical, or electronic penetration or exploitation.
Constituent	An active employee or contractor.
Contractor	A contracted professional with expertise in a particular domain or area.
Data Controller	Any person (including a public authority, agency or any other body) which alone or jointly with others determines the purposes and means of processing Target Privacy Data (EU Directive).
Data Flow	A flow describing and/or depicting the Target Privacy Data for a given Data Subject for a given country or jurisdiction. The data flow defines the Target Privacy Data and the Protected Target Privacy Data collected, stored, used, accessed, shared, transferred across borders of the country or jurisdiction that are secured, retained and retired.
Data Processor	Any person (including a public authority, agency or any other body) that processes Target Privacy Data on behalf of the Data Controller (EU Directive).
Data Subject	Any person who can be identified, directly or indirectly, by information that identifies one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity. In certain countries (such as Austria, Luxembourg and Italy) this also includes information concerning legal entities/corporations.

Data Subject Category	Includes, for example, employees, clients, business partners, customers, or users.
Decision Making Process Flows	A diagram that illustrates what information is used by whom to make what decisions at what frequency that includes a statement of who is responsible, accountable, consulted and informed. The decision making process flow includes ensuring decisions have been implemented, including any corrective action required to achieve the business objective.
Demilitarized Zone (DMZ)	A controlled network space, delimited by firewalls or other policy-enforcing devices, which is neither inside an organization's network nor directly part of the Internet. A DMZ is typically used to isolate an organization's most highly secured information assets while allowing predefined access to those assets that must provide or receive data outside of the organization. The access and services provided should be restricted to the absolute minimum required.
Enclosed	Closed in, surrounded, or included within.
Exception	A result that deviates from the norm or expectation.
External Vulnerability Scan	A systematic review process executed from a network address outside of the target network that uses software tools designed to search for and map systems for weaknesses in an application, computer or network. The intent is to determine if there are points of weakness in the security control system that can be exploited from outside the network.
Externally Facing	The network entry point that receives inbound traffic.
Extranet	An intranet that is partially accessible to authorized outsiders.
Facility	A structure or building, or multiple structures or buildings, in which 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.
Fire Suppression System	A combination of sensors and equipment designed to detect the presence of heat/smoke/fire and actuate a fire retardant or fire extinguishing system.
Firewall	A set of related programs, located at a network gateway server, that protects the resources of private networks from other networks. Firewalls may be application/proxy, packet-filtering, or stateful-based. Examples of firewalls are Cisco PIX, Check Point Firewall, Juniper NetScreen and Cyberguard. (Though they contain some firewall functionality, routers are not included in this definition.)
Firewall Rule	Information added to the firewall configuration to define the organization's security policy through conditional statements that tell the firewall how to react in a particular situation.
Fluid Sensor	A mechanical device that is sensitive to the presence of water or moisture that transmits a signal to a measuring or control instrument.

Gateway	A node on a network that facilitates the communication of information between two or more nodes.
General Perimeter	An 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.
Generator	A device that converts mechanical energy to electrical energy via an engine (usually fuel-powered) that provides electrical current as input to a power source.
Hardware Systems	Includes servers and network devices.
Heat Detector	A mechanical device that is sensitive to temperature and transmits a signal to a measuring or control instrument.
Hot Site	A duplicate of an organization's original site, with full computer systems and near-complete backups of user data.
Immediate Perimeter	A rack or cage that houses the target systems.
Incident	Events outside normal operations that disrupt normal operational processes. An incident can be a relatively minor event, such as running out of disk space on a server, or a major disruption, such as a breach of database security and the loss of private and confidential customer information.
Incident Severity	A ranking of an event's significance that uses, at a minimum, a three-point scale: minor, moderately severe, and severe. For each level of severity, IT organizations should define acceptable resolution times, escalation procedures, and reporting procedures.
Intermediate Distribution Frame (IDF)	A free-standing or wall-mounted rack for managing and interconnecting the telecommunications cable between end user devices and a main distribution frame (MDF).
Internal Vulnerability Scan	A systematic review process using software tools designed to search for and map systems for weaknesses in an application, computer or network, executed from a network address within the target network. Internal vulnerability scans are used to determine whether points of weakness in the security control system exist that could be exploited by a user with access to the internal network.
Internet	A global network connecting millions of computers. More than 100 countries are linked into exchanges of data, news and opinions.
Internet Protocol (IP)	A networking standard that allows messages to be sent back and forth over the Internet or other IP networks.
Intranet	An IP network that resides behind a firewall and is accessible only to people who are members of the same organization.

Intrusion Detection Systems (IDS)	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.
Intrusion Protection System (IPS)	A more sophisticated Intrusion Detection System (IDS) that allows administrators to configure predefined actions to be taken if suspicious activity is detected.
Inventory	An itemized list of current assets.
Local Backup	A method for backing up data on the local system. For example, an attached tape or storage device.
Main Distribution Frame	A wiring rack that connects outside lines with internal lines. Main distribution frames are used to connect public or private lines entering the building to the organization's internal networks
Map of Dependencies	A diagram that illustrates how a business process relates to its supporting capabilities. ("Supporting capabilities" include: people involved in the delivery of the business process, application software, middleware software, servers, storage, networking, physical facilities, and people involved in the IT and physical infrastructure management.)
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: - Reference to a CIR - Date submitted - Date of change - Name of affected system - Approval status (approved or rejected)
MD5	A one-way cryptographic hash algorithm that produces a unique 128-bit alphanumeric fingerprint of its input.
Mobile Code	Software code that is transferred from one computer to another and that executes automatically. Examples of mobile code include scripts (JavaScript, VBScript), Java applets, ActiveX controls, Flash animations, Shockwave movies (and Xtras), and macros embedded in Microsoft Office documents.
Modem	A device that allows a computer or terminal to transmit data over an analog telephone line.
Network Address Translation (NAT)	A process of rewriting the source and/or destination addresses of IP packets as they pass through a network device.
Network Devices	Units that mediate data in a computer network. Computer networking devices are also called network equipment, Intermediate Systems (IS) or InterWorking Unit (IWU).

Network Segment	A portion of a computer network that is separated from the remainder of the network by a device such as a repeater, hub, bridge, switch or router. Each segment may contain one or multiple computers or other hosts. Network segments are typically established for throughput and/or security reasons.
Network time protocol (NTP)	A protocol designed to synchronize the clocks of computers over a network.
Node	Any physical device with a unique network address.
Non-Employees	Auditors, consultants, contractors, and vendors.
Non-Public Information	Any personally identifiable or company proprietary information that is not publicly available. Non-Public Information includes but is not limited to: certain company proprietary information, such as internal policies and memorandums; and personal information such as an individual's name, address or telephone number. It also includes information requiring higher levels of protection according to the company's security policy, such as company proprietary trade secrets or personal information that bundles an individual's name, address or telephone number with a Social Security number, driver's license number, account number, credit or debit card number, personal identification number, health information, religious opinions or a user ID or password.
Non-Public Personal Information (NPPI)	Any personally identifiable financial information that is not publicly available. Non-Public Personal 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.
Notice Consent Language	Any Data Subject consent language in a Privacy Notice to be accepted by a Data Subject (expressly or by implication). The language may relate to consent to the entire Privacy Notice or to particular uses of the Target Privacy Data where a Data Subject's non-consent to this use of the Target Privacy Data results in a Data Subject rejecting the Privacy Notice. Examples of uses include cross-border transfer of Target Privacy Data, special use of the Target Privacy Data, or special local regulatory requirements.
Owner	An individual or entity that has approved management responsibility for controlling the production, development, maintenance, use and security of the assets. Ownership is not an indication of property rights to the asset.
Ownership	A formally assigned responsibility for a given asset.
Permission	Any Data Subject permission (opt in or opt out) required to use or share Target Privacy Data that can be easily switched on and off, including for the following purposes: marketing; affiliate sharing; product use; promotions; newsletters; tailoring services to Data Subject's particular requirements; behavioral and purchasing patterns; social networking; and professional networking, excluding Notice Consent Language.

Personal Identification Number (PIN)	A secret shared between a user and a system that can be used to authenticate the user to the system.
Physical Media	Any portable device or substance (e.g., paper) used to store data for specific and legitimate purposes. Examples of physical media include: - 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
Port Scan	A systematic scan of a computer's ports that identifies open doors. Used in managing networks, port scanning also can be used maliciously to find a weakened access point from which to break into computer.
Post-Deployment Test Document	A document that provides evidence that the change was tested and approved in the production environment. The document must contain: - Reference to a CIR - Identified deployment resources - Deployment start date - Deployment end date - Expected results - Actual results - Approval signature - Approval date
Power Redundancy	Any type of power delivery mechanism that provides continuous power to connected systems in the event of a failure in the main delivery mechanism for electricity. Such mechanisms include multiple electric feeds, automatic failover generators, and uninterruptible power supplies.
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. A pre-deployment test document is inspected for: - Reference to a CIR - Identified testing resources - Testing start date - Testing end date - Expected test results - Actual test results
Privacy Applicable Law	Relevant laws, enactments, regulations, binding industry codes, regulatory permits and licenses that are in effect and address the protection, handling and privacy of Target Privacy Data, selected as being in scope by the Service Provider or Client.

Privacy Inventory Flow	The most current Target Privacy Data inventory/list and flow by Data Subject Category that has been approved by management of the organization. A privacy inventory flow identifies the ownership of the Target Privacy Data, its sources, collection methods, storage locations, uses (by who, where and for what purpose), sharing within the Service Provider and among its Third Parties, trans-border flows and adequacy mechanisms chosen to ensure the protection of such Target Privacy Data, security, retention and deletion schedules and mechanisms.
Privacy Notice	Notice given to Data Subjects on the collection, use, storage, sharing, transfer, retention and destruction of their Target Privacy Data in accordance with Privacy Applicable Law and organization policy.
Privacy Policy	An organization's internal policy adopted for the life cycle of the Target Privacy Data.
Protected Target Data	Target Data or any other data that requires a higher level of protection or special treatment due to its sensitivity under: Security Applicable Law; company security policy; and/or as identified in the Scope Definition of Protected Target Data of the Shared Assessments Standardized Information Gathering Questionnaire (SIG) and Agreed Upon Procedures (AUP). This may include: Target Data, such as name, address or telephone number in conjunction with Social Security number, driver's license number, account number, credit or debit card number, personal identification number, user ID or password; an individual's health information; company trade secrets or certain confidential information. For data that falls under the definitions of both Target Data and Protected Target Data, (for example, credit card details).
Protected Target Privacy Data	Any Target Privacy Data required to have a higher level of protection or special treatment under Privacy Applicable Law due to its sensitivity, e.g., encryption. This includes EU "sensitive personal data" (health, religion, criminal records, trade union membership, sexual orientation and race). In the US, Protected Target Privacy Data includes name, address or telephone number in conjunction with Social Security number, driver's license number, account number, credit or debit card number, personal identification number, or user ID or password
Protocol	A set of rules and formats that enable the proper exchange of information between different systems.
Publicly Accessible	In networking terms, able to accept a connection originating from the public domain, e.g., the Internet.
Raised Floor	Used in data center construction, a raised floor above the "true" floor allows air conditioning flow and wiring to pass freely under equipment. The space between the true and raised floors is accessed by removable floor tiles.
Receiver Company	The organization that has contracted with a service provider for a specific service.
Residual Risk Rating Scoring Method	A calculation of the risk that remains after security controls have been applied.

Risk Prioritization Scoring Method	A systematic approach that quantifies risk in terms of loss potential, then sequences individual risks to determine the order in which compensating controls should be implemented.
Scoping Meeting	A meeting held prior to commencement of a Shared Assessments engagement, to determine the target systems to be included in a company's Standardized Information Gathering Questionnaire (SIG) and Agreed Upon Procedures (AUP) assessment.
Secure Perimeter	A space fully enclosed by walls that surround the immediate perimeter and that extend from floor to ceiling (beyond raised floors and ceilings), which is contained, and whose points of entry are secured.
Secure Socket Layer (SSL)	A protocol developed by Netscape for transmitting private documents via the Internet. SSL uses a cryptographic system with 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.
Secure Workspace	An environment from where people work from their desks with the purpose of accessing, editing or inputting Target Data on a computer, telephone or physical media, e.g., a BPO or call center environment.
Secure Workspace Perimeter	A space fully enclosed by walls that surround the Secure Workspace which is contained, and whose points of entry and exit are secured.
Security Applicable Law	Applicable laws, enactments, regulations, binding industry codes, regulatory permits and licenses which are in effect that address the protection, handling and security of Target Data and Protected Target Data and that are determined to be in scope by the Service Provider or Client at the scoping of the engagement.
Security Policy	A published document or set of documents 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.
Server	A computer that makes services, such as access to data files, programs, and peripheral devices, available to workstations on a network.
Service Provider	An organization that provides outsourced services, such as data processing, business operations, applications, systems or staffing.
Service Set Identifier (SSID)	A 32-character unique identifier attached to the header of packets sent over a wide area network to identify each packet as part of that network.
Simple Mail Transfer Protocol (SMTP)	The de facto standard for email transmissions across the Internet.
Smoke Detector	A mechanical device that is sensitive to the presence of smoke or particulate material in the air that transmits a signal to a measuring or control instrument.

Status Change	Change to employment status that is recorded by human resources, such as promotions, demotions or departmental changes.
Stewardship	The act of managing and maintaining a given asset.
System Owner	The business unit that retains financial ownership or decision rights for the business use of the asset.
System Steward	The primary assigned administrator responsible for maintenance and day-to-day tasks that support the business.
Target Data	A client's Non-Public Personal Information (NPPI), Protected Health Information (PHI), Personal Information (PI) or Non-Public Information that is stored, transmitted or processed by the Service Provider. Target Data may also include any data selected as being in scope by the Service Provider or Client at the scoping of the engagement. Any reference to Target Data includes Protected Target Data, where applicable.
Target Privacy Data	Any information relating to a Data Subject, who can be identified, directly or indirectly, by that information and in particular by reference to an identification number or to one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity. Examples of Target Privacy Data include name, address, telephone number, and email address. Target Privacy Data may exist in any media or format. Any reference to Target Privacy Data includes Protected Target Privacy Data, where applicable.
Target System	Computer hardware and software in scope for the engagement that contains target data.
Third Party	All entities or persons that work on behalf of the organization but are not its employees, including consultants, contingent workers, clients, business partners, service providers, subcontractors, vendors, suppliers, affiliates and any other person or entity that accesses Target Privacy Data.
Threat Impact Calculation Method	A systematic method of determining the loss potential of a particular threat, based on the value of assets affected.
Threat Probability Calculation Method	A systematic method of determining the potential for a particular threat to occur, based on the likelihood of the occurrence collected from internal staff, past records, and official security records. Threats x Vulnerability x Asset Value = Total Risk (Threats x Vulnerability x Asset Value) x Controls Gap = Residual Risk
Token	A unique identifier generated on both a host and small, user-held device that allows the user to authenticate to the host.
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.
Unidentified	Being or having an unknown or unnamed source.
Uninterruptible Power Supply (UPS)	A power supply consisting of a bank of batteries, which is continually charged. When power fails, the UPS becomes the source of electrical current for computer equipment until the batteries are discharged. A UPS is often connected to a generator that can provide electrical power indefinitely.
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.
Virtual Private Network (VPN)	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.
Volumetric Alarm Sensor	An alarm sensor designed and employed to detect an unauthorized person in a confined space when the space is normally unoccupied. Such alarms include ultrasonic, microwave, and infrared sensors.
War Walk	Also known as "war drive," using a laptop to "sniff" for wireless access points. War walking may be used to locate a public access point for personal use or as a controls assessment to identify access points that are inadequately secured and may indicate an elevated risk of breach.
Warm Site	A remote facility which replicates production data in set intervals.
Water Sensor	A mechanical device sensitive to the presence of water or moisture that transmits a signal to a measuring or control instrument.
Workstation	(1) Single-user computers typically linked together to form a local area network, that can also be used as standalone systems. (2) In networking, any computer connected to a local area network, including a workstation or personal computer.

Y. Sampling Parameters

Population	Sample Size
X > 300	30
2 < X < 300	The greater of 10% or 3
X < 3	All

Z. Practitioners' Notes

Procedures that require additional technical guidance refer to the Practitioners' Notes section. The specific guidance for each of these procedures is outlined below.

AUP users should understand that:

- These procedures were written with the assumption that *network devices* have been documented at the scoping level; and
- It is highly recommended that practitioners utilize the *service provider's* staff to perform the technical procedures; the practitioner's role should be limited to viewing and compiling the results of the AUP assessment. (When applicable, steps may be performed online or through use of hard copy obtained from the *service provider*.)

G.2 Network Management – Encrypted Authentication Credentials
The main *network devices* typically deployed are Cisco devices, which use similar common commands across network platforms.

Cisco
1) Log on to device.
2) Execute the command:
1) PIX# *show run; or*
2) 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) website at www.rfc-archive.org or the respective vendor website to determine whether encryption is enabled.*