Global Information Assurance Certification Paper

A Practical Guide to Auditing an ASP

GSNA Certification Practical Assignment version 3.1, Option 2

Written by Josie Ollinger

March 22, 2005

Abstract

Auditing an Application Service Provider (ASP) can be a difficult and arduous task for the auditor and auditee alike. Since ASPs service such a wide variety of businesses there may be several regulations that an ASP may be audited against. Additionally, depending on the number and types of customers the ASP entertains, the quantity of requested audits can virtually be boundless.

Currently there are no "how-tos" or publications on auditing an ASP. Therefore, in this assignment I plan to provide a clear and practical guide on how to audit an ASP. This guide will first define what an ASP is and provide a brief history on the ASP market. Next, the guide will document the actual approach or method of auditing an ASP. This method will contain information on how to research the targeted ASP, determine the audit scope (which due to the environment can be a difficult task), complete the risk assessment, develop controls that encompass the numerous standards, map the controls to regulations, create a checklist, conduct the actual audit, and finally generate a report.

This guide will truly benefit the security community and auditors, as it will provide a clear set of controls mapped to regulations and tools for testing those controls, which is something that the industry is sincerely lacking.

To avoid confusion, this document will be written as if an independent auditor was hired to audit the client's ASP; however the same methodology can be used by an internal auditor as well. It can also be used as a guide for the ASP's internal auditing department.

I. Introduction

Some businesses often struggle with affordability and management of their own Information Technology infrastructure and applications. Application Service Providers (ASPs) allow those businesses to abandon old beliefs that IT must be provided "in house" by offering them an outsourced solution to many of their IT predicaments. ASPs eliminate the need for businesses to manage their own applications, which require infrastructure, servers, software licensing and headcount. This appeals to many businesses because of the reduced cost burden. ASPs have the dynamic and routinized ability to provide cost-effective solutions which include: software, infrastructure, servers, applications, development, security, management, support and service. ASPs can provide these services over the internet with the scalability and customization needed to appeal to many business sizes and types. In essence, ASPs take on the role of the IT department while allowing the entity to focus on their core business strategies.

ASP-like offerings first surfaced in the 1960's. During that time period, companies like IBM and GE offered hardware and software support to businesses that were unable to afford to service their own computing software and/or hardware. This was called “time-sharing” and allowed the customers to connect to a mainframe in order to access their software applications. The advent and the popularization of the internet greatly facilitated the ability and growth of ASPs so by the late 1990's, ASPs evolved and established themselves as strong competitors in the market space.

Due to their potential for substantial growth, ASPs were considered a trend during the “technology bubble” of the late 90s. After the "technology bubble" burst, only the ASPs with a strong business model survived. According to ASPnews.com, "by 2002/2003, the ASP market seemed all but dead, with a whopping 90 percent failure rate, according to industry analysts."[1] The more business-savvy and time-tested ASPs have emerged from fad status and are now considered sources of viable technological solutions. Today, many ASPs offer Business Process Outsourcing (BPO) solutions that provide back office applications such as accounting, finance, human resources, and procurement. Examples of such applications include Enterprise Resource Planning (ERP), System Application Products (SAP), Customer Relationship Management (CRM), as well as e-commerce applications messaging, database, web hosting...

II. Method

The instructions below will provide the auditor with the guidance necessary regarding the following:

- researching the ASP through the use of questionnaires,
- using standards, regulations and guidelines in determining the scope of the audit,
- identifying which systems need to be audited,
- conducting the risk assessment,
- developing a checklist,
- conducting the audit,
- testing and gathering evidence by using various tools,
- and reporting on the findings.

This guide contains several modifiable items such as an example risk assessment and a checklist for the auditor's own use. It also contains some recommended references and tools that if used, will greatly benefit the auditor.

A. Researching your ASP

Several tasks must be completed by the auditor prior to entering into the ASP audit. Reconnaissance must be completed not only on the ASP but on the hiring customer as well. This preliminary research will help the auditor determine the scope. The customer's type of business and their needs should determine the type of audit that will be performed. For example if the business is a clinical trials organization, the scope of the audit may incorporate tests against HIPAA or 21CFR11 controls. (*These standards are explained in the Standards and Regulations section.)*

Presently, many businesses are finding themselves having to conform to regulations such as HIPAA, Graham Leach Bliley Act (GLB Act), Payment Card Industry (PCI) Data Security Standard, and Sarbanes Oxley (SOX). Auditors should familiarize themselves with the numerous regulations and research what types of businesses are required to conform and what are the deadlines if applicable.

In summary, becoming familiar with the type of business the requester has, and what type of their data is handled by the ASP are critical elements in assessing the requester's needs. For example, "Is the business a public, non-profit or private company?" The answer to that question will help the auditor determine if the business has to comply with section 404 of Sarbanes-Oxley. It is recommended that this type of research be done prior to determining the scope of the audit but can also be accomplished by filling out the Pre-Audit Questionnaire in the *Determining Scope* section below.

B. Determining Scope

Clearly, the client who requested the audit of the ASP has an objective for the audit. Prior to the entrance conference with the client/ASP, the client's reasons for requesting the audit must be ascertained which will help the auditor to determine the type of audit that is to be performed and its scope. The scope of the audit could be merely a vulnerability assessment on a system or it could be a more time consuming conformance audit of all their controls. The reasons that the customer would request an audit could be for compliance reasons; or perhaps they are assessing a potential ASP and would like to audit them prior to signing on the dotted line. In any case, the objective of the audit should be established prior to determining the scope thus keeping the auditor and their client on the "same page".

After preliminary research and outlining an audit objective, the overall scope of the audit should be determined. The auditor should send both the client and the ASP a general pre-audit questionnaire to assist in this effort. The pre-audit questionnaires will help to facilitate the direction of the audit. Some of the questions can and should be answered prior to the entrance conference by the auditor through simple reconnaissance measures (ie. Web searches). The questions that the auditor can't answer will need to be answered by the client and the ASP. The questions should be general in nature leaving the specific material related questions for the actual audit. The questionnaires should also be comprehensive and, depending on the audit objective(s) of the client, they should incorporate most of the following subjects provided in Table B.1: Pre-Audit Questionnaire.

Table B.1: Pre-Audit Questionnaire

Topics	Description	Client	ASP
Company Name	What is the name of the company?	✔	✔
Contact Person(s)	Who is the contact person for the audit?	✔	✔
Contact Info	What is the contact person's information?	✔	✔
Dates of Audit	What are some preliminary dates of the audit? When would the client like audit completed by?	✔	

Onsite Visit Date Preferences	***Client –*** There should be a face-to-face meeting with the client but this can also be done via phone, although not preferred. This meeting's purpose would be to review the prepared scope and to answer any preliminary questions prior to meeting with the ASP. ***ASP*** - Provide some dates for the auditor to come on site to view documentation, review controls, perform tests and review any outstanding items.	✔	✔
Type of Audit	This should be determined prior to the engagement. For consistency purposes, it would be beneficial to include this in the questionnaire to prevent a loss of focus.	✔	
Audit Objectives	This is a chance for the client to clearly state the intentions of the audit.	✔	
Type of Business	This can be researched prior to sending the questionnaire. This will help to define the audit, especially if there are any regulations that the type of business would dictate compliance with. (I.e. Widget's manufacturer)	✔	
Is the business Public, Non-Profit or Private?	This can also be researched prior to the questionnaire. This helps to determine what types of regulations apply.	✔	
End of fiscal year?	This helps the auditor determine if there are any deadlines.	✔	
Age of business	The auditor can research this prior to sending the questionnaire. This may also provide background on the ASP such as to mergers with other ASP's, how old their processes/procedures are…		✔

Size of business	How large is the ASP? Does the ASP have a number of other reputable clients?		✔
List of services provided to the client	***Client*** - What types of services does the ASP provide? This is a very important question in that it will help to determine the scope of the audit as well. Are there any Service Level Agreements (SLA's) in place? Can the SLA be reviewed? ***ASP*** – What types of services does the ASP provide to the customer requesting the audit? Are there any SLA's in place? Can the SLA be reviewed?	✔	✔
List of Systems and Their Function	Obtaining a list from both parties will help to ensure consistency. Upon obtaining the list, the auditor should check for any inconsistencies and inform the customer. ***Client*** – Provide a list of systems names, the system's function, IP addresses that the ASP is responsible for. Provide a list of what is the auditable entity. (What is the auditor responsible for.) ***ASP*** – Provide a list of the client's systems, their function and their associated IP addresses.	✔	✔
System OS	A list of each system's OS will be needed to determine scope and testing.		✔
Applications on Systems	A list of each client system's applications will be needed to determine scope and testing.		✔

Network Topology	Is the client's environment a shared service or dedicated service model? Is any part of the infrastructure shared? Are applications shared or are clients in their own segregated environment with their own individualized systems? The ASP should be able to provide network drawings pertaining to the client environment.		✔
Number of firewalls	Do customers share or have dedicated firewalls? How many firewalls are used in the client environment?		✔
Firewall OS/Application	What types of firewalls are used? What software types of software/hardware is used? What are the version levels?		✔
Firewall Policy	Is a copy of the firewall configuration/ruleset available for review?		✔
Intrusion Detection	Is IDS used? What type is used in the client environment (HBIDS? NIDS? Both?) What software/hardware is used? What version levels?		✔
Policies	What types of policies are in place? Are those policies available for review?		✔
DR/BCP	Is there a Business Continuity Plan or Disaster Recovery Plan? If so will this be available for review? Is it client specific or is it for infrastructure only?		✔
Procedures	What types of procedures exist? Are they available for review?		✔
Contracts	Are service contracts available for review?		✔
QA/Audit Department/Third Party Audits	Is there an internal audit or QA department? If so what are they responsible for? Is a third party audit performed?		✔

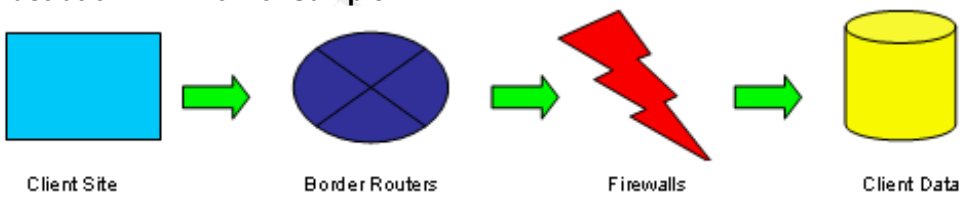
Certifications	Does the organization hold any certifications such as ISO9000, SAS70 Type I, Type II or SysTrust?		✔

Other questions not listed can be added to the Pre-Audit Questionnaire above. It is completely modifiable. Some questions may be omitted however, it is imperative for the auditor to get as much information up front so the on-site visit goes as smoothly as possible. A comprehensive Pre-Audit questionnaire is highly beneficial to all parties and can save the auditor embarrassment during the audit. The Pre-Audit Questionnaire will help arm the auditor with the right tools for the actual audit.

Determining what is Beyond Scope

Perhaps the most important answer to the questionnaire above refers to the audit objective(s). As with any audit, the audit objective will help the auditor stay in scope. When working with an ASP, it is the auditor's responsibility to limit the scope enough so that the audit is not burdensome, while ensuring that the sample reflects the customer's environment. It is important for the auditor to keep the client expectations intact as well. Auditing an entire ASP environment is not a likely or realistic expectation. When an auditor agrees to audit a client's ASP, it is essential for the auditor to establish a sample that models the client's environment. The obvious portion of that sample would be the client's systems hosted at the ASP. Determining what else needs to be added to that list can be complicated. It is suggested that the auditor start at the ASP's perimeter and work inward towards the client systems at the ASP, keeping the audit objective in mind the entire time. The auditor must then choose critical systems along the way to audit such as border routers, border firewalls, firewalls or routers, and switches pertaining to the client.

Illustration B.1: Flow of Sample:



In the table below some guidelines in determining what is in scope and what is beyond scope have been provided.

Table B.2: Determining Scope

In Scope	Beyond Scope

Strict adherence to the objectives of hiring client.	Objective not enumerated by the hiring client. (As stated previously due to the nature of the ASP the scope can get immense so it is the auditor's job to keep the hiring client's objectives in mind and not lose focus!)
Random sampling of client's servers. Depending on the client, the auditor should choose a sample that represents the client's environment. (Web server, application server, database.)	Every one of the servers listed as having to do with the client, unless the number is manageable.
Routers managed by ASP on client site or routers which provide connectivity to ASP on client site. (One configuration if redundant.)	Routers at client site not managed by ASP that do not provide access to ASP.
Border facing routers at ASP that are in the path to the client environment. (One configuration if redundant.)	All of the ASP routers.
Customer specific firewall. (One configuration if redundant.) If there are no customer specified firewalls then a configuration of a firewall in the path to their environment should be chosen.	All ASP firewalls.
Sampling of systems and applications.	Systems belonging to other customers of the ASP.
Hiring client SLA.	Other customer SLA's.
Policies/Procedures pertaining to client	Other customer specific policies or procedures.

As previously stated, particular regulations may help to drive the scope of the audit, therefore it is important for the auditor to be familiarized with current regulations and how they apply to the client. The section below provides a brief explanation of some of the current regulations.

Using Guidelines, Regulations and Standards

This section will help those auditors that find themselves auditing an ASP to ensure they comply with a regulation such as HIPAA or Sarbanes-Oxley. If particular guidelines, regulations or standards drive the audit, then it is imperative to include this section as part of determining the scope. Prior to reading this guide it should be noted that this document only covers several of the controls found in the regulations 21 CFR 11, Sarbanes-Oxley section 404, and HIPAA. NIST SP 800-26 and NIST SP 800-18 will be referred to as well.

There are several other current regulations and standards listed below that today's auditor should be familiar with, yet they are not included in the scope of this document. Regardless of the reasons for the audit this document can assist the auditor greatly in the understanding that meeting general controls can actually contribute to complying with several of the regulations or standards as described below.

NIST SP 800-26 can be used by internal and external auditors alike. Since an ASP usually has a wide variety customers their internal auditor most likely will have to address several standards. Since the controls are so general and the guide is thorough, it can be used to verify if specific controls in several of the regulations/standards below are met. Also, a company that does business with a ASP may hire an auditor to ensure compliance with the standards their business type defines. This publication will assist those auditors to assess the needs of the client and address the ASPs ability to conform with the regulation/standard that applies to their client.

Table B.3: Guidelines, Regulations and Standards

21CFR11	
What is it?	Title 21 Code of Federal Regulations (21 CFR Part 11) AKA - Electronic Records; Electronic Signatures Act Prior to the electronic age, paper records were passed throughout an organization to obtain signatures. Since then, technology has driven the workplace into a paperless state, thus begging for a regulation that recognizes electronic signatures as being the handwritten equivalent. In 1997, the FDA issued 21 CFR 11 in response to this necessity. Due to the 21 CFR Part 11, electronically signed documents or records can be considered equivalent to hand signatures records if there are specific controls in place as delineated by the FDA.
Who is responsible for conforming?	FDA-regulated industries are responsible for conforming, such as: health-care, pharmaceutical, veterinary, medical, personal care products, food and beverage, etc.
More information	http://www.fda.gov/OHRMS/DOCKETS/98fr/03-4312.pdf
NIST SP 800-26	
What is it?	The National Institute of Standards and Technology (NIST) published a document called Security Self-Assessment Guide for Information Technology Systems. This document contains a list of guidelines, or a set of standards, that an auditor can use to evaluate the security of a particular system. "The control objectives and techniques are abstracted directly from long-standing requirements found in statute, policy, and guidance on security." [2]
Who is responsible for conforming?	This is not a regulation; rather it is a "self assessment guide". The guide is helpful in the government's certification and accreditation processes such as the DoD Information Technology Security Certification & Accreditation Process (DITSCAP) and the National Information Assurance Certification and Accreditation Process (NIACAP). This guide, coupled with the Federal Information Technology (IT) Security Assessment Framework, may be used to assess a current government organization's security program. NIST SP 800-26 can also be helpful in providing supporting controls that help to substantiate the compliance with several of the overall control objectives found in a specified regulation.
More information	http://csrc.nist.gov/publications/nistpubs/800-26/sp800-26.doc
Sarbanes Oxley (SOX, SARBOX)	

What is it?	As a result of several public corporations questionable auditing practices, such as inflating their earnings during 1990's, the Sarbanes-Oxley Act was signed into law. Authored by Senator Paul Sarbanes and Representative Michael Oxley the law was created to protect investors by providing more stringent procedures in accounting and financial reporting. "The Sarbanes-Oxley Act itself is organized into eleven titles, although sections 302, 404, 401, 409, 802 and 906 are the most significant with respect to compliance (Sarbanes Oxley section 404 seems to cause most concern) and internal control." [3] Section 404, titled "Management Assessment of Internal Controls" has several IT-related components such as IT Management and Organization, IT Architecture, Systems Development Lifecycle (SDLC) , Change Management, Access Control, Security, etc. Unfortunately for many companies, the legislation does not give specifics on how to comply with Section 404. There is neither a detailed magic recipe nor a checklist provided. As a result of this, many public companies are in a panic and spending well over their initial SOX budget in fear of non-compliance. Their fear is not unwarranted seeing that there are significant penalties if a company is non-compliant. These penalties include jail time (up to twenty years) and stiff fines. The IT Governance Institute (ITGI) offers a comprehensive guide to Sarbanes-Oxley and can be utilized by auditors to help them understand Section 404 and its requirements. This guide combines the Committee of the Sponsoring Organizations of the Treadway Commission's (COSO) internal framework and *Control Objectives for Information and related Technology* (COBIT). COBIT is further explained in its own section below.
Who is responsible for conforming?	This regulation currently only applies to public companies, however there is talk of extending this to non-profit companies and many states are looking at possibly forming a standard for private organizations. The following quote outlines the timeframes of compliance: "Most public companies must meet the financial reporting and certification mandates for any end of year financial statements filed after November 15th 2004 (amended from June 15th). Smaller companies and foreign companies must meet these mandates for any statements filed after 15th July 2005 (amended from April 15th)." [4]

More information	http://www.aicpa.org/info/birdseye02.htm http://www.sarbanes-oxley-forum.com/ http://www.aicpa.org/info/birdseye02.htm http://www.sox404.biz/ ITGI's guide called the IT Control Objectives for Sarbanes-Oxley can be found at the following address: http://www.isaca.org/Content/ContentGroups/Research1/Deliverables/IT_Control_Objectives_for_Sarbanes-Oxley_7july04.pdf
HIPAA	
What is it?	Passed in 1996, HIPAA or the Health Insurance Portability and Accountability Act's main intention was to set standards to protect health information. The final rule or "Security Rule", which passed in February of 2003, further addressed standards for the security of electronic health information. "Any electronic protected health information, (ePHI), that is received, created, maintained or transmitted by a covered entity must be protected under the security rules." [5] The HIPAA security standard rule is broken down into three subsequent sections: Administrative, Physical and Technical Safeguards. These safeguards cover such areas as: policies, procedures, physical and logical access controls, risk analysis/ management, contingency plans, and audit capabilities.
Who is responsible for conforming?	Anyone who transmits health information in an electronic manner is responsible for complying with this regulation. Specifically, Covered Entities (CEs) such as "health plans, health care clearinghouses or health care providers"[6] must adhere to this regulation. The final rule, referred to as the "Security Rule" will need to be addressed by all CEs by April 21st, 2006. Larger CEs have an earlier deadline of April 21st, 2005. Thereafter, there will be a $100 penalty fee for each violation of non-compliance. In the event of wrongful disclosure, there could be penalties as high as $250,000 and a ten-year prison sentence!
More information	http://www.cms.hhs.gov/hipaa/hipaa2/regulations/security/default.asp
SAS70	

What is it?	A Statement on Auditing Standards No. 70 (SAS70) audit "represents that a service organization has been through an in-depth audit of their control activities, which generally include controls over information technology and related processes."[7] The SAS70 was developed by the American Institute of Certified Public Accountants (AICPA). The AICPA provides guidelines on how to conduct a SAS70 audit and the components that are required to be in the report. There are two types of SAS70 audits/reports; Type I and Type II. A SAS70 Type II audit is more comprehensive in that it tests the organization's stated controls over a specified period of time (six months minimum), whereas a Type I audit does not necessarily require the controls be tested, nor is there a required period of time. There are four elements of the SAS70 report. Section one contains the scope and method of the auditor and the depending on the type of report, the auditor's opinion. This opinion either details material weaknesses found within the overall control objective(s) (Qualified Opinion) or suggests the auditor's findings have led them to believe that all overall control objectives are adequately met (Unqualified Opinion). This section is written by the independent auditor. Both SAS70 Types I and II require this section. Section two contains the service organization's description of controls. This section is the responsibility and must be written by the organization. The AICPA does not provide a checklist of controls; rather it provides standards that should be contained within the organization's description of controls. Both SAS70 Types I and II require this section. Section three is required only for SAS70 Type II. It is an optional section for a Type I report. This section contains overall control objectives, controls that make up those objectives, detailed tests of the aforementioned controls and test results. The auditors are responsible for this section. Section four of the report contains a description of terms, acronyms and other pertinent information. This is not a required section for either type of report.
Who is responsible for conforming?	The SAS70 is not a requirement; therefore there is no mandate for any businesses or organizations to comply. A service organization may choose to disclose their controls and opt to have them tested. By doing so the organization can distribute the report to clients, which could potentially lessen their number of client audits.
More information	www.sas70.com
COBIT	

What is it?	Control Objectives for Information and Related Technology or COBIT is a framework that provides good controls using best practices.
Who is responsible for conforming?	This is used as a reference for auditors, managers of systems and other IT personnel. It is not a regulation therefore no compliance is necessary.
More information	http://www.isaca.org/Template.cfm?Section=COBIT6&Template=/TaggedPage/TaggedPageDisplay.cfm&TPLID=55&ContentID=7981
Payment Card Industry (PCI) Data Security Standard	
What is it?	Due to the increasing rise in identity theft cases and stolen information on line and In order to protect customers and manage their data securely the payment card industry has responded with a general best practices framework called the PCI Data Security Standard. These guidelines when applied correctly will assist in preventing the loss of data integrity and maintain the customer's confidentiality. "The PCI Data Security Standard consists of the following basic requirements supported by more detailed sub-requirements: • Build and Maintain a Secure Network • Protect Cardholder Data • Maintain a Vulnerability Management Program • Implement Strong Access Control Measures • Regularly Monitor and Test Networks • Maintain an Information Security Policy "[8]
Who is responsible for conforming?	The requirements found in the PCI Data Security Standard apply to all members, merchants, and service providers that store, process or transmit cardholder data.
More information	http://usa.visa.com/download/business/accepting_visa/ops_risk_management/cisp_PCI_Data_Security_Standard.pdf https://sdp.mastercardintl.com/pdf/PCD_Manual.pdf
Graham Leach Bliley Act (GLB Act)	
What is it?	The Financial Modernization Act of 1999, or "Gramm-Leach-Bliley Act" (GLB Act), is similar to HIPAA in that it was created to protect consumer information; however it applies to their personal financial information held at financial institutions rather than personal health information.

Who is responsible for conforming?	Several financial related institutions including: banks, securities firms, and insurance companies. Service companies such as: lending, brokering, credit counseling, and financial advisors. Companies that offer the following services: transferring/safeguarding money, preparing individual tax returns, providing residential real estate and settlement, collecting consumer debts, and several other businesses that perform financial related activities. This regulation required all of the affected businesses to comply by July 2001.
More information	http://banking.senate.gov/conf/

Identifying the System(s) to be Audited

After reviewing the results of the initial questionnaire, the auditor can then begin defining the scope. When auditing an ASP, it is important for the auditor to contain the scope given that it can grow quickly and wind up in disarray. For example, if the client has fifteen servers managed by the ASP, it would be too costly and time consuming to audit every server, on top of the entire network infrastructure. Auditing the entire ASP environment would not be manageable; therefore it is recommended that the audit be performed by obtaining a sample of the environment. For example, if the ASP manages fifteen of the client's servers, the auditor should choose a sample that represents the client's environment. (For example: One web server, an application server and two database server.) The audit will then become more manageable and effective by using the sample method. The same situation holds true with infrastructure devices. Auditing the ASP's entire network would be extraordinarily labor-intensive and in most cases a waste of the auditor's resources.

Table B.4: Standards/Regulations/Guidelines Driving Scope If regulations/standards define the overall audit objective then the following systems should be reviewed during the audit:

Standard/Regulation/Guideline	Systems to be Audited
21 CFR 11	Client-specific systems (particularly access controls in place.)
Sarbanes-Oxley Act	Perimeter security devices including router ACL's, firewalls, and IDS. System infrastructure such as firewalls, routers, and switches (access control specific). Client specific systems.

HIPAA	Perimeter security devices including firewall ACL's, firewalls, IDS, and anti-virus. Client specific systems that contain Electronic Protected Health Information (EPHI), focusing on access control, secure storage, audit logs, file integrity, authentication, and encryption.

Using the above methodology and the results of the Pre-Audit Questionnaire, the scope can be determined. The defined scope should be emphasized and revisited throughout the entire audit.

C. Conducting the Risk Assessment

Risk assessment is the process of studying threats and vulnerabilities that could cause loss or inflict damage. The primary goal of completing a risk assessment is to reveal areas where controls or safeguards need to be increased. Particular attention must be placed on the nexus of the degree of the threat with the degree of vulnerability. The steps below briefly explain the risk assessment process which is followed by an example ASP Risk Assessment.

Step I: Evaluating threats.

When conducting a risk assessment the first step is to evaluate threats. Threats are defined as the potential impact or consequences if a vulnerability becomes exploited. The following table addresses how a threat and its capacity to inflict damage are rated.

Table C.1: Threat Capacity

Capacity Rating	Capacity to Inflict Damage
HIGH (>50%)	This threat has a high capacity of inflicting damage.
MEDIUM (10%-50%)	There is a moderate chance of this threat inflicting damage.
LOW (< 10%)	There is a slight chance of this threat inflicting damage.

Threats should be identified and then their capacity to inflict damage should be assessed and assigned a rating using the chart above.

Specific ASP Threats are defined in the Section D – ASP Example Risk Assessment section in this document.

Step II: Identify assets that are affected by identified threats.

The next step is then to identify the critical assets which may be affected by the identified threats. Usually when a risk assessment is conducted, the step of identifying assets is completed prior to identifying threats. However, in this case, the assessment of assets is conducted thereafter. This helps to simplify the assessment and keep it within scope.

Step III: Identify the vulnerabilities.

A vulnerability is defined as a weakness or a flaw. The task in this step is to identify those flaws or weaknesses and to assess their impact on the previously listed threats. The table below outlines the ranking of vulnerabilities and their degree of exposure.

Table C.2: Risk Exposure

Exposure Rating	Degree of Exposure
HIGH (>50%)	There are few or no controls in place, therefore exposure is high.
MEDIUM (10%-50%)	There are some controls in place, therefore the exposure is moderate.
LOW (< 10%)	There are many controls in place, therefore the exposure is minimal.

Step IV: Evaluate Risk.

Risk is measured by looking at both vulnerabilities and threats.

Vulnerability x Threat = Risk Potential (Sans Institute Track 7 – Auditing Networks, Perimeters & Systems – Auditing Principals and Concepts 2004 page 2-34.)

There are many methods of classifying risks. Determining the likelihood that risk will occur is somewhat subjective. For the purposes of this document this table will indicate the following risk rankings:

Table C.3: Risk Potential

Risk Rating	Impact on Assets
HIGH (>50%)	There is a high chance of having a negative or devastating impact on assets.
MEDIUM (10%-50%)	There is a moderate chance of causing a negative or devastating impact on assets.
LOW (< 10%)	There is a slight chance of causing a negative or devastating impact on assets.

Regardless of how the risk is rated, all risks should eventually be addressed. The rating should stress the urgency of addressing the risk. It should not be used as a decisive factor in actually addressing the risk or not, therefore all risks should eventually be addressed or mitigated. It is recommended that if the risk is rated as HIGH then the ASP address the issue immediately, if the risk is rated as MEDIUM the risk be addressed within one month, and if the risk is rated as LOW then the risk be addressed within the next six months.

Step V: Reduce Risk

Risks can be minimized by reducing the vulnerabilities. Although a threat may still exist, without vulnerability there is no risk. Through mitigation and remediation, risk can be reduced. It is the goal of the auditor to identify vulnerabilities and offer recommendations, safeguards, and controls to help curtail risk. Once something is determined to be of risk controls should be suggested in efforts to remediate or mitigate the risk.

D. ASP Example Risk Assessment

Assessing the ASP Threats

As stated previously the auditor should first assess the threats to both the client and the ASP. A threat that is not mitigated or remediated is considered as a warning, in that something potentially damaging or dangerous could occur.

According to NIST Special Publication 800-30, there are three major threat categories; Natural, Environmental and Human. Natural threats are naturally occurring such as tornadoes, ice storms, hurricanes, etc. Environmental threats include HVAC, power-failure, chemical spills, etc. Human Threats are caused by human intervention and can be broken down into two distinct categories: internal and external.

Internal threats come from inside the company such as disgruntled or untrained employees. External threats come from outside the company such as hackers or those that have been previously employed by the company. Both threat types can be either intentional or accidental. This guide will address human threats and touch on environmental threats. Lists of potential environmental and natural threats can be obtained from local and governmental sources and on-

line.

When auditing an ASP, threats should be viewed with the understanding that, not only are there human external threats to the client, but there are threats to the ASP as well. Depending on the client's type of business the intensity of external threats can vary. For example, suppose an ASP has two distinctly different clients. The first subject is a very well known independent credit card issuer called Edison's Incorporated. Edison's Inc. accepts and processes millions of credit card applications a day. The second client is a discount clothing chain called Oscar's Attire. External threats would most likely target Edison's Inc. rather than Oscar's Attire due to the perceived or potential value of the information.

Another factor that the auditor should consider is the political ramifications of the client's name. The client's name alone may also make them more of a target of external, intentional threats. If the name of the company has a stigma which elicits political or social animosity, that entity they may be unknowingly on a target list.

The auditor must also remember to review the type of services rendered from the ASP in order to do a thorough threat assessment. If the customer is a web hosting customer then most likely the "loss of database files" threat won't pertain to them. By following Step I listed in Conducting the Risk Assessment section above, the table below was created. This table provides the auditor a start on defining generalized threats to the client's ASP.

Table D.1: ASP Threats:

Number	Threat Description	Capacity to Inflict Damage
1.	Deletion of client data.	High
2.	Destruction of client data.	High
3.	Exposure or disclosure of client's proprietary information.	High
4.	Unauthorized access to client system(s).	Medium
5.	Loss of connectivity to client's systems.	Low
6.	Denial of Service (DoS) and other attacks on the client's system.	High
7.	Release of malicious code onto client system(s).	High
8.	Theft of client data or customized application.	High

9.	Installation of bad code on client system.	Medium
10.	Denial of Service Attacks or other attacks against ASP or client.	High

Categorizing the ASP's Assets

Categorizing assets for the client is a bit simpler when an ASP is involved. When performing a client audit, the auditor must take into account such assets as infrastructure, equipment, facilities, data, power, etc. It is essential for the auditor to differentiate between client and ASP assets. Since the ASP hosts the client's data and applications, the list of assets that are directly related to the client is limited. Hardware, software, power, etc. are assets of the ASP itself. They are not to be confused with the client's assets. Client assets however, cannot exist without the use of the assets of the ASP.

For example, suppose the client's data, which is determined to be their number one asset, is loaded into an ASP configured and owned database which is installed on an ASP-owned and configured server. If there is risk to the server or the database then there is risk to the client's asset, meaning their data. Therefore, this should be considered in the risk assessment. However, it is important for the auditor to recognize the owners of each asset and to understand the relationship of each. As per Step II of the Risk Assessment, the tables below list several assets owned by the client and those that are owned by the ASP. The following listed assets below have the potential of being vulnerable to risks therefore they should be subject to the ASP risk assessment.

Table D.2: Client Assets

Number	Asset	Asset Description
1.	Data	This is data specific to the client such as proprietary information, information on their customers. If the audit subject pertains to HIPAA then this asset would be described as health information. Data that pertains to a SOX client could be financial, payroll…
2.	Customized Software	These are applications that are specific to the customer.
3.	Availability	Availability of services/applications as contracted to the customer.

Table D.3: ASP Assets

Number	Asset	Asset Description
1.	Customers	Customers equal revenue.
2.	Customer Information	This includes but is not limited to customer related diagrams, build-sheets, configurations, notes, etc.

3.	Proprietary Information	Processes, procedures, contracts, intellectual property, etc.
4.	Customized or Proprietary Software	Software configured for the use of the ASP or built “in house”.
5.	Network Infrastructure	Cabling, circuits, DNS servers, domain controllers…
6.	Hardware	Router, switches, servers, desktops, printers, wireless access points, modems, wireless cards…
7.	Software	OS, Applications, Anti-virus, Anti-spam, licenses, etc.
8.	Physical Security Systems	Biometrics, Badge readers, floor to ceiling cages…
9.	Employees	This includes employees and can include contractors and temporary help as well.
10.	Information Security Systems	Firewalls, Intrusion Detection, Vulnerability scanners
11.	Environmental Control Systems	HVAC, fire suppression
12.	Data Center	The facility or building and grounds.
13.	DR Facility	If applicable a disaster recovery site.
14.	Utilities	Power, water, telephony

Analyzing the ASP’s Vulnerabilities

The success of the ASP depends on keeping its customer data secure, while maintaining confidentiality and integrity. In doing so all vulnerabilities must be minimized or eliminated. A vulnerability is “a flaw or weakness in system security procedures, design, implementation, or internal controls.”[9]

Vulnerabilities must be analyzed to assist in the rating of risk and the identification of mitigating/corrective controls. As per Step III above, a vulnerability table has been created below which encompasses several vulnerabilities that an ASP would likely confront. Exposure is dependent on the controls that are found in place during the audit, therefore they have been left out of the table intentionally. The auditor should assess the exposure during the audit process. For the auditor's clarification the vulnerabilities listed below have been separated into three distinct categories: Administrative, Physical and Technical. The potential impact on the organization is provided for each listed vulnerability.

Table D.4: Administrative Vulnerabilities

Vulnerability	Impact on Assets	Exposure (TBD)
Administrative 1: *Untrained Personnel*	Untrained personnel can result in inadvertent loss of customer data.	
Administrative 2: *Lack of Documented Procedures*	Poor, or lack of documented procedures can result in a loss of cohesiveness within an organization. This could lead to systems being misconfigured.	
Administrative 3: *Poor, or Lack of Documented Policies* .	Documented policies provide the auditor with proof that there are policies in place in their organization. The potential impact of this vulnerability when coupled with another could be devastating to client data.	
Administrative 4: *Deficient Security Awareness Program*	The potential impact of this vulnerability is that employees could fall prey to social engineering tactics, open/download attachments that contain viruses, etc. all of which could threaten the client's data.	
Administrative 5: *No Incident Response Plan*	Events are not handled or addressed, resulting in longer downtime and loss of service. Improper handling of incidents can also result in loss of the ability to obtain forensic information.	
Administrative 6: *No Termination Process*	If a termination process does not exist, disgruntled employees may still have access to facilities or to the client data possibly resulting in loss of client data and services.	
Administrative 7: *No Employment Procedures*	When there are no procedures for hiring new employees, several critical activities such as background, credit and/or reference checks, may not be performed. This can allow for a potential employee who has been subverted by a competitor to steal information from the ASP or client. Additionally, employees may not get adequate training.	

Administrative 8: *Contracts for Services are Inadequate or Outdated*.	Service contracts, such as maintenance contracts for fire equipment, power, generators, etc., that are not in the best interest of the company or are not being met may potentially cause several problems (failure of fire alarms, redundant power supply fails to start...)	
Administrative 9: *Lack of SOD Policies and Procedures.*	The lack of segregating duties could result in untrained personnel having access and could result in the loss of customer data.	
Administrative 10: *Policies are not being enforced.*	Enforcement is critical to the effectiveness of a policy. Policies are meaningless and ineffectual without the proper enforcement. Refer to Administrative Vulnerability 3 in assessing the impact on assets since it is essentially the same.	
Administrative 11: *Quality Records are not Maintained on a Routine Basis*	Quality records such as policies and procedures should be updated on a regular basis to ensure their integrity. When not properly maintained, the lack of awareness of updates to policies or procedures is sure to follow.	

Table D.5: Physical Vulnerabilities

Vulnerability	Impact on Assets	Exposure (TBD)
Physical 1: *Weak or lack of physical access controls to client systems*	If unauthorized access is granted to client systems then there is potential to do great damage to the system or data. Theft of the data or system could result as well.	
Physical 2: *Electronic Media is not Disposed of Properly*	If there are no controls in place for the proper disposal of electronic media, there is a possibility that the data can be restored and stolen.	
Physical 3: *Environmental controls are inadequate.*	Environmental controls such as room temperature or overhead sprinklers can affect the state of the media, therefore altering or destroying the client's data and service.	

Table D.6: Technical Vulnerabilities

Vulnerability	Impact on Assets	Exposure (TBD)

Technical 1: *Applications are Configured Incorrectly*	Poorly configured applications can result in loss or denial of service, loss or exposure of customer data.	
Technical 2: *Operating system configuration not hardened.*	Unhardened systems can lead to compromise, exposure and/or deletion of client data	
Technical 3: *Insufficient change management process.*	Changes to systems that are not tracked can lead to unauthorized, unwanted changes to client application possibly disrupting service.	
Technical 4: *Inadequate logging*	Some standards require that logs contain certain information. By not logging pertinent information, doing effective forensic analysis or troubleshooting may be challenging.	
Technical 5: *Logs can be overwritten or deleted.*	When logs can be overwritten or deleted their integrity is compromised.	
Technical 6: *Logs (audit trail) are not retained for an adequate time period.*	Audit trails are maintained for review and forensic analysis purposes.	
Technical 7: *Client system(s) are not up to date with service packs or patches*	If there is no patch management system in place client data can be compromised by malicious code, internal or external attacks.	
Technical 8: *No IDS is used or signatures on IDS System are Out of Date*	If intrusions are not identified as being potential attacks or mitigated against they may consequentially result in loss, theft or manipulation of customer data.	
Technical 9: *Out of date definition files on AV server/client or lack of AV solution.*	This could devastate the organization by bringing the entire network down, which would cause a loss of service or a possible loss or exposure of client data.	

Technical 10: *Lack of application test environment.*	Poor or bad application code being pushed to production could cause a loss of service.	
Technical 11: *Lack of security on perimeter devices*	Lack of security on perimeter devices such as the use of access lists, strong passwords and configurations, can lead to theft, loss, deletion, corruption of client's data, and/or loss of service.	
Technical 12: *Network device(s) not configured correctly*	Poorly configured network equipment such as routers, switches, VLANs, and PVLANS can result in loss of services.	
Technical 13: *Access controls on client systems are weak*	Unauthorized access could lead to either inadvertent or intentional loss of client data.	
Technical 14: *Weak passwords*	Weak passwords can lead to a compromised system which could expose a client's data.	
Technical 15: *Lack of internal or external audits*	Audits help to minimize vulnerabilities and risks. The lack of internal and external audits could lead to the existence of numerous undiscovered vulnerabilities. The larger number of vulnerabilities the greater the higher the risk of the client's data.	
Technical 16: *Regular backups are not being performed.*	If a restoration of client data is necessary and no backups are performed then the customer's data could potentially be lost.	
Technical 17: *Backup information is not retained for adequate time period.*	Backup information should be retained for an adequate time period. Backup data is usually used mostly for forensic purposes. Not retaining logs for proper period of time can result in loss of forensic capabilities.	

Categorizing the ASP's Risks

Risk can be assessed by using the Risk Potential Table in Step IV, the threats and the vulnerabilities listed above. The risk assessment below provides an example of how risk can be determined and rated. Since the "Exposure" and "likelihood" of each risk has to be ascertained by the auditor during the actual audit process, these have not been filled out intentionally.

Table D.7: Example ASP Risk Assessment

Vulnerability	Threat	Potential Risk(s)	Exposure (TBD)	Capacity to Inflict Damage	Risk Rating (TBD)
Administrative #1*: Untrained Personnel*	#1- Deletion of client data.	▪ Temporary or permanent data loss. ▪ Loss of service/availability. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**HIGH**	
	#2 – Destruction of client data.	▪ Temporary or permanent data loss. ▪ Loss of service/availability. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**HIGH**	

	#3 – Exposure or disclosure of client's proprietary information.	▪ Theft of data. ▪ Extortion. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**HIGH**	
	#5 –Loss of connectivity to client's system(s).	▪ Loss of service/availability. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**LOW**	
	#7 – Release of malicious code onto client systems.	▪ Temporary or permanent data loss. ▪ Loss of service/availability. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**HIGH**	
	#9 - Installation of bad code on client system.	▪ Loss of service/availability. ▪ Loss of reputation. ▪ Financial ramifications.		**MEDIUM**	
Administrative #2: *Lack of Documented Procedures*	#1 - Deletion of client data.	▪ Temporary or permanent data loss. ▪ Loss of service/availability. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**HIGH**	

#2 - Destruction of client data.	▪ Temporary or permanent data loss. ▪ Loss of service/availability. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**HIGH**	
#3 – Exposure or disclosure of client's proprietary information.	▪ Theft of data. ▪ Extortion. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**HIGH**	
#4 - Unauthorized access to client system(s).	▪ Temporary or permanent data loss. ▪ Loss of service/availability. ▪ Theft of data. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**MEDIUM**	
#5 - Loss of connectivity to client's systems.	▪ Loss of service/availability. ▪ Loss of reputation. ▪ Financial ramifications.		**LOW**	

	#6 - Denial of Service (DoS) and other attacks on the client's system.	▪ Temporary or permanent data loss. ▪ Loss of service/availability. ▪ Theft of data. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**HIGH**	
	#7 - Release of malicious code onto client system(s).	▪ Temporary or permanent data loss. ▪ Loss of service/availability. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**HIGH**	
	#8 - Theft of client data or customized application.	▪ Loss of intellectual property. ▪ Extortion. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**HIGH**	
	#9 - Installation of bad code on client system.	▪ Loss of service/availability. ▪ Loss of reputation. ▪ Financial ramifications.		**MEDIUM**	

Administrative: #3 *Poor, or Lack of Documented Policies*	#1 - Deletion of client data.	▪ Temporary or permanent data loss. ▪ Loss of service/availability. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**HIGH**	
	#2 - Destruction of client data.	▪ Temporary or permanent data loss. ▪ Loss of service/availability. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**HIGH**	
	#3 - Exposure or disclosure of client's proprietary information.	▪ Theft of data. ▪ Extortion. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**HIGH**	
	#4 - Unauthorized access to client system(s).	▪ Temporary or permanent data loss. ▪ Loss of service/availability. ▪ Theft of data. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**MEDIUM**	

	#5 - Loss of connectivity to client's systems.	▪ Loss of service/availability. ▪ Loss of reputation. ▪ Financial ramifications.		**MEDIUM**	
	#7 - Release of malicious code onto client system(s).	▪ Temporary or permanent data loss. ▪ Loss of service/availability. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**HIGH**	
	#8 - Theft of client data or customized application.	▪ Loss of intellectual property. ▪ Extortion ▪ Loss of reputation. ▪ Financial and legal ramifications.		**HIGH**	
	#9 - Installation of bad code on client system.	▪ Loss of service/availability. ▪ Loss of reputation. ▪ Financial ramifications.		**MEDIUM**	
Administrative#4: *Deficient Security Awareness Program*	#1 - Deletion of client data.	▪ Temporary or permanent data loss. ▪ Loss of service/availability. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**HIGH**	

#2 - Destruction of client data.	▪ Temporary or permanent data loss. ▪ Loss of service/availability. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**HIGH**	
#3 - Exposure or Disclosure of client's proprietary information.	▪ Theft of data. ▪ Extortion ▪ Loss of reputation. ▪ Financial and legal ramifications.		**HIGH**	
#4 - Unauthorized access to client system(s).	▪ Temporary or permanent data loss. ▪ Loss of service/availability. ▪ Theft of data. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**MEDIUM**	
#5 - Loss of connectivity to client's systems.	▪ Loss of service/availability. ▪ Loss of reputation. ▪ Financial ramifications		**LOW**	

	#7 - Release of malicious code onto client system(s).	▪ Temporary or permanent data loss. ▪ Loss of service/availability. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**HIGH**	
	#8 - Theft of client data or customized application.	▪ Loss of intellectual property. ▪ Extortion. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**HIGH**	
Administrative #5: *No Incident Response Plan*	#1 - Deletion of client data.	▪ Temporary or permanent data loss. ▪ Loss of service/availability. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**HIGH**	
	#2 - Destruction of client data.	▪ Temporary or permanent data loss. ▪ Loss of service/availability. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**HIGH**	

#3 - Exposure or disclosure of client's proprietary information.	▪ Theft of data. ▪ Extortion. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**HIGH**	
#4 - Unauthorized access to client system(s).	▪ Temporary or permanent data loss. ▪ Loss of service/availability. ▪ Theft of data. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**MEDIUM**	
#5 - Loss of connectivity to client's systems.	▪ Loss of service/availability. ▪ Loss of reputation. ▪ Financial ramifications. ▪ Prolonged outage/downtime.		**LOW**	

	#6 - Denial of Service (DoS) and other attacks on the client's system.	▪ Temporary or permanent data loss. ▪ Loss of service/availability. ▪ Theft of data. ▪ Loss of reputation. ▪ Financial and legal ramifications. ▪ Prolonged outage/downtime.		**HIGH**	
	#7 - Release of malicious code onto client system(s).	▪ Temporary or permanent data loss. ▪ Loss of service/availability. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**HIGH**	
	#8 - Theft of client data or customized application.	▪ Loss of intellectual property. ▪ Extortion. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**HIGH**	
	#9 - Installation of bad code on client system.	▪ Loss of service/availability. ▪ Loss of reputation. ▪ Financial ramifications.		**MEDIUM**	

Administrative #6: *No Termination Process*	#1 - Deletion of client data.	▪ Temporary or permanent data loss. ▪ Loss of service/availability. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**HIGH**	
	#2 - Destruction of client data.	▪ Temporary or permanent data loss. ▪ Loss of service/availability. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**HIGH**	
	#3 - Exposure or disclosure of client's proprietary information.	▪ Theft of data. ▪ Extortion. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**HIGH**	
	#4 - Unauthorized access to client system(s).	▪ Temporary or permanent data loss. ▪ Loss of service/availability. ▪ Theft of data. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**MEDIUM**	

	#5 - Loss of connectivity to client's systems.	▪ Loss of service/availability. ▪ Loss of reputation. ▪ Financial ramifications.		**LOW**	
	#6 - Denial of Service (DoS) and other attacks on the client's system.	▪ Temporary or permanent data loss. ▪ Loss of service/availability. ▪ Theft of data. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**HIGH**	
	#7 - Release of malicious code onto client system(s).	▪ Temporary or permanent data loss. ▪ Loss of service/availability. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**HIGH**	
	#8 - Theft of client data or customized application.	▪ Loss of intellectual property. ▪ Extortion. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**HIGH**	

Administrative #7: *No Employment Procedures*	#1 - Deletion of client data.	▪ Temporary or permanent data loss. ▪ Loss of service/availability. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**HIGH**	
	#2 - Destruction of client data.	▪ Temporary or permanent data loss. ▪ Loss of service/availability. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**HIGH**	
	#3 - Exposure or Disclosure of client's proprietary information.	▪ Theft of data. ▪ Extortion ▪ Loss of reputation. ▪ Financial and legal ramifications.		**HIGH**	
	#4 - Unauthorized access to client system(s).	▪ Temporary or permanent data loss. ▪ Loss of service/availability. ▪ Theft of data. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**MEDIUM**	

#5 - Loss of connectivity to client's systems.	▪ Loss of service/availability. ▪ Loss of reputation. ▪ Financial ramifications.		**LOW**	
#6 - Denial of Service (DoS) and other attacks on the client's system.	▪ Temporary or permanent data loss. ▪ Loss of service/availability. ▪ Theft of data. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**HIGH**	
#7 - Release of malicious code onto client system(s).	▪ Temporary or permanent data loss. ▪ Loss of service/availability. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**HIGH**	
#8 - Theft of client data or customized application.	▪ Loss of intellectual property. ▪ Extortion. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**HIGH**	

	#9 - Installation of bad code on client system.	▪ Loss of service/availability. ▪ Loss of reputation. ▪ Financial ramifications.		**MEDIUM**	
Administrative #8: *Contracts for Services are Inadequate or Outdated*.	#1 - Deletion of client data.	▪ Temporary or permanent data loss. ▪ Loss of service/availability. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**HIGH**	
	#2 - Destruction of client data.	▪ Temporary or permanent data loss. ▪ Loss of service/availability. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**HIGH**	
	#3 - Exposure or Disclosure of client's proprietary information.	▪ Theft of data. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**HIGH**	
	#5 - Loss of connectivity to client's systems.	▪ Loss of service/availability. ▪ Loss of reputation. ▪ Financial and legal ramifications		**LOW**	

Administrative #9: *Lack of SOD Policies and Procedures.*	#1 - Deletion of client data.	▪ Temporary or permanent data loss. ▪ Loss of service/availability. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**HIGH**	
	#2 - Destruction of client data.	▪ Temporary or permanent data loss. ▪ Loss of service/availability. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**HIGH**	
	#3 - Exposure or Disclosure of client's proprietary information.	▪ Theft of data. ▪ Extortion. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**HIGH**	
	#4 - Unauthorized access to client system(s).	▪ Temporary or permanent data loss. ▪ Loss of service/availability. ▪ Theft of data. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**MEDIUM**	

	#5 - Loss of connectivity to client's systems.	▪ Loss of service/availability. ▪ Loss of reputation. ▪ Financial ramifications.		**LOW**	
	#9 - Installation of bad code on client system.	▪ Loss of service/availability. ▪ Loss of reputation. ▪ Financial ramifications.		**MEDIUM**	
Administrative #10: *Policies are not being enforced.*	#1 - Deletion of client data.	▪ Temporary or permanent data loss. ▪ Loss of service/availability. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**HIGH**	
	#2 - Destruction of client data.	▪ Temporary or permanent data loss. ▪ Loss of service/availability. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**HIGH**	
	#3 - Exposure or Disclosure of client's proprietary information.	▪ Theft of data. ▪ Extortion. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**HIGH**	

#4 - Unauthorized access to client system(s).	▪ Temporary or permanent data loss. ▪ Loss of service/availability. ▪ Theft of data. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**MEDIUM**	
#5 - Loss of connectivity to client's systems.	▪ Loss of service/availability. ▪ Loss of reputation. ▪ Financial ramifications.		**LOW**	
#7 - Release of malicious code onto client system(s).	▪ Temporary or permanent data loss. ▪ Loss of service/availability. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**HIGH**	
#8 - Theft of client data or customized application.	▪ Loss of intellectual property. ▪ Extortion. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**HIGH**	

	#9 - Installation of bad code on client system.	▪ Loss of service/availability. ▪ Loss of reputation. ▪ Financial ramifications.		**MEDIUM**	
Administrative #11: *Quality Records are not Maintained on a Routine Basis*	#1 - Deletion of client data.	▪ Temporary or permanent data loss. ▪ Loss of service/availability. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**HIGH**	
	#2 - Destruction of client data.	▪ Temporary or permanent data loss. ▪ Loss of service/availability. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**HIGH**	
	#3 - Exposure or Disclosure of client's proprietary information.	▪ Theft of data. ▪ Extortion. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**HIGH**	

#4 - Unauthorized access to client system(s).	▪ Temporary or permanent data loss. ▪ Loss of service/availability. ▪ Theft of data. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**MEDIUM**	
#5 - Loss of connectivity to client's systems.	▪ Loss of service/availability. ▪ Loss of reputation. ▪ Financial ramifications.		**LOW**	
#6 - Denial of Service (DoS) and other attacks on the client's system.	▪ Temporary or permanent data loss. ▪ Loss of service/availability. ▪ Theft of data. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**HIGH**	
#7 - Release of malicious code onto client system(s).	▪ Temporary or permanent data loss. ▪ Loss of service/availability. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**HIGH**	

	#8 - Theft of client data or customized application.	▪ Loss of intellectual property. ▪ Extortion. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**HIGH**	
	#9 - Installation of bad code on client system.	▪ Loss of service/availability. ▪ Loss of reputation. ▪ Financial ramifications.		**MEDIUM**	
Physical #1: *Weak or lack of physical access controls to client systems*	#1 - Deletion of client data.	▪ Temporary or permanent data loss. ▪ Loss of service/availability. ▪ Theft. ▪ Damage to equipment. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**HIGH**	

#2 - Destruction of client data.	▪ Temporary or permanent data loss. ▪ Loss of service/availability. ▪ Theft. ▪ Damage to equipment. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**HIGH**	
#3 - Exposure or Disclosure of client's proprietary information.	▪ Theft of data. ▪ Extortion. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**HIGH**	
#4 - Unauthorized access to client system(s).	▪ Temporary or permanent data loss. ▪ Loss of service/availability. ▪ Theft of data. ▪ Damage to equipment. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**MEDIUM**	

	#5 - Loss of connectivity to client's systems.	▪ Loss of service/availability. ▪ Loss of reputation. ▪ Financial ramifications.		**LOW**	
	#8 - Theft of client data or customized application.	▪ Temporary or permanent data loss. ▪ Extortion. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**HIGH**	
Physical #2: *Electronic Media is not Disposed of Properly*	#3 - Exposure or disclosure of client's proprietary information.	▪ Theft of data. ▪ Extortion. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**HIGH**	
	#8 - Theft of client data or customized application.	▪ Loss of intellectual knowledge. ▪ Loss of proprietary information. ▪ Extortion. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**HIGH**	

Physical # 3: *Environmental controls are inadequate.*	#1 - Deletion of client data.	▪ Temporary or permanent data loss or corruption. ▪ Loss of service/availability. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**HIGH**	
	#2 - Destruction of client data.	▪ Temporary or permanent data loss or corruption. ▪ Loss of service/availability. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**HIGH**	
	#5 - Loss of connectivity to client's systems.	▪ Loss of service/availability. ▪ Loss of reputation. ▪ Financial ramifications.		**LOW**	
Technical # 1: *Applications are Configured Incorrectly*	#1 - Deletion of client data.	▪ Temporary or permanent data loss. ▪ Loss of service/availability. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**HIGH**	

#2 - Destruction of client data.	▪ Temporary or permanent data loss. ▪ Loss of service/availability. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**HIGH**	
#3 - Exposure or Disclosure of client's proprietary information.	▪ Theft of data. ▪ Extortion. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**HIGH**	
#4 - Unauthorized access to client system(s).	▪ Temporary or permanent data loss. ▪ Loss of service/availability. ▪ Theft of data. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**MEDIUM**	
#5 - Loss of connectivity to client's systems.	▪ Loss of service/availability. ▪ Loss of reputation. ▪ Financial ramifications.		**LOW**	

	#8 - Theft of client data or customized application.	▪ Temporary or permanent data loss. ▪ Extortion. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**HIGH**	
Technical # 2: *Operating system configuration not hardened.*	#1 - Deletion of client data.	▪ Temporary or permanent data loss. ▪ Loss of service/availability. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**HIGH**	
	#2 - Destruction of client data.	▪ Temporary or permanent data loss. ▪ Loss of service/availability. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**HIGH**	
	#3 - Exposure or Disclosure of client's proprietary information.	▪ Theft of data. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**HIGH**	

#4 - Unauthorized access to client system(s).	▪ Temporary or permanent data loss. ▪ Loss of service/availability. ▪ Theft of data. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**MEDIUM**	
#5 - Loss of connectivity to client's systems.	▪ Loss of service/availability. ▪ Loss of reputation. ▪ Financial ramifications.		**LOW**	
#6 - Denial of Service (DoS) and other attacks on the client's system.	▪ Temporary or permanent data loss. ▪ Loss of service/availability. ▪ Theft of data. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**HIGH**	
#7 - Release of malicious code onto client system(s).	▪ Temporary or permanent data loss. ▪ Loss of service/availability. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**HIGH**	

	#8 - Theft of client data or customized application.	▪ Temporary or permanent data loss. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**HIGH**	
Technical # 3: *Insufficient change management process.*	#1 - Deletion of client data.	▪ Temporary or permanent data loss. ▪ Loss of service/availability. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**HIGH**	
	#2 - Destruction of client data.	▪ Temporary or permanent data loss. ▪ Loss of service/availability. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**HIGH**	
	#5 - Loss of connectivity to client's systems.	▪ Loss of service/availability. ▪ Loss of reputation. ▪ Financial and legal ramifications		**LOW**	
	#9 - Installation of bad code on client system.	▪ Loss of service/availability. ▪ Loss of reputation. ▪ Financial ramifications.		**MEDIUM**	

Technical # 4: *Inadequate logging*	#1 - Deletion of client data.	▪ Prolonged outage/downtime. ▪ Lack of forensic capability. ▪ Legal ramifications.		**HIGH**	
	#2 - Destruction of client data.	▪ Prolonged outage/downtime. ▪ Lack of forensic capability. ▪ Legal ramifications.		**HIGH**	
	#3 - Exposure or Disclosure of client's proprietary information.	▪ Lack of forensic capability. ▪ Legal ramifications.		**HIGH**	
	#4 - Unauthorized access to client system(s).	▪ Lack of forensic capability. ▪ Legal ramifications.		**MEDIUM**	
	#6 - Denial of Service (DoS) and other attacks on the client's system.	▪ Prolonged outage/downtime. ▪ Lack of forensic capability. ▪ Legal ramifications.		**HIGH**	
	#7 - Release of malicious code onto client system(s).	▪ Prolonged outage/downtime. ▪ Lack of forensic capability. ▪ Legal ramifications.		**HIGH**	

	#8 - Theft of client data or customized application.	▪ Prolonged outage/downtime. ▪ Lack of forensic capability. ▪ Legal ramifications.		**HIGH**	
	#9 - Installation of bad code on client system.	▪ Prolonged outage/downtime. ▪ Lack of forensic capability. ▪ Legal ramifications.		**MEDIUM**	
Technical # 5: *Logs can be overwritten or deleted.*	#1 - Deletion of client data.	▪ Lack of forensic capability. ▪ Legal ramifications.		**HIGH**	
	#2 - Destruction of client data.	▪ Lack of forensic capability. ▪ Legal ramifications.		**HIGH**	
	#3 - Exposure or Disclosure of client's proprietary information.	▪ Lack of forensic capability. ▪ Legal ramifications.		**HIGH**	
	#4 - Unauthorized access to client system(s).	▪ Lack of forensic capability. ▪ Legal ramifications.		**MEDIUM**	
	#6 - Denial of Service (DoS) and other attacks on the client's system.	▪ Lack of forensic capability. ▪ Legal ramifications.		**HIGH**	

	#7 - Release of malicious code onto client system(s).	▪ Lack of forensic capability. ▪ Legal ramifications.		**HIGH**	
	#8 - Theft of client data or customized application.	▪ Lack of forensic capability. ▪ Legal ramifications.		**HIGH**	
	#9 - Installation of bad code on client system.	▪ Lack of forensic capability. ▪ Legal ramifications.		**MEDIUM**	
Technical # 6: *Logs (audit trail) are not retained for an adequate time period.*	#1 - Deletion of client data.	▪ Lack of forensic capability. ▪ Legal ramifications.		**HIGH**	
	#2 - Destruction of client data.	▪ Lack of forensic capability. ▪ Legal ramifications.		**HIGH**	
	#3 - Exposure or Disclosure of client's proprietary information.	▪ Lack of forensic capability. ▪ Legal ramifications.		**HIGH**	
	#4 - Unauthorized access to client system(s).	▪ Lack of forensic capability. ▪ Legal ramifications.		**MEDIUM**	

	#6 - Denial of Service (DoS) and other attacks on the client's system.	▪ Lack of forensic capability. ▪ Legal ramifications.		**HIGH**	
	#7 - Release of malicious code onto client system(s).	▪ Lack of forensic capability. ▪ Legal ramifications.		**HIGH**	
	#8 - Theft of client data or customized application.	▪ Lack of forensic capability. ▪ Legal ramifications.		**HIGH**	
	#9 - Installation of bad code on client system.	▪ Lack of forensic capability. ▪ Legal ramifications.		**MEDIUM**	
Technical # 7: *Client system(s) are not up to date with service packs or patches*	#1 - Deletion of client data.	▪ Temporary or permanent data loss. ▪ Loss of service/availability. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**HIGH**	
	#2 - Destruction of client data.	▪ Temporary or permanent data loss. ▪ Loss of service/availability. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**HIGH**	

#3 - Exposure or Disclosure of client's proprietary information.	▪ Theft of data. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**HIGH**	
#5 - Loss of connectivity to client's systems.	▪ Loss of service/availability. ▪ Loss of reputation. ▪ Financial ramifications.		**LOW**	
#6 - Denial of Service (DoS) and other attacks on the client's system.	▪ Temporary or permanent data loss. ▪ Loss of service/availability. ▪ Theft of data. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**HIGH**	
#7 - Release of malicious code onto client system(s).	▪ Temporary or permanent data loss. ▪ Loss of service/availability. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**HIGH**	

	#8 - Theft of client data or customized application.	▪ Temporary or permanent data loss. ▪ Extortion. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**HIGH**	
Technical # 8: *No IDS is used or signatures on IDS System are Out of Date*	#1 - Deletion of client data.	▪ Prolonged outage/downtime. ▪ Lack of forensic capability. ▪ Legal ramifications.		**HIGH**	
	#2 - Destruction of client data.	▪ Prolonged outage/downtime. ▪ Lack of forensic capability. ▪ Legal ramifications.		**HIGH**	
	#3 - Exposure or Disclosure of client's proprietary information.	▪ Prolonged outage/downtime. ▪ Lack of forensic capability. ▪ Legal ramifications.		**HIGH**	
	#4 - Unauthorized access to client system(s).	▪ Lack of forensic capability. ▪ Legal ramifications.		**MEDIUM**	
	#5 - Loss of connectivity to client's systems.	▪ Prolonged outage/downtime. ▪ Lack of forensic capability. ▪ Legal ramifications.		**LOW**	

	#6 - Denial of Service (DoS) and other attacks on the client's system.	▪ Prolonged outage/downtime. ▪ Lack of forensic capability. ▪ Legal ramifications.		**HIGH**	
	#7 - Release of malicious code onto client system(s).	▪ Prolonged outage/downtime. ▪ Lack of forensic capability. ▪ Legal ramifications.		**HIGH**	
	#8 - Theft of client data or customized application.	▪ Prolonged outage/downtime. ▪ Lack of forensic capability. ▪ Legal ramifications.		**HIGH**	
Technical # 9: *Out of date definition files on AV server/client or lack of AV solution.*	#1 - Deletion of client data.	▪ Temporary or permanent data loss. ▪ Loss of service/availability. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**HIGH**	
	#2 - Destruction of client data.	▪ Temporary or permanent data loss. ▪ Loss of service/availability. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**HIGH**	

	#3 - Exposure or Disclosure of client's proprietary information.	▪ Theft of data. ▪ Extortion. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**HIGH**	
	#5 - Loss of connectivity to client's systems.	▪ Loss of service/availability. ▪ Loss of reputation. ▪ Financial ramifications		**LOW**	
	#7 - Release of malicious code onto client system(s).	▪ Temporary or permanent data loss. ▪ Loss of service/availability. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**HIGH**	
	#8 - Theft of client data or customized application.	▪ Temporary or permanent data loss. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**HIGH**	
Technical # 10: *Lack of application test environment.*	#1 - Deletion of client data.	▪ Temporary or permanent data loss. ▪ Loss of service/availability. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**HIGH**	

	#2 - Destruction of client data.	▪ Temporary or permanent data loss. ▪ Loss of service/availability. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**HIGH**	
	#3 - Exposure or Disclosure of client's proprietary information.	▪ Theft of data. ▪ Extortion. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**HIGH**	
	#5 - Loss of connectivity to client's systems.	▪ Loss of service/availability. ▪ Loss of reputation. ▪ Financial and legal ramifications		**LOW**	
	#9 - Installation of bad code on client system.	▪ Loss of service/availability. ▪ Loss of reputation. ▪ Financial ramifications.		**MEDIUM**	
Technical # 11: *Lack of security on perimeter devices*	#1 - Deletion of client data.	▪ Temporary or permanent data loss. ▪ Loss of service/availability. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**HIGH**	

#2 - Destruction of client data.	▪ Temporary or permanent data loss. ▪ Loss of service/availability. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**HIGH**	
#3 - Exposure or Disclosure of client's proprietary information.	▪ Theft of data. ▪ Extortion. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**HIGH**	
#4 - Unauthorized access to client system(s).	▪ Temporary or permanent data loss. ▪ Loss of service/availability. ▪ Theft of data. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**MEDIUM**	
#5 - Loss of connectivity to client's systems.	▪ Loss of service/availability. ▪ Loss of reputation. ▪ Financial ramifications.		**LOW**	

	#6 - Denial of Service (DoS) and other attacks on the client's system.	▪ Temporary or permanent data loss. ▪ Loss of service/availability. ▪ Theft of data. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**HIGH**	
	#7 - Release of malicious code onto client system(s).	▪ Temporary or permanent data loss. ▪ Loss of service/availability. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**HIGH**	
	#8 - Theft of client data or customized application.	▪ Temporary or permanent data loss. ▪ Extortion. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**HIGH**	
Technical # 12: *Network device(s) not configured correctly*	#1 - Deletion of client data.	▪ Temporary or permanent data loss. ▪ Loss of service/availability. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**HIGH**	

#2 - Destruction of client data.	▪ Temporary or permanent data loss. ▪ Loss of service/availability. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**HIGH**	
#3 - Exposure or Disclosure of client's proprietary information.	▪ Theft of data. ▪ Extortion. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**HIGH**	
#4 - Unauthorized access to client system(s).	▪ Temporary or permanent data loss. ▪ Loss of service/availability. ▪ Theft of data. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**MEDIUM**	
#5 - Loss of connectivity to client's systems.	▪ Loss of service/availability. ▪ Loss of reputation. ▪ Financial ramifications		**LOW**	

	#8 - Theft of client data or customized application.	▪ Temporary or permanent data loss. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**HIGH**	
Technical # 13: *Access controls on client systems are weak*	#1 - Deletion of client data.	▪ Temporary or permanent data loss. ▪ Loss of service/availability. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**HIGH**	
	#2 - Destruction of client data.	▪ Temporary or permanent data loss. ▪ Loss of service/availability. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**HIGH**	
	#3 - Exposure or Disclosure of client's proprietary information.	▪ Theft of data. ▪ Extortion. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**HIGH**	

	#4 - Unauthorized access to client system(s).	▪ Temporary or permanent data loss. ▪ Loss of service/availability. ▪ Theft of data. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**MEDIUM**	
	#8 - Theft of client data or customized application.	▪ Temporary or permanent data loss. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**HIGH**	
Technical # 14: *Weak passwords*	#1 - Deletion of client data.	▪ Temporary or permanent data loss. ▪ Loss of service/availability. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**HIGH**	
	#2 - Destruction of client data.	▪ Temporary or permanent data loss. ▪ Loss of service/availability. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**HIGH**	

#3 - Exposure or Disclosure of client's proprietary information.	▪ Theft of data. ▪ Extortion. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**HIGH**	
#4 - Unauthorized access to client system(s).	▪ Temporary or permanent data loss. ▪ Loss of service/availability. ▪ Theft of data. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**MEDIUM**	
#6 - Denial of Service (DoS) and other attacks on the client's system.	▪ Temporary or permanent data loss. ▪ Loss of service/availability. ▪ Theft of data. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**HIGH**	
#7 - Release of malicious code onto client system(s).	▪ Temporary or permanent data loss. ▪ Loss of service/availability. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**HIGH**	

	#8 - Theft of client data or customized application.	▪ Loss of intellectual property. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**HIGH**	
Technical # 15: *Lack of internal or external audits*	#1 - Deletion of client data.	▪ Loss of reputation. ▪ Financial and legal ramifications.		**HIGH**	
	#2 - Destruction of client data.	▪ Loss of reputation. ▪ Financial and legal ramifications.		**HIGH**	
	#3 - Exposure or Disclosure of client's proprietary information.	▪ Loss of reputation. ▪ Financial and legal ramifications.		**HIGH**	
	#4 - Unauthorized access to client system(s).	▪ Financial and legal ramifications.		**MEDIUM**	
	#5 - Loss of connectivity to client's systems.	▪ Loss of reputation. ▪ Financial and legal ramifications.		**LOW**	
Technical # 16: *Regular backups are not being performed.*	#1 - Deletion of client data.	▪ Permanent data loss. ▪ Loss of service/availability. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**HIGH**	

	#2 - Destruction of client data.	▪ Permanent data loss. ▪ Loss of service/availability. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**HIGH**	
Technical # 17: *Backup information is not retained for adequate time period.*	#1 - Deletion of client data.	▪ Permanent data loss. ▪ Loss of service/availability. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**HIGH**	
	#2 - Destruction of client data.	▪ Permanent data loss. ▪ Loss of service/availability. ▪ Loss of reputation. ▪ Financial and legal ramifications.		**HIGH**	

E. Developing Controls

Current State of Practice

As detailed in Section B – Determining Scope, there are several current guidelines, standards and regulations with specific controls that are applicable to today's businesses; therefore some of them that were mentioned above are further described in this section, because they provide a framework of what is to be contained in the control checklist.

Due to the broad nature of the ASP audit, several sources should be used in developing controls, determining best practices and developing a checklist. Only the guidelines, regulations and standards listed below are in the scope of this guide. However, as mentioned previously, quite often the controls that make up specific regulations are similar and frequently overlap. This guide can be used as a baseline in that other regulations can be easily added at another point in time.

NIST:

The National Institute of Standards and Technology has an abundance of checklists, best practices and implementation guides.

- http://csrc.nist.gov/pcig/cig.html

The National Institute of Standards and Technology also has a library which is loaded with technical documentation.

- http://csrc.nist.gov/publications/nistpubs/

Specific NIST documents that assisted in the creation of this guide are listed as follows:

- NIST SP 800-26: "Security Self-Assessment Guide for Information Technology Systems"
  - This special publication offers an excellent comprehensive checklist that contains numerous controls.
  - http://csrc.nist.gov/publications/nistpubs/800-26/sp800-26.pdf

- NIST SP 800-30: "Risk Management Guide for Information Technology Systems"
  - This special publication serves as a guide in conducting a risk assessment.
  - http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

21 CFR 11 Related Documents:

One would assume that 21 CFR 11 checklists would be freely available since the regulation has been in existence since 1997 and has mandated the compliance of several industries. That assumption is not necessarily accurate.

Several of the available checklists are software-specific and some of them are only attained by paying for them. Luckily, developing a checklist based on this regulation is a fairly straightforward task. Listed below, are some checklists that pertain to 21 CFR 11, although they are software-specific, they can still assist the auditor in developing a good checklist.

- Certified Software:
  - http://www.certifiedsoftware.com/documents/css_electronic_signature_checklist.pdf

- Novotek:
  - http://www.novotek.nl/News/Docs/21CFR11_Meeting.pdf

- Here is a link to the FDA regulation itself which can easily be turned into a checklist:
  - http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/CFRSearch.cfm?CFRPart=11&showFR=1

Sarbanes-Oxley Related Documentation:
Since the inception of the Sarbanes-Oxley Law, several new businesses have either been started or set their focus on assisting other businesses with regulation compliance. Most checklists can only be obtained by purchasing them. COBIT, however offers a guide for free. It is a comprehensive framework that provides controls that will assist in the compliance with the somewhat vague regulation. The framework of controls can be found here:
  - http://www.isaca.org/Template.cfm?Section=About_Isaca&Template=/ContentManagement/ContentDisplay.cfm&ContentID=12406

HIPAA:
The HIPAA Security Implementation book offered as part of the SANS Step-by-Step Series is a thorough resource on the security rule of the HIPAA regulation. The manual is rich in material and covers topics such as developing a project plan, performing a risk analysis, the HIPAA audit, safeguards and much more. The guide can be purchased from SANS:
  - https://store.sans.org/store_category.php?category=stepxstep&portal=baea86b5dc2300ed92bffbf7c9659b01

SANS INFOSEC Reading Room:
There are countless documents and examples of audits that served as guidance to the completion of this document.
  - http://www.sans.org/rr/

These are some references specific to the types of controls broken down into their respective areas.

Administrative Safeguard Guides/References:

- Another valuable *NIST* document is Special Publication 800-50, **"**Building an Information Technology Security Awareness and Training Program." It can be used as a reference to create an Info-Security Program checklist.
  - http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf

Physical Safeguard Guides/References:

- *SANS Institute* has an ISO 17799 Checklist on their SCORE website. The checklist with regards to physical controls is just a small portion of what this document has to offer.
  - http://www.sans.org/score/ISO_17799checklist.php

- *The University of Massachusetts* has an excellent checklist on their website.
  - http://www.security.umassp.edu/index.cfm?fuseaction=generic.506

Technical Safeguard Guides/References:

- *INFOSYSSEC* is a security portal for security professionals. Among all of the other beneficial information, there are some whitepapers on securing systems and applications.
  - http://www.infosyssec.com/infosyssec/whitepap1.htm

- *Microsoft' Security Guidance Center* offers some wonderful resources for their products. The center provides links to security checklists, documents, articles and other security related information.
  - http://www.microsoft.com/security/guidance/default.mspx

- Many organizations struggle with patch management. This guide from *Microsoft* can be used as a reference in evaluating an effective patch management program.
  - http://www.microsoft.com/security/guidance/topics/PatchManagement.mspx

- *Carnegie Mellon's Software Engineering Institute* presents an abundance of information on their *CERT* Coordination website. This is a link to a UNIX related checklist.
  - http://www.cert.org/tech_tips/usc20_full.html

- *Auditnet.org* has a document that contains checklists for wireless, Windows, Remote Desktop, Citrix, Oracle, SQL and IDS.
  - http://www.auditnet.org/docs/ICQs/Multi-Security%20Assessment%20Checklist.doc

- *The National Security Agency* offers several security configuration guides on their website:
  - http://www.nsa.gov/snac/index.cfm?MenuID=scg10.3.1

Establishing General Controls

In order to keep things cohesive and organized, similar to the vulnerabilities listed in the Conducting a Risk Assessment section above, this section will also be broken down into three areas: Administrative Controls, Physical Controls and Technical Controls.

Table E.1: Administrative Controls: These are controls to assure that processes and procedures are in place and executed.

Control Number	Control Description
A-01	There is a security awareness program in place.
A-02	There are current documented security policies and procedures.
A-03	Security Policies are enforced.
A-04	Security Policies are formally communicated or available to staff.
A-05	Security Policy topics are reinforced.
A-06	Employees have been provided the Acceptable Use Policy.
A-07	Management approves the security plan.
A-08	There is a current documented Incident Response Plan.
A-09	The Incident Response Plan is available.
A-10	Employees are trained on how to handle an incident.
A-11	Incidents are reported appropriately.
A-12	Incidents are handled according to the Incident Response Plan.
A-13	Data has been classified and classification levels are documented.
A-14	A contingency plan has been developed and tested.
A-15	Duties are segregated and assigned appropriately.
A-16	Job descriptions accurately reflect segregation of duties.
A-17	Employees are trained to fill their job requirements.
A-18	Employee Training is documented.
A-19	There is a process for requesting, establishing, issuing, and closing user accounts. (NIST SP 800-18)
A-20	Hiring procedures are established and documented.
A-21	Background, credit and/or reference checks are performed on new employees/contractors.

A-22	Termination procedures are established and documented.
A-23	Quality Records are maintained.
A-24	Client system quality records exist and are maintained.

Table E.2: Physical Controls*:* These are controls that address the protection of the information system's physical environment and physical security access controls.

Control Number	Control Description
P-01	Physical Access Control Policies are documented.
P-02	Physical Access Control Procedures are documented.
P-03	Access to facilities is appropriately controlled.
P-04	Access control lists are reviewed on a regular basis.
P-05	Access to keys and/or badge making/security equipment is appropriately restricted.
P-06	Emergency exit and re-entry procedures ensure that only authorized personnel are allowed to re-enter after fire drills, etc. (NIST SP 800-18)
P-07	Visitors are processed accordingly and escorted through sensitive areas.
P-08	Physical access is monitored and logged.
P-09	Physical access logs are reviewed regularly.
	Suspicious activity is investigated.
P-10	If used, pin #'s or security codes to access facilities are regularly updated.
P-11	Appropriate fire suppression and prevention devices installed and working. (NIST SP 800-18)
P-12	Fire ignition sources, such as failures of electronic devices or wiring, improper storage materials, and the possibility of arson, reviewed periodically. (NIST SP 800-18)
P-13	Heating and air-conditioning systems are regularly maintained. (NIST SP 800-18)
P-14	There a redundant air-cooling system. (NIST SP 800-26)
P-15	In power outages uninterruptible power supplies or backup generators are used. (NIST SP 800 -26)
P-16	Physical media is properly disposed of.
P-17	Deposits and withdrawals of tapes and other storage media from the library authorized and logged. (NIST SP 800-26)
P-18	Media is sanitized prior to being reused.
P-19	Inventory lists are maintained.

Table E.3: Technical Controls*:* These are controls that are met through the use hardware and software to thwart any breach of security of information systems.

Control Number	Control Description
T-01	Applications are configured and tested prior to being implemented.
T-02	Operating systems are hardened.
T-03	System activities are logged appropriately.
T-04	Logs cannot be overwritten.
T-05	Logs are retained for an appropriate timeframe.
T-06	Systems are current on service packs and patches.
T-07	All patches and service packs are tested prior to being implemented.
T-08	IDS signatures are current.
T-09	An anti-virus solution is implemented.
T-10	Anti-virus definitions/subscriptions are up to date.
T-11	Perimeter devices are used and configured securely.
T-12	All devices are configured appropriately and all deviations are documented.
T-13	Access control mechanisms on devices are used.
T-14	Shared accounts are not used.
T-15	Complex passwords are used.
T-16	Password controls are in place.
T-17	Regular technical audits/assessments are performed.
T-18	Regular backups are performed.
T-19	Backups are retained for an adequate period of time.

Mapping Controls to Regulations

In this section, the controls from the Standard Control section above will be mapped to the equivalent or approximate control found in HIPAA, Sarbanes-Oxley and 21 CFR 11. The HIPAA reference numbers are taken directly from the regulation itself. The Sarbanes-Oxley/Cobit numbered reference is taken from the *Appendix B—Company-level Questionnaire* section of the IT Control Objectives for the Sarbanes Oxley (pages 52-57). The actual question number will be referenced.

The Control Objectives in the chart below were taken directly from the Sarbanes-Oxley/COBIT Reference section under the Appendix C—IT Control Objectives (pages 57-78). Each of the control objectives was assigned a Roman numeral as outlined in the chart below. If a Roman numeral was referenced in the Regulation to Control Mapping table then either a corresponding illustrative control under the control objective was found, or it is a control that supports the overall objective.

Table E.4: COBIT Control Objectives

#	Control Objective

I.	Controls provide reasonable assurance that application and system software is acquired or developed that effectively supports financial reporting requirements.
II.	Controls provide reasonable assurance that technology infrastructure is acquired so that it provides the appropriate platforms to support financial reporting applications.
III.	Controls provide reasonable assurance that policies and procedures that define required acquisition and maintenance processes have been developed and are maintained, and that they define the documentation needed to support the proper use of the applications and the technological solutions put in place.
IV.	Controls provide reasonable assurance that the systems are appropriately tested and validated prior to being placed into production processes and associated controls operate as intended and support financial reporting requirements.
V.	Controls provide reasonable assurance that system changes of financial reporting significance are authorized and appropriately tested before being moved to production.
VI.	Controls provide reasonable assurance that service levels are defined and managed in a manner that satisfies financial reporting system requirements and provides a common understanding of performance levels with which the quality of services will be measured.
VII.	Controls provide reasonable assurance that third-party services are secure, accurate and available, support processing integrity and defined appropriately in performance contracts.
VIII.	Controls provide reasonable assurance that financial reporting systems and subsystems are appropriately secured to prevent unauthorized use, disclosure, modification, damage or loss of data.
IX.	Controls provide reasonable assurance that all IT components, as they relate to security, processing and availability, are well protected, would prevent any unauthorized changes, and assist in the verification and recording of the current configuration.
X.	Controls provide reasonable assurance that any problems and/or incidents are properly responded to, recorded, resolved or investigated for proper resolution.
XI.	Controls provide reasonable assurance that data recorded, processed and reported remain complete, accurate and valid throughout the update and storage process.
XII.	Controls provide reasonable assurance that authorized programs are executed as planned and deviations from scheduled processing are identified and investigated, including controls over job scheduling, processing, error monitoring and system availability.

The 21CFR 11 reference numbers are taken from the regulation itself.

Some controls when applied together with other similar controls will support an overall control in the regulation. If the regulatory control can not be mapped to a Control Reference # then it will be annotated as “not applicable” (N/A).

Table E.6: Regulation to Control Mapping

Control Reference #	HIPAA Reference	Sarbanes-Oxley/COBIT Reference	21 CFR 11 Reference
A-01	164.308(a)(5)	23, VIII	11.10j
A-02	164.308(a)(1) 164.309(a)(1) 164.312(c)(1) 164.310(c) 164.312(d)	27, VIII	N/A
A-03	164.308(a)(1) 164.310(c)	30, 31, VIII	N/A
A-04	N/A	28, VIII	N/A
A-05	164.308(a)(5)	VIII	N/A
A-06	164.310(b) 164.310(c)	13, 21, 27, VIII	11.10j
A-07	N/A	27, 28, VIII	N/A
A-08	164.308(a)(6)	18, X	N/A
A-09	164.308(a)(6)	27, 28, X, XII	11.300c 11.300d
A-10	164.308(a)(6)	18, X, XII	N/A
A-11	164.308(a)(6)	18, X, XII	11.300d
A-12	164.308(a)(6)	X, XII	11.300d
A-13	N/A	25, 26, XI	N/A
A-14	164.308(a)(7)	VIII	N/A
A-15	164.308(a)(3)	15, VIII	11.10i
A-16	164.308(a)(3)	8, 11, 15, VIII	N/A
A-17	164.308(a)(3)	8, 20, 22, VIII	11.10i
A-18	N/A	22	11.10i
A-19	164.308(a)(3)	27, VIII	11.10d
A-20	N/A	27, VIII	N/A
A-21	164.308(a)(3)	21, VIII	N/A
A-22	164.308(a)(3)	19, VIII	11.10d 11.300b
A-23	164.308(a)(8)	45, 47, III	N/A
A-24	164.308(a)(8)	45, 47, III	11.10k
P-01	164.309(a)(1)	27, VIII	11.10c
P-02	164.309(a)(1) 164.310(c)	27, VIII	11.10c
P-03	164.309(a)(1)	39, VIII	11.10c
P-04	N/A	VIII	N/A
P-05	N/A	39, VIII	N/A
P-06	N/A	39, VIII	11.10c
P-07	164.309(a)(1)	39, VIII	11.10c
P-08	164.309(a)(1)	VIII	N/A
P-09	N/A	60, VIII	N/A
P-10	N/A	VIII	11.10c

P-11	N/A	41, VIII	11.10c
P-12	N/A	41, VIII	11.10c
P-13	N/A	41, VIII	11.10c
P-14	N/A	41, VIII	11.10c
P-15	N/A	41, VIII	N/A
P-16	164.310(d)	VIII	N/A
P-17	N/A	VIII	N/A
P-18	164.310(d)	VIII	N/A
P-19	164.310(d)	9	N/A
T-01	164.312(c)(1)	IV	N/A
T-02	164.312(c)(1)	IV, IX	11.10c
T-03	164.308(a)(1) 164.312(b)	XII	11.10e
T-04	164.312(b)	XII	11.10e
T-05	164.312(b)	XII	11.10e
T-06	N/A	VIII, IX	11.10c
T-07	164.312(c)(1)	IV	11.10c
T-08	N/A	VIII, IX	11.300d
T-09	164.308(a)(5)	VIII, IX	11.10c
T-10	164.308(a)(5)	VIII IX	11.10c
T-11	N/A	VIII IX	11.10c
T-12	164.312(c)(1)	III, IX	11.10c
T-13	163.308(a)(3) 164.308(a)(4) 164.312(a)(1)	VIII IX	11.100a 11.100b 11.200a
T-14	164.312(a)(1)	VIII, IX	11.100a 11.300a
T-15	164.308(a)(5)	VIII, IX	11.200a
T-16	164.308(a)(5)	VIII, IX	11.200a 11.300b
T-17	164.308(a)(1)	31, IX	11.300e
T-18	164.308(a)(7) 164.310(d)	XII	11.10c
T-19	164.308(a)(7) 164.310(d)	XI	11.10c

Some controls are so specific to the regulation they could not covered by the general controls section above. They are listed in the Gap Analysis section of this paper.

F. Creating a Checklist

After the auditor determines the list of controls that need to be tested, the next step is to create a checklist. The checklist is used as a tool for maintaining focus and tracking what needs to be assessed during the audit. The overall objective should be evident in each item. The following components are suggestions that should be included in a well-organized checklist.

Items Included in a Checklist

Item Number

For tracking purposes, the auditor should first start off with formulating a number

system. Although the design of the checklist is not standardized, it is strongly recommended that item numbers be used. Each item should have a unique number assigned. The ASP auditor needs to keep in mind that there may be considerable amounts of data passing hands so item numbers are essential. When requesting samples or documentation from the ASP the auditor should reference the checklist number to circumvent confusion and maintain the organization of the audit, which will quicken the overall process.

Item Name

It is also of critical importance to include the item name. Items are usually general and can encompass many controls. For example "Security Plan" is a general item. The item may encompass security awareness, security policies, enforcement, security reminders, etc.

Item Reference

References are sometimes dependent on the overall audit objective. If the audit is based on compliance with a regulation then that regulation should be referenced. This is where the auditor can reference the checklist items found in the *Mapping Controls to Regulations* section above**.**

If the audit is not specific to any regulation, references, such as industry best practices (i.e. SANS Top Twenty), should be noted. Tools used should also be noted in this section as well.

Risk

The risk is based on the findings during the audit. After the auditor determines the exposure to the vulnerabilities listed above in the Risk Assessment Table, they can then determine the risk.

Test Procedure/Compliance Criteria

Since an ASP audit can get out of scope quickly, it is detrimental to include the scope for each item being assessed. The defined test procedure assists the auditor in maintaining scope. The testing procedures or compliance criteria will depend greatly on the overall objective and may reference a specific regulation. The sample below illustrates this point.

Oscar's Ornithology Clinic is requesting an audit of their ASP to determine compliance with the 21CFR 11 Regulation. The control being tested is, A-06 – "Employees have been provided an acceptable use policy". Keeping the overall audit objective in mind, the test portion of the this checklist should be written as follows: Ensure that the "written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification."[10] Simply stating "Ensure the employees have been provided an AUP" is not adequate. Test procedures should be specific as possible.

Objective vs. Subjective Testing
Objective tests are tests that result in observable, non-biased output. Objective tests often employ tools to get achieve their results. For example if the auditor scans a network for the Subseven Trojan and the scan comes up with three systems that have Subseven installed then there is no opinion to be made on the results. They results are cut and dry in that three systems are more than likely infected. Subjective tests are tests that result in the auditor having to interpret the data to and in doing so may provide biased results. For example, if the auditor has to review quality documents to ensure they incorporate best security practices the results of that test would involve the opinions of the auditor, therefore that type of test would be subjective. The auditor should know what type of tests they are using in their checklist and attempt to keep a balance in the types of testing. Objective tests are always preferred.

Evidence
This section of the checklist is reserved for when results of the audit have been determined. It will be populated by evidence found during the audit. It is recommended that this section be filled out during the steps found in the Conducting the Audit, Testing, Evidence Findings section.

Pass/Fail
This is reserved for the auditor's findings and conclusions whether the objective was met or not.

Mitigation
This field of the checklist is reserved for suggestions on what the ASP should do to mitigate the risk. Best practices and the controls found in guidelines, regulations and standards as referenced in the Current State of Practice section above should be used in determining the methods of mitigating risks.

Notes
The notes section is recommended. If the auditor shares the checklist with the client or ASP it will be beneficial to them, as well as the auditor. The client or ASP can use this field to comment or ask questions. The auditor can use it as well.

Example Format

An example of a how to put all of the items together in a cohesive format has been provided below:

Table F.1: Example Checklist

#. Item Name		Risk:	
General Reference(s): Personal Experience	**HIPAA:**	**SOX:**	**21 CFR 11:**
Test Procedures/Compliance Criteria: **General Audit:** **HIPAA:** **SOX:** **21 CFR 11:**			
Evidence:			
Pass/Fail:			
Mitigation:			
Notes:			

ASP Checklist

Since this document serves as a reference guide for ASP auditors, it is only appropriate to include an actual checklist as part of this guide. The checklist below is derived from the *Risk Assessment* and *Developing Controls* examples in the above sections. The Evidence, Pass/Fail, Mitigation and Notes sections of the example checklist below have been omitted because they are addressed in the sections G and H of this guide. Some of the checklist tests below are more general due to the fact that environments, systems, hardware and software will be different for each audit. Several guidelines on how to audit specific systems, hardware and software can be found in SANS Information Security Reading Room.

The testing sections of this checklist assume that all of the tools are loaded on a testing machine. Links to the tools have been provided below in the Creating a Toolbox section.

Table F.2: ASP Checklist Example

A-I. Security Plan		**Risk:**	
General Reference(s): Controls A-01 through A-06 Personal Experience NIST SP 800-18 NIST SP 800-26 British Standard (BS) 7799-1 ISO 17799	**HIPAA:** 164.308(a)(1) 164.308(a)(5) 164.309(a)(1) 164.312(c)(1) 164.310(b) 164.310(c) 164.312(d)	**SOX:** 13, 21, 23, 27, 28, 30, 31, VIII	**21 CFR 11:** 11.10j

Test Procedures/Compliance Criteria:

General Audit:
Evidence of the following will be needed:

1) *Security Organization*: Obtain a copy of the organization chart to ensure there is a security organization. Obtain copies of job descriptions, employee training documentation and educational/experience references pertaining to security. Compare job titles, descriptions and experience to ascertain if the position is appropriately filled and that there is a security organization. Retain any documentation as evidence.
2) *Awareness program:* Get dates of any training and training materials. Check to see if tests/quizzes are administered. If training is done electronically check to see if it is tracked or logged and review any outputs from the logs. Review a sample of employee training documentation and cite any security related training. Ensure that training materials address: Acceptable Use, Ethical Conduct, Data Classification, Access Control, Physical Security, Passwords, Anti-virus, Security Best Practices, Workstation Security, Hardening, OS Security, Application/Database Security, Contractor security, Vendor security. Log employee names, topics covered and training dates as evidence.
3) *Security Policies* – Review the ASP's security policies. Ensure that they are current by checking the version control. Use the version control section to determine if documents are being reviewed on a regular basis to ensure integrity. Ensure that they use strong decisive language like "must". Ensure policies are formally communicated or available by either obtaining a copy of a policy related email or by actually clicking on a security policy related link on the ASP's intranet. If the organization makes them available via a documentation repository or a shared drive attempt to access the policies. If the ASP does not allow such a thing ask to see a demonstration of a random employee accessing the documents. Review documents for management approvals. Ensure there is a section in the policy that is dedicated to management approval. Several topics should be addressed within a corporation's policies: Acceptable Use, Ethical Conduct, Data Classification, Access Control, Physical Security, Passwords, Anti-virus, Security Best Practices, Workstation Security, Hardening, OS Security, Application/Database Security, Contractor security, Vendor security. Ensure that policies are enforced. Review any documented violations and remedial efforts to ensure policies and procedures are enforced. Either obtain printouts of the document's title page, table of contents, tracking/version control and approvals or annotate the title, version number, revision dates, approval names and approval dates as evidence.
4) *Security Reminders* **–** View newsletters, policy statements, posters, briefings, emails, banners, pop-ups, meeting minutes, and security paraphernalia to ensure that policy topics are being reinforced. Retain any copies as evidence.

HIPAA:

1) *164.308(a)(1) – Secutity Management Process:* Ensure there is a "Sanction Policy" in place that references how to secure EPHI and how the policy is enforced. Tests three and four from the A-I, General Audit section generally addresses security policy. The auditor should ensure that the ASP has policies that specifically reference EPHI.
2) *164.308(a)(5) – Security Awareness Training*: The general audit test items from above should address this standard. Specifically, security reminders are an important element of this section. Also, ensure that there is an AUP and AV policy and procedure in place that address issues such as opening attachments, downloading unapproved software, anti-virus desktop software and virus definition file updates. View policies on access controls and passwords. View procedures in obtaining access. Confirm that the password policy contains elements such as password strength and complexity, account lockouts, and password re-use, which will be tested via stimulus-response in part three of this test. Confirm that the procedures address the process of requesting, approval, creating, deleting/disabling, and particularly monitoring accounts particular to the client system. This will also be tested via stimulus-response in test 2b below of this section.
3) 164.309(a)(1) – Facility Access Controls:

    a. *Facility Security Plan*: View the physical security policy. Validate there are procedures and policies in place that are particular to safeguarding the client equipment. Ensure that role-based access controls are used. Upon arrival to

A-II. Incident Response		Risk:	
General Reference(s): Personal Experience Controls A-08 through A-12 Personal Experience NIST SP 800-3 British Standard (BS) 7799-1 ISO 17799 Incident Response and Computer Forensics, Second Edition *by Chris Prosise, Kevin Mandia, Matt Pepe* CERT - http://www.cert.org/nav/index_red.html BugTraq- http://www.securityfocus.com/archive/1	**HIPAA:** 164.308(a)(6)	**SOX:** 18, 27, 28, X, XII	**21 CFR 11:** 11.300c 11.300d

Test Procedures/Compliance Criteria:

General Audit:

1) *Documented Incident Response Plan:* Ensure there is a plan in place that encompasses incidents pertaining to the client's systems. Review the plan to see if the following components are present: Incident Reporting, Roles and Responsibilities, incident identification, containment, eradication, recovery and reporting. Ensure that the Incident Response Plan is available by accessing it (via link on the ASP's intranet, shared drive, accessing it in the documentation repository.) Either obtain printouts of the document's title page, table of contents, tracking/version control and approvals or annotate the title, version number, revision dates, approval names and approval dates as evidence.
2) *Preventative Plan:* Ensure that there is a prevention plan in place. Review the results found in the General Audit in Section A-I above. Ensure there is a daily or weekly review of vulnerabilities, especially pertaining to the client system. This can be demonstrated by analyzing emails, reviewing a log of vulnerabilities that were addressed, reviewing change management records or service records that would reveal indications that systems were patched to prevent the exploitation of announced vulnerabilities, reviewing meeting minutes on vulnerability management. Retain any evidence. The ASP may subscribe to a vulnerability advisory service. In this case, compare the ASP recent advisories (i.e. Emails) with sources such as CERT or BugTraq to ensure the ASP has reliable and effective service (getting recent, up-to-date vulnerabilities). Retain any copies of emails or advisories as evidence.
3) *Incident Response Teams:* Review roles and responsibilities addressed in plan. Ensure that the team meets regularly (meeting minutes/notes). Obtain an organization chart. Obtain a list of the incident response team members. Match each employee up to the roles and responsibilities of the Incident Response Plan. Determine that the appropriate SME's are involved from each area pertaining to the client's system. (OS, Application, physical security, logical security…) Document the list of the teams and their members and any meeting dates or briefing dates and retain as evidence.
4) *Incident Response Training:* Get dates of any training and training materials. Check to see if tests/quizzes are administered. Obtain the test/quiz results of one or several client system users to ensure they were involved in training. If training is done electronically check to see if it is tracked or logged. Review any outputs from those logs to ensure that recent training has been performed. Review a sample of employee training documentation and cite any incident response related training. Ensure that training materials address: Incidents related to physical security and logical security, incident handling and incident reporting. Obtain evidence such as: emails reminders, newsletter articles, security posters…that reference Incident Response.
5) *Incident Tracking:* Ensure that incidents are logged and tracked in a ticketing system, email, logbook, etc. Review the logs to see if incidents are appropriately handled. Ensure that all phases of incident response are covered (Reporting Identification, Classification, Containment, Eradication, Recovery, Reporting/Review) If there were any incidents regarding the client retain logs/emails as evidence.
6) *Testing:* Ensure that the plan has been tested by reviewing test dates, meeting minutes, ticketing system entries and/or log book entries. Review version control of the documented Incident Response Plan. Correlate plan testing with revisions of the plan. Document dates of testing as evidence.

HIPAA:

1) *164.308(a)(6) – Security Incident Procedures*: Tests one and five from the A-II – General Audit Section above will sufficiently test this control.

SOX:

1) *18 – IT Organization and Relationships*: Test 5 from the A-II General Audit section above addresses this. See if logs reveal that management was either involved in the incident, or a report of the incident was sent to them. Review the Incident Response Plan, specifically to see what types of roles management plays. Retain a copy of management roles as written in the Incident Response Plan or Incident Handling logs as evidence.

A-III. Human Resources		Risk:	
General Reference(s): Personal Experience Controls A-15 through A-22 Personal Experience NIST SP 800-18 NIST SP 800-26 British Standard (BS) 7799-1 ISO 17799	**HIPAA:** 164.308(a)(3)	**SOX:** 8, 11, 15,19, 20, 21, 22, 27, VIII	**21 CFR 11:** 11.10d 11.10i 11.300b

Test Procedures/Compliance Criteria:

General Audit:

1) *Segregation of Duties (SOD):* Review any policies and procedures for SOD elements pertaining to the client system(s). Obtain an organization chart, a list of employees that have access to the system both physically and logically, and their respective job descriptions. Determine roles of the organization and client system support roles. Ensure that job descriptions match the support roles and SOD is reflected. Ensure that there is a segregation of duties. (Is security a separate function? Is quality assurance a separate function? Are developers and application testers separated from support personnel?) This will be further tested in sections P-I and T-IV below. Ensure that there are procedures on handling role changes within the organization. Either obtain printouts of the document's title page, table of contents, tracking/version control and approvals or annotate the title, version number, revision dates, approval names and approval dates as evidence.
2) *Training:* Obtain a list of employees with access to the client's system. Obtain training documentation and training plans, applications and related resumes, job descriptions. Ensure that levels of experience and training adequately meet the role/job description. Training and training dates should be determined to ensure that training is adequate and relevant. Certifications and any documentation read that are relevant to the client's system should be noted as well. Retain copies of a blank training plan, and document employee's names with training dates and certifications as evidence.
3) *Evaluation Procedures:* Obtain a copy of a blank evaluation and ensure that there is a section on areas of improvement or training needed. Obtain a list of evaluation dates. Request to see a random evaluation to ensure that the dates on it are current. (Comments/Grades may be blacked out to ensure privacy.) Retain all copies as evidence.
4) *Hiring Procedures:* Review hiring procedures to ensure background, credit and/or reference checks are a part of the hiring process. Review procedures to ensure they address setting up accounts or access (badges/keys/pins). Either obtain printouts of the document's title page, table of contents, tracking/version control and approvals or annotate the title, version number, revision dates, approval names and approval dates as evidence.
5) *Termination Procedures:* Review procedures to ensure that all components of access (physical, logical, remote) to client systems are covered. Tests for this will be further tested in sections P-I and T-IV below. Either obtain printouts of the document's title page, table of contents, tracking/version control and approvals or annotate the title, version number, revision dates, approval names and approval dates as evidence.

HIPAA:

1) *164.308(a)(3) – Workforce Clearance Procedures :* Test one in section A-III covers this. Ensure that access to client systems is appropriately assigned.

SOX:

1) *8 – IT Organization and Relationships:* General Audit test two in section A-III covers this. Ensure that employees with access to client systems have been properly trained by reviewing items in test two.
2) *11 – IT Organization and Relationships:* General Audit tests one and two in section A-III adequately cover this. Using information in test one ensure that employees with access to client systems can access them based on their defined role and ensure that they have been properly trained by reviewing items in test two.
3) *15 – IT Organization and Relationships:* General Audit test one in section A-III covers this. Ensure that access to client systems is appropriately assigned. Sections P-1 and T-IV will test this further.
4) *19 – Management of Human Resources:* General Audit tests one and five in section A-III cover this. Tests for this will be further tested in sections P-I and T-IV below. Ensure that role changes and terminations are addressed in procedures.
5) *20 – Management of Human Resources: General* Audit test two in section A-III covers this. Review training plan documents to ensure that development is a part of job responsibilities.

A-IV. Contingency Plan		Risk:	
General Reference(s): Personal Experience Control A-14 Personal Experience NIST SP 800-34 NIST SP 800-18 NIST SP 800-26 British Standard (BS) 7799-1 ISO 17799	**HIPAA:** 164.308(a)(7)	**SOX:** VIII	**21 CFR 11:** N/A

Test Procedures/Compliance Criteria:

General Audit:

1) *Documented Plan*: Ensure that a formal contingency plan is documented that encompasses the client's systems. Ensure that the BCP identifies and prioritizes critical IT systems and data. Review the plan to see if the following components are present: contingency plan objectives, roles and responsibility identification, identification of key systems and data, business continuity requirements, backup requirements, management endorsement, and recovery strategies. Ensure that the BCP is available by accessing it (via link on the ASP's intranet, shared drive, accessing it in the documentation repository.) If there is an alternate site for recovery, determine if the type of site meets the client's needs. (Refer to Table 3-1 Alternate Site Criteria Selection in NIST SP 800-34). Review the contract between the ASP and the alternate site to ensure that it contains some of the elements found in NIST 800-34. i.e. contract/agreement duration, site guarantee, guarantee of compatibility as they pertain to the client. Obtain a list of employees that support the client system(s). Obtain training documentation to ensure that the employee has read and has been trained on the BCP. Document employee names, training dates and topics discussed relating to the BCP as evidence. Repeat the latter test if a BCP team is defined in the documentation. Either obtain printouts of the plan's title page, table of contents, tracking/version control and approvals or annotate the title, version number, revision dates, approval names and approval dates as evidence.
2) *BCP Testing*: Ensure that the BCP tests or exercises have been performed by obtaining test results of plan. Compare the dates of tests to the BCP version control. (Are walkthroughs or dry runs performed? Are test roles defined? Were the tests conducted fairly recently? Was the plan revised after the tests were performed to correct any deficiencies?) Document test dates and retain as evidence.

HIPAA:

1) *164.308(a)(7) – Contingency Plans:* Review the BCP and ensure that it addresses the client's data backup plan, recovery of the data, and procedures to protect and make sure that EPHI data and applications available in an emergency. A-IV, General Audit test two addresses BCP testing. Obtain any documentation in regards to client specific BCP plans or DR plans. Print out the document's title page, table of contents, tracking/version control and approvals or annotate the title, version number, revision dates, approval names and approval dates as evidence.

SOX:

1) *VIII:* Ensure that BCP has been endorsed by management and is formally communicated to critical staff. A-IV, General Audit test one addresses this.

A-V. Data Classification		Risk:	
General Reference(s): Personal Experience Controls A-13 Personal Experience NIST SP 800-18 NIST SP 800-26 British Standard (BS) 7799-1 ISO 17799 All in One CISSP Certification Exam Guide *by Shon Harris*	**HIPAA:** N/A	**SOX:** 25, 26, VIII	**21 CFR 11:** XI

Test Procedures/Compliance Criteria:

General Audit:

1) *Owner*: Ensure that the ASP and the client have agreed to the defined classification and security levels of their data and systems through verbal assessment. Ascertain any exceptions through verbal discussions. Review system/client documentation to ensure that agreed upon classifications and exceptions are documented. Review documented changes to the agreed upon classifications and exceptions.
2) *Policy*: Ensure that a documented policy exists. Ensure that the policy addresses the following: data classification levels and their associated security control levels (encryption), physical access, data transmission and data access (digital certificates), management endorsement and version tracking. Verify the client's system maintains the correct security controls (encrypted files), use of digital certificates, physical access. Those will be tested further in sections P-I, T-I and T-IV. Obtain evidence that the policy formally communicated and employees responsible for the client system(s)/data have been trained on data classifications and handling. This can be tested using the same methods found in A-I, General Audit tests two and three.
3) *Procedure*: Ensure the procedure details how data is classified and how each sensitivity level of data is handled. Ensure that personnel are trained on the sensitivity levels and how to handle the data. This can be tested using the same methods found in A-I, General Audit tests two and three.

SOX:

1) 25 – Review and compare the ASP's Data Classification Policy and their Security Policy to ensure that they are cohesive.
2) 26 – Review findings from tests one trough three of the A-V, General Audit section. Ensure that classification levels of client's data and systems have the minimum set of security controls defined as outlined in the policies and procedures. (Does the client's data classification mandate any of the following are used: firewalls, host based intrusion detection, network based intrusion detection, system vulnerability assessments, encrypted transmissions, VPNs, two factor authentication, biometrics, badges, keys, pin codes, passwords, secret questions…)
3) XI – Ensure that sensitive client information is protected by performing tests in sections P-1, T-1 and T-IV.

A-VI. Quality Records		Risk:	
General Reference(s): Personal Experience Controls A-23 – A-24 Personal Experience NIST SP 800-18 NIST SP 800-26 British Standard (BS) 7799-1 ISO 17799	**HIPAA:** 164.308(a)(8)	**SOX:** 45, 47, III	**21 CFR 11:** 11.10k

Test Procedures/Compliance Criteria:

General Audit:

1) *Quality Management*: Ensure that there are document and data management procedures that exist. Review them to ensure that they define requirements in regards to formatting, managing, publishing, reviewing and approving quality records. Compare documentation obtained thus far to the quality management procedures/guidelines/policies and note any discrepancies.
2) *Version Control*: Ensure that policies and procedures collected previously have a tracking section that tracks at least version numbers. It is a bonus if the version tracking section includes the modifier's name, a brief statement as to the modifications made, and the modification date.
3) *Reviews/Approvals*: Ensure that the quality management procedures/guidelines/policies involve management and key staff in the approval process. Review previously collected documents to ensure documents are being approved following the procedures as outlined. (If the documentation is client specific ensure that the client has approved the document.) Ensure that quality records are reviewed as outlined in the quality management guidelines/policy, which should at least be when the process has been modified or on a regular basis. This can be done by reviewing the approval section of the document. Ensure the frequency of reviews meets the client's expectations.
4) *Reviews/Revisions*: Ensure that revisions to the documents have been made on a relatively frequent basis or when the process has been changed. Ensure that revisions are tracked appropriately by reviewing the version control section of the previously acquired documents.
5) *Storage*: Ensure that quality documents that pertain to the customer are stored in a secured area and are accessible to key personnel only. This can be demonstrated by reviewing client support personnel list with access control logs. Match up names with log entries and note any discrepancies. Retain a copy of logs and access lists as evidence. Ensure that quality records are being stored for an adequate amount of time (*For example HIPAA requires six years of quality records be kept*), by reviewing the version control on documents pertaining to the system set up. Note all records by title, version numbers and associated dates as reference.

HIPAA:

1) 164.308(a)(8) - *Evaluation*: Ensure that periodic review of quality records is performed by performing test three in section A-VI General Audit.

SOX:

1) 45 – *Management of Quality*: Ensure that quality documents exist pertaining to client. Review the documents to ensure they meet the quality standards in that they are maintained, reviewed and controlled. See tests in the A-VI, General Audit section for further clarification.
2) 47 – *Management of Quality* – Ensure that the quality management policy/guidelines/procedures regarding documentation have been communicated to staff and that the guide is available. Review system documentation, policy documents, procedures to ensure that there is standard formatting which demonstrates that QA documentation guidelines/policies/procedures have been communicated.
3) III – Ensure that client support documentation (user manuals) exists that illustrates the proper use of applications. Ensure that client system documents are maintained by performing tests two through four in the A-VI, General Audit section.

21 CFR 11:

1) 11.10k – Refer to test five in the A-VI, General Audit section.

P-I. Physical Access Control		Risk:	
General Reference(s): Personal Experience Controls P-01 through P-06 Personal Experience NIST SP 800-18 NIST SP 800-26 Physical Security Audit Checklist – (*See references Section*) Information Security Management - BS 7799.2:2002 Audit Checklist for SANS by Val Thiagarajan *(See references section)*	**HIPAA:** 164.309(a)(1) 164.310(c)	**SOX:** 27, 39,60 VIII	**21 CFR 11:** 11.10c

Test Procedures/Compliance Criteria:

General Audit:

1) *Quality Records:* Ensure that physical access policies and procedures are documented as part of the security plan by performing tests as outlined in the General audit in section A-I and test two of A-I, HIPAA. Ensure that Physical Security quality records address the following topics: visitor, cleaning-crew, client, maintenance, and vendor access. Ensure that there is a documented access review procedure and that it is being followed by reviewing reports, findings, email evidence.
2) *Walk Thru*: Ensure that visitors are appropriately identified and processed according to the Physical Security policy during the engagement. (Is there a sign in process? Are guards used? Are persons requesting access appropriately identified? By watching access, is piggybacking evident? Are badges administered? Are visitors escorted?) Ensure that there is some type of access control mechanism such as a badge system, keyed entry, pin entry, use of biometrics into the facility. Test the system by attempting to gain access. (i.e. – type in a random code, attempt to use a visitors badge, attempt to gain access by using handprint, try opening doors to secured areas) Obtain logs from the system verify the unauthorized access attempts were logged. Ensure that client systems are placed in a separate secured area within the building. Ensure there are access control mechanisms into secured areas. Attempt the same tests as above. Review access via floor and ceiling by lifting floor/ceiling tile. (Can access be gained by crawling under?) Ensure there are no other windows, doors and other entry points into the secured area. If cameras an close circuit TV's are used, ensure that they are covering the appropriate areas. (Is someone dedicated to watching the tapes? Are tapes held for an adequate amount of time?) Ensure that security equipment (keys, badge makers, etc) stored in a secured room. Attempt to gain access to the room by swiping badge, jiggling door handle… If access to the room is logged review logs to ensure that access attempts were written.
3) *Access*: Obtain a list of employees with access to the secured area where the client's systems reside. Obtain a list of key personnel which have access to security equipment rooms. Request random access logs of each to ensure that persons on logs are authorized to have access.
4) *Emergency entry*: Review re-entry policies and procedures. Ensure that only authorized personnel are allowed re-entry after emergencies or fire drills. Verify that policies require unauthorized individuals such as visitors, contractors, maintenance workers, cleaning crew, vendors, clients are required to check in again. Request logs from the day of the last fire drill to ensure there is evidence of this.

HIPAA:

1) *164.309(a)(1) – Access Control and Validation*: P-I, General Audit tests should adequately address this.
2) *164.310(c) – Workstation Security:* P-I, General Audit tests should adequately address this, namely test three.

SOX:

1) 27 – *Communication of Management Aims and Directions*: P-I, General Audit test one should adequately address this.
2) 39 – *Risk Assessment*: P-I, General Audit tests should adequately address this.
3) 60 – *Adequacy of Internal Control*: Ensure that reviews done periodically. P-I, General Audit test one should adequately address this.
4) VIII – P-I, General Audit tests should adequately address this.

21 CFR 11:

1) 11.10c – P-I, General Audit tests should adequately address this.

P-II. Facilities		Risk:	
General Reference(s): Personal Experience Controls P-11 through P-15 Personal Experience NIST SP 800-18 NIST SP 800-26 Physical Security Audit Checklist – (*See references Section*) Information Security Management - BS 7799.2:2002 Audit Checklist for SANS by Val Thiagarajan *(See references section)*	**HIPAA:** N/A	**SOX:** 41, VIII	**21 CFR 11:** 11.10c

Test Procedures/Compliance Criteria:

General Audit:

Fire Suppression and Devices: Ensure the following: fire extinguishers are present and have been inspected by reviewing tags, smoke detectors are present, fire alarms are tested on a regular by reviewing test procedures and other documentation. Ensure that fire suppression devices have been recently inspected. Obtain a copy of the inspection and document any findings. In the event of a fire ensure that client data will be protected by reviewing emergency plans.

Fire Ignition Source Review: Review procedures to ensure that fire ignition sources are reviewed on a regular basis. Ensure that reviews are taking place by reviewing any result documentation/emails/reports.

Maintenance Contracts: Items such as fire equipment inspections, power and room temperature controls all may be maintained by a third party. If this is the case, review maintenance contracts to validate services provided and contract dates.

Room Temperature: Ensure that the temperature in the room is adequate. Ensure there is a back-up for air cooling system.

Power: Ensure that generators or Uninterruptible Power Supplies are used. Ensure that the facility has a redundant power source.

Cabling: Ensure that cabling is protected from water/fire sources.

Raised Flooring: Ensure that flooring is raised flooring (elevated at least 18 inches).

SOX:

1) 41 - P-II, General Audit tests should adequately address this.
2) VIII - P-II, General Audit tests should adequately address this.

21 CFR 11:

1) 11.10c - P-II, General Audit tests should adequately address this.

P-III. Back Up Media		Risk:	
General Reference(s): Personal Experience Controls P-16 through P-18 Personal Experience NIST SP 800-18 NIST SP 800-26 British Standard (BS) 7799-1 ISO 17799 Physical Security Checklist by TeCrime International, Inc *(See references section)* Device and Media Controls – Disposal *by Alan R. Mercer*	**HIPAA:** 164.310(d)	**SOX:** VIII	**21 CFR 11:** N/A

Test Procedures/Compliance Criteria:

General Audit:

1) *Physical Media Quality Records*: Ensure that there are policies and procedures in place in reference to physical media. Ensure that policies and procedures contain the following elements: handling, storage, protection, access, labeling, re-use and disposal. Ensure that Segregation of Duties is evident in the back up quality documents.
2) *Handling, Storage & Protection*: Ensure that physical back up media (back-up tapes) are stored in a secured area. Test access to the area Tests from the P-I, General Audit section above should be performed to ensure that access to the media is limited. Ensure that tape removal is adequately logged or documented by reviewing logs. Review logs specific to client to ensure that only appropriate personnel had access to client's media. Review client backup tapes to ensure they are labeled appropriately. (Client name should not be evident on the label.)
3) *Re-Use* : Ensure degaussing procedures are followed if media is re-used. (Does the ASP use a degaussing service? Do they own or rent a degausser?) Ensure that if media is written over are there software controlled expiration dates that will cause the image to expire.
4) *Disposal*: Ensure that disposal is performed in an adequate manner (overwriting of data, degaussing) in accordance with information security best practices. Ensure that disposal of media is documented. "Identify the asset or media to be disposed and include the dates and means of authorization, removal of media, removal of data, and disposal of the device and/or media."[11]
5) *Restoration*: Review the restoration process to ensure that only approved personnel can handle restoration tapes. Ensure that restorations are appropriately logged (Requestor, request date, delivery date, restore date). Obtain logs and approved access lists to ensure only legitimate persons have access. Ensure that persons that there are limited a limited number of persons with the authority to change the requestor list. Ensure that segregation of duties is effective in that persons authorizing requestors are not part of the requestor list.

HIPAA:

1) *164.310(d) – Device and Media Controls*: Ensure that EPHI is removed prior to re-use or disposal and that it is documented by performing the tests from the P-III, General Audit section above.

SOX:

1) *VIII* - Tests from the P-III, General Audit section above address this.

P-IV. Inventory Control	**Risk:**

General Reference(s):	HIPAA:	SOX:	21 CFR 11:
Personal Experience Controls P-19 Personal Experience NIST SP 800-18 NIST SP 800-26 British Standard (BS) 7799-1 ISO 17799 Sample Internal Control Checklist by OFM *(See references section.)*	164.310(d)	9	N/A

Test Procedures/Compliance Criteria:

General Audit:

1) *Quality Documents*: Ensure that policies/procedures exist in regards to Inventory and tracking assets. Ensure that inventory lists contain the following elements owners, serial/part numbers, part/software/hardware description, relevant dates of purchase (for tracking), version controls.
2) *Inventory Manager*: Ensure that one or more employees are responsible for maintaining the inventory list. Ensure that the employees that maintain this list are on the org chart.
3) *Lists*: Ensure that inventory is accurately tracked comparing inventory lists a list of the client's systems/hardware/software. Ensure that list is maintained by reviewing the version control. **(**Are lists automated? Is inventory taken and compared to lists to ensure integrity of the list? Are lists validated?)

HIPAA:

1) *164.310(d) – Device and Media Controls*: Tests in the P-IV, General Audit section above address this adequately.

SOX:

1) 9 – Ensure that client systems have been identified and those systems are represented in inventory lists. Ensure that client name (data owner) is represented in inventroy list.

T-I. Perimeter Security		Risk:	
General Reference(s): Personal Experience Controls T-08-T11 Personal Experience NIST SP 800-18 NIST SP 800-26 British Standard (BS) 7799-1 ISO 17799 Auditing a Cisco A Cisco 1721 Router: An Auditor's Perspective *by Ray Welshman* Router Security Configuration Guide *by NSA* RAT – *The Center for Internet Security*	**HIPAA:** N/A	**SOX:** VIII, IX 11.300d 11.10c	**21 CFR 11:** VIII, IX 11.300d 11.10c

Test Procedures/Compliance Criteria:

General Audit:

1) *Quality Records:* Review all quality documents ensuring that perimeter security related policies and procedures exist and are updated on a regular basis. (Topics to look for would be firewalls, ACL's, NAT, router/switch configuration, intrusion detection systems (HBIDS, NBIDS), configuration and vulnerability assessments, modems, change management, and system upgrades.) Either obtain printouts of the document's title page, table of contents, tracking/version control and approvals or annotate the title, version number, revision dates, approval names and approval dates as evidence.
2) *Physical Security*: Ensure that all perimeter devices and security devices are stored in a secure area by performing tests as outlined in P-I.
3) *Change Management*: Ensure that all changes to perimeter devices are documented and go through a change management process by performing test two in the T-II, General Audit section.
4) *Firewalls Ruleset Configuration*: Obtain copies of firewall rulesets for client firewalls. Review policy to ensure that only specified traffic gets through by doing the following:
    a. Check to ensure Default Deny rules and stealth rules are in place.
    b. Rules that have "Any" as a source, destination or service are checked should be noted.
    c. Check to ensure that Network groups and ranges are identified and belong to client.
    d. Check sources and destinations to ensure they are live hosts/ips of the client.
    e. Check rules for comments which may explain why they exist. Change management identification numbers may be referenced. If they are present obtain copies of the actual change documents and cross reference them ensuring the rules in place went through the change process and have been approved by the client. Retain copies for evidence.
    f. ASP specific rules should be noted (monitoring, dns, smtp, HBIDS, ip and tunneling protocols)
    g. Note any temporary, expired or disabled rules.
    h. Note any rules that can be combined.

    Test the configuration by also running a port or nmap scan as directed below of the client's systems and the firewall. (*See example steps below.*) This should be done from both the client site and the internet. Ensure that the firewall is behaving as it should (blocking certain ports and allowing certain ports.) Compare the results of the scan to the firewall policy and note any discrepancies.
    a. Using a command prompt navigate to the nmap directory.
    b. Type in the following:
    C:\Tools\NMAP>nmap –n –P0 -O -v 192.168.1.3 > nmapresults
    c. Either view the output by using cat or more commands or if using Windows exit out of the command prompt and navigate to the directory where the results were sent, in this example it would be the NMAP directory. Open the "nmapresults" file with notepad.
    d. Obtain logs from the firewalls and IDS systems during the scanning timeframe and retain as evidence.
5) *Firewall OS/Software Configuration*: Ensure that firewall is dedicated and is not running a web server, dns, ftp, telnet… This can be tested by running test two in section T-II, General Audit section. Review vendor documentation and obtain screenshots of software versions to ensure that the OS is at its latest patch level.
6) *Routers*: Verify the version numbers provided in the preliminary questionnaire are accurate by doing typing show version command while logged in to the router. (This assumes that it is a Cisco router).

    Oscars_router> sh ver

    Request router configurations or obtain them by running the show running configuration command on the router.

    Oscars_router> sh run

7) Save the configuration to a text file as evidence. Review Review the router configuration to ensure they are configured securely. Check for the following:

    a. Warning banners are configured

T-II. Configuration Management		Risk:	
General Reference(s): Personal Experience Controls T-01-02, T-06-07, T-12 Personal Experience NIST SP 800-18 NIST SP 800-26 British Standard (BS) 7799-1 ISO 17799 See Reference Section: ✓ SANS Top Twenty List ✓ RU Secure – Security Checklist *by Rutgers University* ✓ SuperScan - Foundstone ✓ *Intrusion Detection FAQ- What port numbers do well-known trojan horses use?* by SANS ✓ *Port Numbers* – IANA ✓ *MBSA* – Microsoft ✓ Common UNIX Services to Disable *by York University* ✓ Sun Patch Reporter ✓ Hardcopy Pro – *by Desksoft* ✓ Default Password List – *by Phenoelit* ✓ N-Stealth *by ZMT COMUNICAÇÕES E TECNOLOGIA LTDA* ✓ Database Vulnerability Scanners- *by Talisker or Pete Finiagan*	**HIPAA:** 164.312(c)(1)	**SOX:** III, IV, IX, VIII	**21 CFR 11:** 11.10c

Test Procedures/Compliance Criteria:

General Audit:

1) ***Quality Records****:* Review all quality documents ensuring that SDLC related policies and procedures exist and are updated on a regular basis. (Topics to look for would be SDLC, development, testing, hardening, patch management, configuration assessments, documenting configurations, change management, system upgrades) Randomly choose a sampling of servers from the client's environment (see Identifying Systems to Be Audited section above) review system configuration documentation. Review recent changes to system. Compare changes to system documentation to ensure that system documentation is current and valid. Ensure that there is a documented process in place for receiving security alerts and responding to them. Annotate the title of the procedure and the last date updated. Ensure that there is regular review of alerts by looking at evidence such as alert reports, emails, logbooks, etc.
2) ***Change Management:*** Ensure that the ASP has a change management process in place by obtaining a list of changes to the client's system/environment within the last X months. Obtain sample copies of client related change from each category: OS changes, application changes, hardware changes and firewall changes. Ensure that each change contains a description of and reason for the change, client and other approval, fallback/back-out plans. Ensure there are SoD present within in the changes in that the requestor of the change would not be allowed to approve it. Save copies of change management forms or document change numbers, dates that changes took place, a brief description of the change and whether the change was successful and retain as evidence.
3) ***Operating System:***
    a. *Hardening:* Ensure that servers have been hardened by compare system configuration documentation to hardening guidelines/templates. If no documentation is maintained then randomly select a system and check the following items below. Review the results of the Nessus scan performed in test ten of the T-I, General Audit section. Note any warnings or holes found in the scan.

    b. *Services: Ensure that services running are appropriate by doing the following tests below.*

Microsoft
UNIX/Solaris

Test b-1: Verify appropriate services are running by running SuperScan as follows:

1) If there are more than one IP create text file of servers that need to be scanned.
2) Open scanner either enter in the IP of the server or click on "Read IP's from file".
3) Click on the file that was previously created then click Open.
4) Verify the IPs were imported correctly in the scanner.
5) Click on host service and discovery tab. Ensure that it is set to scan at least ports 1-1024.
6) Click on arrow to start.
7) Review results. Compare results with configuration documentation to ensure appropriate services are running. Ensure that no Trojan ports are running. Compare unidentified open ports with port definition lists.
8) Take a screen capture as evidence. Save to evidence folder/repository or print a hardcopy.

Test b-1: Verify the appropriate services are running by doing the following:

1) Go to a command prompt on the system to be audited and type the following:

```
[root@oscarspc] # netstat –a > oscar
[root@oscarspc] # more oscar
```

2) Review results. Compare results with configuration documentation to ensure appropriate services are running. Ensure that no Trojan ports are running. Compare unidentified open ports with port definition lists.
3) Save either a screen capture of the output or the file that was created "oscar" in the evidence folder/repository or print a hardcopy.

Test b-2: Verify the appropriate services are running by doing the following:

T-III. Logging		Risk:	
General Reference(s): Personal Experience Controls T-03 – T-05 Personal Experience NIST SP 800-18 NIST SP 800-26 British Standard (BS) 7799-1 ISO 17799 Understanding Windows Logging – *by windowsecurity.com*	**HIPAA:** 164.312(b)	**SOX:** XII	**21 CFR 11:** 11.10e

Test Procedures/Compliance Criteria:

General Audit:

1) *Content:* Ensure that logs have limited access and that the access to them is "read only" so they can't be overwritten by checking permissions on log files. Ensure that logs are chronological by reviewing a sample of logs and viewing timestamps. Ensure that the log configuration is capturing the content as instructed by the client such as accesses to a particular file, timestamps, operator actions (print, create, modify…). Review the logs and note any dissimilarity between what is being logged and what is expected. Ensure that the client's critical applications (webserver, database) are being logged by obtaining and reviewing the logs. Retain all logs as evidence. Ensure that systems are logging events such as failed logins, failed services, configuration file alterations, errors, security events by checking the event viewer in Windows and var/admin, var/admin/messages, var/log and var/log/btmp in UNIX. Save all log files as evidence.
2) *Manual Logs:* Ensure that client system access logs are appropriately filled out if done manually by obtaining the log and validating the name on the log with the organization chart. Also, validate the any change or service request/ticket in the log to actual work performed.(troubleshooting, hardware swap, new employee account). Ensure that manual logs can't be overwritten. (Permanent ink vs. pencil) Obtain a copy for evidence purposes.
3) *Regular Review:* Ensure that there is a dedicated employee or a team of employees that regularly reviews the client's logs. Document names of reviewers and review schedules and what types of logs they are responsible for viewing. *(Security logs, performance logs, error logs)*
4) *Log Audit Review:* After all tests have been performed in sections A, T and P request the following logs: access logs showing the auditor's attempted failed access, IDS and firewall logs to ensure Nessus and port scan data was logged. These tests ensure that logging is appropriately configured. Retain a copy of these logs as evidence.
5) *Retention/Rotation:* Ensure that access logs are kept for an adequate timeframe by asking for samples. The definition of "Adequate" will depend on the client. For example HIPAA related documents should be kept for six years whereas Hazardous materials records should be kept for thirty years. Annotate the timestamps and save the logs as evidence.

HIPAA:

1) *164.312(b) – Unique User ID*:
    a. Ensure that all user activity is logged by selecting a random sample of logs and reviewing them. Correlate user ID's with system users. Ensure that logs demonstrate the use of unique user IDs.
    b. The auditor should access the system or have someone access the system to create, modify, delete and print a record. Ensure that system activity is being logged by reviewing logs thereafter.

SOX:

1) *XII* – Tests one and three of the T-III, General Audit section, address these controls.

21 CFR 11:

1) *11.10e* – Test five of the T-III, General Audit section, addresses these controls.

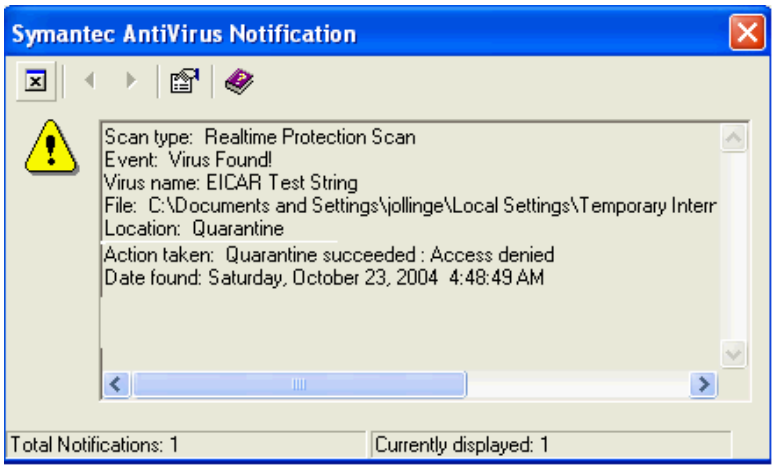
T-IV. Anti-Virus		Risk:	
General Reference(s): Personal Experience Controls A-01 through A-06 Personal Experience NIST SP 800-18 NIST SP 800-26 British Standard (BS) 7799-1 ISO 17799	**HIPAA:** 164.308(a)(5)	**SOX:** VIII, IX	**21 CFR 11:** 11.10c

Test Procedures/Compliance Criteria:

General Audit:

1) *Quality Records*: Review all quality documents ensuring that anti-virus related policies and procedures exist and are updated on a regular basis. (Topics to look for include: updating definition files, enabling/disabling/uninstalling protection, quarantining) Verify that downloading software directly from the internet to the client's system is prohibited. Verify that viewing email on the client system or opening attachments is prohibited. Verify that installing untested or unapproved software on the client's system is prohibited.
2) *Client System Checks:* Randomly choose a sampling of servers from the client's environment (see Identifying Systems to Be Audited section above) and ensure that anti-virus protection is installed and enabled. Verify that the system has the latest definition files by reviewing configuration. Verify that the anti-virus service is running by checking services. Verify the service is configured to automatically obtain updates. If a manual process is in place ensure that all updates are logged. Review logs to ensure that updates are happening in a timely manner.
3) *Virus Download Check:*
    a. 1. Go to the following website to download the test virus: http://www.eicar.org/anti_virus_test_file.htm
    b. Click on any of the following options:

    c. Ensure that the anti-virus program captured and quarantined/removed the virus. Take a screen shot as evidence that file was quarantined or removed successfully.



HIPAA:

1) *164.308(a)(5) – Protection from Malicious Software:* Tests found in section T-IV, General Audit should adequately address this.

SOX:

1) *VIII* – Tests found in section T-IV, General Audit should adequately address this.
2) *IX* - Tests found in section T-IV, General Audit should adequately address this.

21 CFR 11:

11.10c - Tests found in section T-IV, General Audit should adequately address this.

T-V. Logical Access Control		Risk:	
General Reference(s):	**HIPAA:**	**SOX:**	**21 CFR 11:**
Personal Experience Controls T-13 through T-16 Personal Experience NIST SP 800-18 NIST SP 800-26 British Standard (BS) 7799-1 ISO 17799 DumpSec - *SomarSoft Utilities*	164.308(a)(1) 164.308(a)(4) 164.308(a)(5) 164.312(a)(1)	VIII, IX	11.100a 11.100b 11.200a 11.300a 11.300b

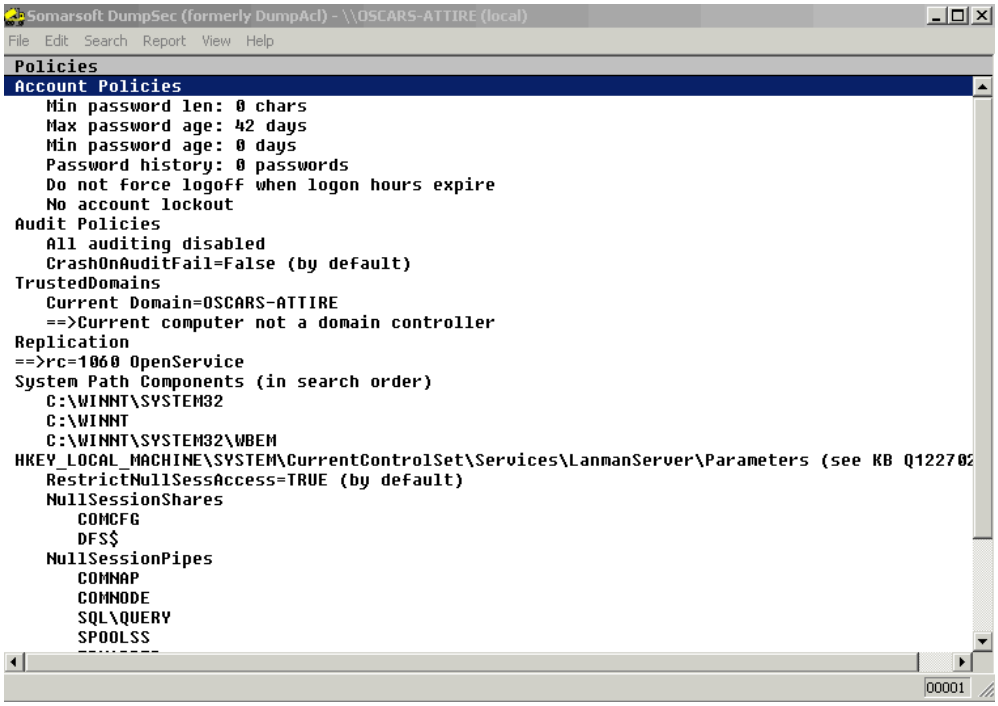
Test Procedures/Compliance Criteria:

General Audit:

1) *Quality Records*: Review all quality documents ensuring that access control related policies and procedures exist and are updated on a regular basis. (Topics to look for include: requesting user accounts, data classifications, administrative accounts, passwords, access logging, account review.) Verify that there is a procedure for requesting an account. Verify there is a password policy in place. Verify that there is a procedure in place for requesting passwords be reset. Verify there is a policy in place that controls access to data based on data classification and SoD. Verify there is a procedure in place to review accounts on a regular basis. Request copies of title pages, tables of contents, version tracking, dates and approvals of all aforementioned quality records. If copies are unavailable document the title, version number, approval names and dates. Retain copies or documentation as evidence.

   Ensure that policies on the client's systems follow written security policies by doing the following:

   - ✓ *Open DumpSec Tool.*
   - ✓ *Go to the Reports Menu.*
   - ✓ *Click on to Dump Policies.*



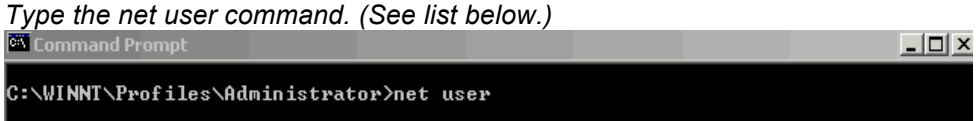
   - ✓ Save output and note any of the following:
     - Minimum password length not set.
     - Maximum age is not set or time does not meet client's requirements.
     - Minimum password age is not set.
     - Password history is not set.
     - Account lockout is not set.
     - No forced logoffs for inactivity.
     - No auditing

Prior to performing tests 2-9 the following should be done:

Obtain Windows User Accounts: Use the Net User Command to obtain user accounts.

a) *Go to a command prompt.*

b) *Type the net user command. (See list below.)*



T-VI. Internal/Third Party Assessment		Risk:	
General Reference(s): Personal Experience Controls A-01 through A-06 Personal Experience NIST SP 800-18 NIST SP 800-26 British Standard (BS) 7799-1 ISO 17799	**HIPAA:** 164.308(a)(1)	**SOX:** 31, IX	**21 CFR 11:** 11.300e

Test Procedures/Compliance Criteria:

General Audit:

1) *Internal Audit:* Obtain any results from internal audits that are performed to client systems. Ensure that client systems are audited on a regular basis. Document dates, methods/types of audit, tools used, results and corrective actions taken.
2) *Third Party Assessments:* Obtain any results from third party audits that are performed to client systems or on the ASP. Ensure that client systems were audited during the third party assessment. Document dates, method/type of audit, tools used, results and corrective actions taken.
3) *Risk Assessment:* Ensure that a risk analysis has been performed on client system by viewing documentation. Ensure that risk management has taken place by reviewing corrective actions and mitigation.
4) *Vulnerability Assessment:* Obtain any results from vulnerability assessments performed on client systems and perimeter devices. Ensure that client systems and perimeter devices are assessed for vulnerabilities on a regular basis. Document dates, methods of audit, tools used, results and corrective actions taken.
5) *Certifications:* Review any certification materials such as SAS70, type I or II, SysTrust…document dates of testing period to ensure that they are current. Document controls tested.

HIPAA:

1) *164.308(a)(1) –Security Management Process* - Test three in the T-VI, General Audit section addresses risk management issues.

SOX:

1) *31 – Communication of Management Aims and Directions:* Tests one through five in the T-VI, General Audit section addresses assessment. Ensure that these tests focus on compliance with policies, procedures and standards.
2) *IX* - Tests one through five in the T-VI, General Audit section addresses assessment. Ensure that these tests focus on assessing software and network infrastructure.

21 CFR 11:

1) *11.300e* - Tests one through five in the T-VI, General Audit section addresses assessment. Ensure that these tests focus on the testing of "tokens or cards that bear or generate identification codes or password information to ensure they function properly and have not been altered in an unauthorized manner."[12]

T-VII. Backup & Storage		Risk:	
General Reference(s): Personal Experience Controls T-18 through T-19 Personal Experience NIST SP 800-18 NIST SP 800-26 British Standard (BS) 7799-1 ISO 17799 General Recordkeeping Requirements - *Work-In-Texas.com*	**HIPAA:** 164.308(a)(7) 164.310(d)	**SOX:** XI, XII	**21 CFR 11:** 11.10c

Test Procedures/Compliance Criteria:

General Audit:

1) *Quality Records*: Review all quality documents ensuring that backup related policies and procedures in regards to the client's systems/data exist and are updated on a regular basis. (Topics to look for include: partial/full backups, method, frequencies, storage, recovery, segregation of duties SoD, logical and physical access and restoration) (Are key systems identified and documented? Are critical files such as logs, database files and system configuration files identified in backup documentation?)
2) *Back up*: Ensure that back-up agents are installed on all critical client systems that require backups and that they are being performed by doing the following:
    a. Check system configuration particularly cron jobs or scheduled tasks for evidence of scheduled backups.
    b. Choose random dates and request logs from those dates. Check backup logs and document the following: client system that was backed up, the type of backup, the size of the backup, the date and time of the backup, and what tape/device it was on.
    c. Choose random dates and request logs from those dates. If backups are done manually review logs for the same entries in the latter section to ensure backups are being performed.
3) *SoD*: Obtain a list of all appropriate persons with access to backup tapes. Obtain a list of appropriate persons that can authorize recalls. Review organization charts and job descriptions to ensure that backup/restore responsibilities are assigned appropriately.
4) *Logging*: Ensure that backup logs are being maintained. Review entries to ensure that logs indicate backups have occurred. For example if the Windows Backup Utility is used review the logs for dates/times of backup events.
5) *Storage*: Ensure that backup tapes are being stored properly. P-I addresses this adequately. Request to see a backup tape ensuring that it is not labeled with client's name, it is not warm to the touch indicating that it may be stored in an improper environment, that it is not worn out or damaged looking in any way.
6) *Testing and Recovery*: Ensure that backups are being tested by reviewing test plans and documentation. Review client requests for recovery, tracking of the restoration efforts and results. If recovery has taken place recently and the process was adequate then no further testing is needed.
7) *Retention:* Ensure that backups are retained for as long as client has requested. For example HIPAA related documents should be kept for six years whereas hazardous materials records should be kept for thirty years. Test this by requesting a sample restore based on the contracted retention time. Document retention periods and the length of time it took from request to recovery and retain as evidence.

HIPAA:

1) *164.308(a)(7) – Data Backup Plan, Disaster Recovery Plan*: T-VII, General Audit test one and six address this.
2) 164.310(d) – *Data and Backup Storage*: Tests six and seven in the section T-VII, General Audit address this.

SOX:

1) *XI* – T-VII, General Audit test one addresses this.

2) *XII* - T-VII, General Audit test one and six address this. Ensure that retention of backup tapes/images meets the criteria of the SOX. Definitions for retention may depend on the types of data/records being stored. Ensure that key data and files are being regularly backed up by requesting a restore. Ensure that keys and certificates are being backed up as per the client contract and document their retention period.

21 CFR 11:

1) 11.10c - Tests six and seven in the section T-VII, General Audit address this.

Gap Analysis

The next table represents regulatory topics or controls which are either not referenced or have not been thoroughly tested in the checklists above. Mostly they are controls specific to a regulation, therefore could not be generally addressed. For example, HIPAA regulation 164.308(a)(2) states that the controlling entity (CE) assign an individual as the HIPAA Security Officer.[13] This could not be directly mapped to a stated control.

Table F.3: Gap Analysis

HIPAA	SOX	21CFR11
164.308(a)(2) 164.308.(a)(3) 164.308(b)(1) 164.312(e)(1)	▪ IT Strategic Planning ▪ Risk Assessment ▪ Manage Performance and Capacity ▪ Monitoring ▪ Adequacy of Internal Control ▪ Independent Assurance ▪ Internal Audit	11.10(a) 11.10(b) 11.10(f) 11.10(g) 11.10(h) 11.10(k) 11.30 11.50(a)(b) 11.70 11.200(a)(b)

Some other topics that the auditor may want to address that weren't in the scope of this document are: wireless, modems, encryption, two-factor authentication, VPN, VLAN, switches, tokens and printers/fax.

G. Conducting the Audit, Testing, Evidence Findings

Audit Steps

The information presented above, along with the steps described below should equip the auditor with the necessary expertise to conduct an ASP audit. To recap the steps above and tie in the steps below, the following table has been created.

Table G.1: Audit Steps

Step #	Step	Resources Provided
I.	**Research the ASP and Client**	Guidance only
II.	**Determine the Scope of the Audit**	Pre-Audit Questionnaire, Guidelines/Regulations/Standards References
III.	**Identify the Systems to be Audited**	Guidance only
IV.	**Conduct the Risk Assessment**	Threat, Vulnerability, Asset and Risk Assessments

V.	**Develop Controls**	Current State of Practice references, List of sample controls, Control Mapping to HIPAA, Sarbanes-Oxley 404/COBIT and 21 CFR 11
VI.	**Create a Checklist**	Sample checklist, Example of an ASP Checklist
VII.	**Gather Information/Evidence**	Pre-Audit Documentation Checklist
VII.	**Create a Toolbox**	Tool Mapping with recommended tools
IX.	**Conduct the Assessment**	Audit Documentation Request List
X.	**Audit Reporting**	Guidance only

Gathering Information/Research

Prior to any field work it is essential that the auditor do as much preparation work as possible. The auditor must ensure that all the necessary legal agreements are in place by confirming that there is a non-disclosure agreement between the client and the ASP and a non-disclosure agreement between the client and the auditor.

Depending on the policies of the ASP and their relationship with the client, it may not be possible to obtain documentation prior to fieldwork. If this is the case, then it is imperative that the auditor be organized and prepared ahead of time. It wouldn't be efficient for the auditor to bring a list of what is needed the day of the audit. It is recommended that the auditor provide the ASP with a list of needs at least a week before the audit. This will give the ASP ample time to gather and prepare materials so when the auditor appears onsite they are ready for the audit to begin.

The examples provided in the Creating a Checklist section will help the auditor in creating a customized list of requirements for the audit. If the client requests a conformance type of audit then the auditor can extract tests from the quality records/documentation sections. If the audit is more of a vulnerability assessment and more technical in nature, then several of the tools and tests mentioned in the checklist can be used. Unfortunately, there is no "cookie cutter" type of approach to conducting an audit. Each audit will be differently designed and conducted, however the processes are generally similar.

A sample of what is needed is provided below. It can be tailored to fit the auditor's needs. It is recommended that the client be the liaison between the auditor and the ASP, therefore the auditor should send the list to the client. This will keep the client thoroughly involved in the audit process.

Illustration G.1: Pre-Audit ASP Documentation

ASP Documentation that will be needed prior to audit:

- ✓ Completed preliminary questionnaire
- ✓ Organization chart
- ✓ Job descriptions of employees who support the client's systems.
- ✓ Network Diagrams
- ✓ Awareness training materials
- ✓ Policies and procedures on the following topics:
    a. Security (Information and physical)
    b. Acceptable Use
    c. Ethical Conduct
    d. Data Classification
    e. Access Control
    f. Passwords
    g. Anti-virus
    h. Workstation/Laptop
    i. Hardening/Configuration
    j. Wireless
    k. Application/Database
    l. Contractor
    m. Vendor
    n. Hiring/Termination
    o. Backup
    p. VPN
    q. Incident response
    r. Segregation of Duties
    s. Inventory
    t. Change management
    u. Quality Assurance
- ✓ Maintenance contracts or agreements for:
    a. Fire suppression systems
    b. UPS/Generators
    c. Power Company
    d. HVAC
- ✓ System configuration (Choose sample)
    a. Application configuration
    b. OS Configuration
- ✓ Tracking (service request, ticket)
- ✓ Detailed permission to run vulnerability assessment.
- ✓ Permission to test physical security access.

Creating a Toolbox

Mapping Tools to Controls

Mapping the tools to the controls that will be tested will help the auditor determine the nature of the tests. Generally when tools are used they have objective output.

Table G.2: Mapping Controls to Tools

Control	Tool Used
T-01 Applications are configured and tested prior to being implemented	N-Stealth (web vulnerabilities only)
T-02 – Operating systems are hardened.	Nessus, SuperScan, netstat, Sun Patch Reporter, Hfnetchk, MBSA
T-06 – Systems are current on service packs and patches.	Sun Patch Reporter, Hfnetchk, MBSA
T-09 – An anti-virus system is implemented.	EICAR
T-11 – Perimeter devices are used and configured securely.	RAT, Nessus, NMAP
T-12 – All devices are configured appropriately and all deviations are documented.	Nessus, SuperScan, netstat, Sun Patch Reporter, Hfnetchk, MBSA
T-13 Access control mechanisms on devices are used.	Net User, DumpSec
T-14 Shared accounts are not used.	Net User, DumpSec
T-15 Complex passwords are used.	John the Ripper
T-16 Password controls are in place.	John the Ripper

During the evidence gathering phase, prior to entering the ASP, the auditor should install and test all of the tools that they will need during their onsite visit. A list of tools and their source is provided below:

Table G.3: Recommended Audit Tools

Recommended Tool	Source
Nessus	http://www.nessus.org/download.html
SuperScan	www.foundstone.com/resources/freetools.htm
netstat	Installed with Windows.
Sun Patch Reporter	http://www-uxsup.csx.cam.ac.uk/~pjb1008/project/patchsun/
Hfnetchk	http://www.majorgeeks.com/download1103.html
MBSA	http://www.microsoft.com/technet/security/tools/mbsahome.mspx
EICAR	http://www.eicar.org/anti_virus_test_file.htm

RAT	http://www.cisecurity.org/bench_cisco.html
NMAP	http://www.insecure.org/nmap/nmap_download.html
Net User	Installed with Windows.
DumpSec	http://www.somarsoft.com/somarsoft_main.htm
John the Ripper	http://www.openwall.com/john/
N-Stealth	http://www.nstalker.com/eng/products/nstealth/
Pete Finnigan Tools	Oracle Specific Audit Tools: http://www.petefinnigan.com/tools.htm
SQLdict	SQL Specific Audit Tool (passwords only): http://ntsecurity.nu/toolbox/sqldict/
HardCopy Pro – (*This little tool is HIGHLY recommended for taking screenshots.)*	http://www.desksoft.com/HardCopy.htm

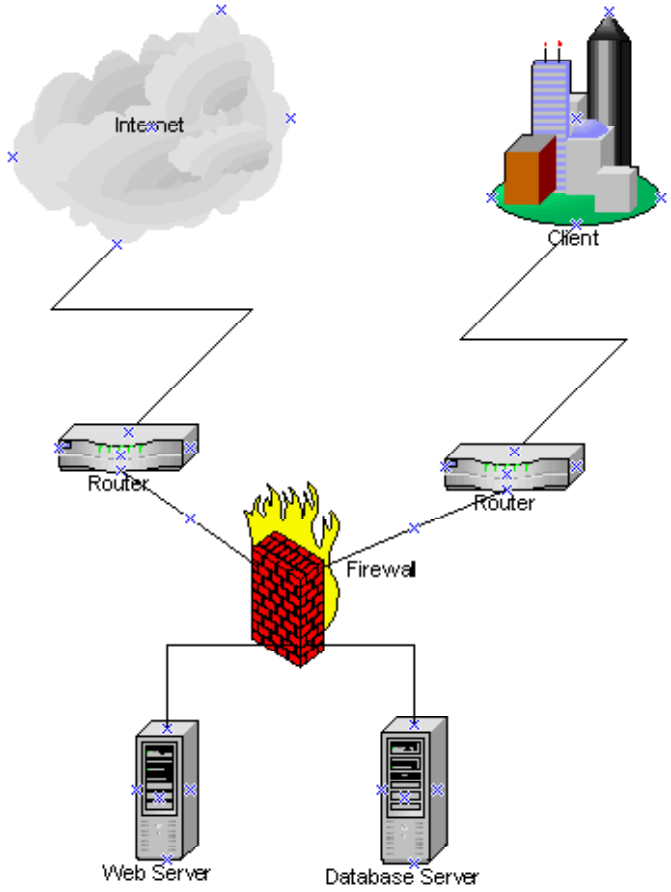
Once all of the preliminary research has been completed and materials have been gathered and checked against the checklists above, the auditor should create a "game plan" of remaining items that will need to be addressed. The plan should include the scope of the audit, a schedule, and a list of remaining checklist items. It is recommended that the ASP receive this list prior to the on-site visit. It will help the ASP prepare and ensure that the correct Subject Matter Experts (SMEs) are available.

Conducting the Assessment

Once the tools are installed the auditor can begin doing some preliminary assessments like running a port or vulnerability scan against the client's environment. This can be done prior to fieldwork. Permission from the ASP will need to be obtained prior to the start of the scan. The ASP will most likely need to know: when the scan will start and stop, the IP address the scan will be coming from, the tools that will be used, and the targeted systems. The auditor shouldn't be discouraged if the ASP doesn't allow vulnerability assessments on shared devices such as routers and firewalls, as this is likely due to the impact it may have on other clients.

As stated in *T-1, General Audit - Test 10: Perimeter Vulnerability Assessment,* the Nessus scan should be run twice to ensure coverage of all entry points into the client's environment. This is dependent on the client's connectivity. If the client has a dedicated connection (ie. circuit or private VPN) to access their systems at the ASP and their applications are not internet facing, then the internet scan is unnecessary. However, if the client's systems are internet facing like in the diagram below, then the auditor must do two separate assessments.

Illustration G.2: Covering All Entry Points



Fieldwork

With tools, checklists and an agenda in hand the auditor should be prepared for fieldwork. Prior to fieldwork the auditor should ensure that the appropriate people are invited to the entrance conference. The auditor should request that relevant SMEs, which will be dependent on the audit objective, attend to answer particular questions. For example, if the audit topic is on the change management process, the auditor should be sure that a SME on the change management process is invited to the entrance conference. The auditor should always remember, the more prepared they are, the smoother the audit will go.

Testing the Controls

Although it is preferred, it is not necessary that the auditor perform the objective tests themselves. If the checklist is detailed enough, it can be handed over to one of the ASP's employees so they can perform the tests while the auditor supervises. This method will ensure that the ASP has a full grasp of what the auditor is trying to achieve while maintaining control.

Audit ASP Documentation

Documentation will also be needed during the audit. Samples will be requested during the audit time. It is also recommended that the ASP receive a copy of

this list as well, so there are no surprises.

Illustration G.3: Audit Documentation

Documentation and other samples that will be needed during the audit:

- ✓ All previously requested documents
- ✓ Employee training samples
- ✓ Job descriptions of employees who support the client's systems.
- ✓ Log files from tests (IDS, server, firewall, security system)
- ✓ Change control tickets/tracking
- ✓ Problem Tickets/Service Requests]
- ✓ Backup tapes
- ✓ Restoration of data
- ✓ Users with access to client data
- ✓ User access control requests and authorizations

Access that will be needed for audit:

- ✓ Access to client systems or assistance from an employee to run tools/commands to gather data.
- ✓ Access to view generator, fire suppression, HVAC and room where backup tapes are stored.
- ✓ Ability to view physical access control procedures to client's systems.
- ✓ Ability to view where security equipment is kept. (firewalls, IDS, badge making equipment, keys.

The checklist can now be completed with the information obtained from the fieldwork, testing, and audit documentation. After all of the evidence is documented, the exposure can then be ascertained, which will assist in determining the risk. The auditor can also establish methods of mitigating the risk(s) by using best security practices and established controls. An example of how to document the evidence, risk and mitigation in the provided checklist is provided below.

Illustration G.4: Evidence and Audit Findings Example

T-II. Configuration Management	**Risk: HIGH**
T-06 Patch Management Evidence: ▪ The security organization reviews security alerts but it is not a formally documented process, nor is it consistent. A vulnerability report was distributed on a weekly basis, but the person in charge of that has since left the company therefore the report creation and distribution has ceased. (Witnessed last documented report: "Vulnerability Report from 2/18/01 – 2/24/01") ▪ Ran Microsoft Baseline Security Analyzer (MBSA) on Oscar12 (192.168.1.3) - 6 critical security updates are missing, 1 product (MSXML)	
Pass/Fail: FAIL	
Mitigation: Revive weekly vulnerability reports. Document a formal process for responding to alerts. Apply all security updates.	
Notes: Exposure is high since the client's server is internet facing and since the ASP has not applied the latest security patches.	

Once the checklist is completely filled out, the auditor can prepare the report.

H. Audit Reporting

The format of the report may take on many forms. Depending on the audience, it may be presented in a document, spreadsheet or slide show. Whichever that format may be, it should contain an executive summary of the audit, the audit findings and the audit recommendations.

Executive Summary

It is suggested that this section be written last. It should contain a summary of the audit and should include the overall audit objective, the scope of the audit and it should briefly state if the audit objectives were met. This section should also include positive feedback on the controls that were in place during the audit, which will make the results more palatable to the audited ASP and provide some level of comfort to the client. Here is an example of how to present a summary of the information:

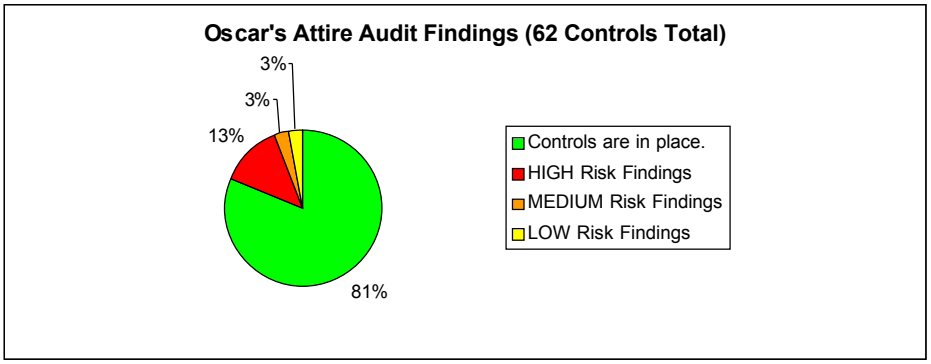
Table H.1: Audit Findings Summary

Oscar's Attire Overall Audit Summary	% of Controls (62 Controls Total)	Recommended Actions:
Controls are in place.	81%	No further action needed.
HIGH Risk Findings	13%	Should be addressed in 2 weeks.

MEDIUM Risk Findings	3%	Should be addressed in 1 month.
LOW Risk Findings	3%	Should be addressed within the next 6 months.

Charts are recommended to further assist in presenting the information.

Illustration H.1: Audit Findings Summary Chart



Audit Findings

In the Audit Findings section of the report the auditor should present the results of the audit. They should detail what was tested and the results of the tests. The Risk, Pass/Fail and Mitigation sections of the checklist are useful in writing this section of the report. Here is an example of how to present the information:

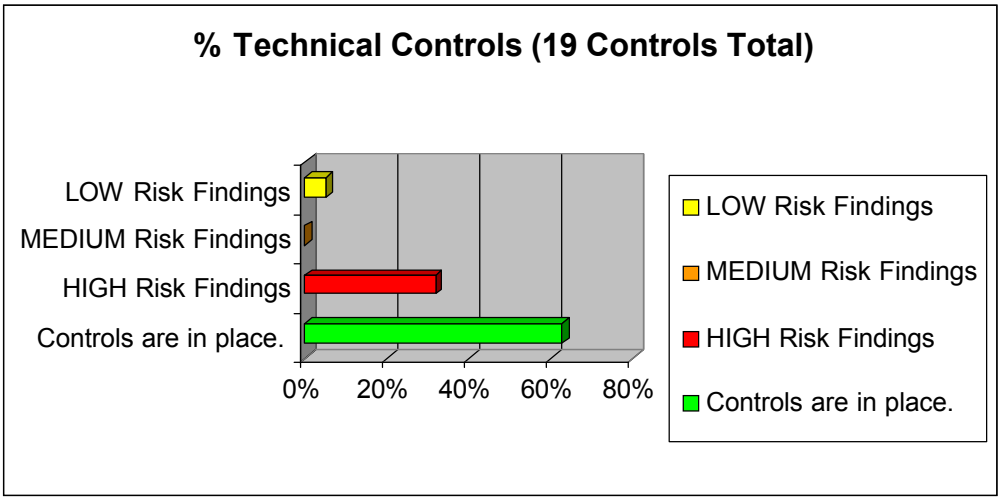
Table H.2: Technical Audit Findings Summary Example

Technical Audit Summary	% of Controls (19 Controls Total)	Recommended Actions:
Controls are in place.	63%	No further action necessary.
HIGH Risk Findings	32%	Should be addressed in 2 weeks.
MEDIUM Risk Findings	0%	Should be addressed in 1 month.
LOW Risk Findings	5%	Should be addressed within the next 6 months.

Table H.2 introduces the audience to the overall summary of the audit.

Charts should be used to reinforce and summarize points.

Illustration H.2: Technical Audit Findings Chart Example



Details of each audit major control, test and finding should be provided.

Table H.3: Detailed Technical Findings Example

Control	Test	Finding	Exposure	Calculated Risk
T-06: Systems are on current service packs and patches.	T-II Configuration Management: Test d-1: Ran Microsoft Baseline Security Analyzer (MBSA) on Oscar12 (192.168.1.3)	6 critical security updates are missing, 1 product (MSXML)	**HIGH**	**HIGH**

Audit Recommendations

The “Mitigation” section of the checklist is used for documenting recommendations on how to eliminate or reduce the risk. The mitigation steps found in the checklist should be represented in the report. They should be clear, understandable steps. In the example below the mitigation steps are general.

It is suggested that the ASP be given a remediation deadline, however the client may choose to change this deadline to meet their particular needs.

Table H.4: Mitigation Example

Control	Finding	Exposure	Calculated Risk	Mitigation
T-06: Systems are on current service packs and patches.	6 critical security updates are missing, 1 product (MSXML)	**HIGH**	**HIGH**	Update system with necessary security updates within the next two weeks.

The auditor may find themselves presenting the findings to the ASP at the client’s request. Regardless of who presents the report to the ASP, it should be clear and concise. This guide will help the auditor to achieve these objectives.

III. References

[1] Lynn Haber, "ASPs Still Alive and Kicking", (ASPnews.com) January 30, 2004 URL: http://www.aspnews.com/trends/article.php/3306221

[2] Marianne Swanson "Security Self-Assessment Guide for Information Technology Systems", Special Publication 800-26, (Washington: National Institute of Standards and Technology – Technology Administration US Department of Commerce, US Government Printing Office, November 2001) page iv., August 2004
URL: http://csrc.nist.gov/publications/nistpubs/800-26/sp800-26.doc

[3] The Sarbanes-Oxley Act Community Forum, September 2004, URL: www.sarbanes-oxley-forum.com

[4] The Sarbanes-Oxley Act Community Forum, September 2004, URL: www.sarbanes-oxley-forum.com

[5] Julie Baumler, Susan Bradley, Stephen Brown, Barbara Filkins, Brian Granier, Robert Happy Grenert, Chad Gross, Wayne Haber, Jason Hilling, Dave Jahne, Ed Mendez, Russell Meyer, Denis Piliptchouk, Olivia Rose, Adam Stone, Laura Taylor, Denise Turner, Russell Walker, Steve Weil, Allen Zhang, HIPAA Security Implementation, Version 1.0, SANS Step-by-Step Series, SANS Press, 2003, page 14.

[6] Julie Baumler, Susan Bradley, Stephen Brown, Barbara Filkins, Brian Granier, Robert Happy Grenert, Chad Gross, Wayne Haber, Jason Hilling, Dave Jahne, Ed Mendez, Russell Meyer, Denis Piliptchouk, Olivia Rose, Adam Stone, Laura Taylor, Denise Turner, Russell Walker, Steve Weil, Allen Zhang, HIPAA Security Implementation, Version 1.0, SANS Step-by-Step Series, SANS Press, 2003, page 1.

[7] Statement on Auditing Standards (SAS) No. 70, "About SAS70 – SAS70 Overview", September 2004, URL: www.SAS70.com

[8] Vigilar, PCI Data Security Standard, Consulting Services – Industry Organizations, March 2005,
URL: http://www.vigilar.com/sol_compliance_industry.html

[9] Gary Stonebaumer, Alice Goguen, Alexis Feringa "Risk Management Guide for Information Technology Systems", Special Publication 800-30, (Gaithersburg MD: National Institute of Standards and Technology – Technology Administration US Department of Commerce, Computer Security Division, July 2002) page 15, August 2004
URL: http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

[10] "21CFR11.10j", Code of Federal Regulations, Title 21, Volume 1, Subpart B - Electronic Records, Section 11.10 - Controls for closed systems, Subpart j, (Department Of Health And Human Services, Food And Drug Administration, April 1, 2004)
URL: http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/CFRSearch.cfm?fr=11.10

[11] Alan R. Mercer, "Device and Media Controls – Disposal", (SANS Institute Inc., SANS Reading Room, 2004, page 7)
URL: http://www.giac.org/practical/GHSC/Alan_Mercer_GHSC.pdf

[12] "21CFR11.300e", Code of Federal Regulations, Title 21, Volume 1, Subpart B - Electronic Records, Sec. 11.300 Controls for identification codes/passwords, Subpart e, (Department Of Health And Human Services, Food And Drug Administration, April 1, 2004)
URL: http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/CFRSearch.cfm?fr=11.10

[13] Julie Baumler, Susan Bradley, Stephen Brown, Barbara Filkins, Brian Granier, Robert Happy Grenert, Chad Gross, Wayne Haber, Jason Hilling, Dave Jahne, Ed Mendez, Russell Meyer, Denis Piliptchouk, Olivia Rose, Adam Stone, Laura Taylor, Denise Turner, Russell Walker, Steve Weil, Allen Zhang, HIPAA Security Implementation, Version 1.0, SANS Step-by-Step Series, SANS Press, 2003, page 20.

Other sources used in the creation of this document:

***SANS Reading Room Practicals and References**:*

Yolanda Martinez, "Auditing a Systems Security Consultant's Laptop Running Fedora Core 2", (SANS Institute Inc., SANS Reading Room, December 20, 2004)
URL: http://www.giac.org/certified_professionals/practicals/gsna/185.php

Don Murdoch, "Building a Secured OS for a Root Certificate Authority" (SANS Institute Inc., SANS Reading Room, 2004)
URL: http://www.sans.org/rr/whitepapers/honors/1487.php

SANS, Inc., "Small Business Checklist for Evaluating an ASP" (SANS Institute, Security Consensus Operational Readiness Evaluation (SCORE), REV 1.1 August 2003)
URL: http://www.sans.org/score/checklists/ASP_checklist.doc

Val Thiagarajan "Information Security Management - BS 7799.2:2002 Audit

Checklist for SANS", (SANS Institute Inc., SANS Reading Room, June 2003)
URL: http://www.sans.org/score/checklists/ISO_17799_checklist.pdf

"SANS Top Twenty List - The Twenty Most Critical Internet Security Vulnerabilities", Version 5.0, SANS Institute, October 2004
URL: http://www.sans.org/top20/

Joakim von Braun "Intrusion Detection FAQ - What port numbers do well-known trojan horses use?" (SANS Institute Inc., SANS Resources) October 2004
URL: http://www.sans.org/resources/idfaq/oddports.php

Ray Welshman, "Auditing a Cisco A Cisco 1721 Router: An Auditor's Perspective" (SANS Institute Inc., February, 2004)
URL: http://www.giac.org/practical/GSNA/Ray_Welshman_GSNA.pdf

SANS Information Security Reading Room, March 2005
URL: http://www.giac.org/GSNA.php

Other websites, documents, articles, and publications:

Laurie Sullivan, "History 101: Hosted Apps, From Time-Sharing To On-Demand", Information Week, June 21, 2004
URL: http://www.informationweek.com/showArticle.jhtml?articleID=22100717

Steve Winn, "The ASP Model", (RealPage, Inc. and KPMG Consulting, February 2001)
URL: http://www.realpage.com/company/news/whitepapers/dec_2000.pdf

Stewart McKie, Outsourcing With ASPs in the Internet Age (Business Finance Mag.com, Originally printed in *Business Finance, November 1999)*
URL:
http://www.businessfinancemag.com/magazine/archives/article.html?articleID=13186

William K. Hubbard, "Federal Regulation Doc. 03–4312" (Department Of Health And Human Services - Food And Drug Administration), February 20, 2003
URL: http://www.fda.gov/OHRMS/DOCKETS/98fr/03-4312.pdf

"Title 21 Code of Federal Regulations (21 CFR Part 11) Electronic Records; Electronic Signatures Final Rule", (Department Of Health And Human Services, Food And Drug Administration, Published in the Federal Register) March 2000
URL: http://www.fda.gov/ora/compliance_ref/part11/frs/background/11cfr-fr.htm

Julie Baumler, Susan Bradley, Stephen Brown, Barbara Filkins, Brian Granier, Robert Happy Grenert, Chad Gross, Wayne Haber, Jason Hilling, Dave Jahne,

Ed Mendez, Russell Meyer, Denis Piliptchouk, Olivia Rose, Adam Stone, Laura Taylor, Denise Turner, Russell Walker, Steve Weil, Allen Zhang, HIPAA Security Implementation, Version 1.0, (SANS Step-by-Step Series, SANS Press), 2003, page 30.

21CFR11.com, Waters Corporation, October 2004
URL: http://www.21cfrpart11.com/

Tim Grance, Karen Kent, Brian Kim, "Computer Security Incident Handling Guide", NIST Special Publication 800-61, Formerally SP 800-3, (Gaithersburg, MD: National Institute of Standards and Technology – Department of Commerce, Computer Security Division, January 2004)
URL: http://csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf

Chris Prosise, Kevin Mandia, Matt Pepe, Incident Response and Computer Forensics, Second Edition (Emeryville, CA: McGraw Hill/Osborne, 2003)

CERT Coordination Center, Carnegie Mellon – Software Engineering Institute, September 2004
URL: http://www.cert.org/nav/index_red.html

BugTraq Archive, Security Focus, September 2004
URL: http://www.securityfocus.com/archive/1

Marianne Swanson, Amy Wohl, Lucinda Pope, Tim Grance, Joan Hash, Rav Thomas, "Contingency Planning Guide for Information Technology Systems", NIST SP 800-34 (Washington: National Institute of Standards and Technology – Department of Commerce, Technology Administration, June 2002)
URL: http://csrc.nist.gov/publications/nistpubs/800-34/sp800-34.pdf

"Physical Security Audit Checklist", Protiviti Inc., September, 2004
URL:
http://www.knowledgeleader.com/iafreewebsite.nsf/content/TechnologyAuditPhysicalSecurityAuditChecklist?OpenDocument

"Physical Security Checklist", TeCrime International, Inc., September 2004
URL: http://www.tecrime.com/0secure.htm

"Internal Control Checklist", Office of Financial Management (OFM), September 2004
URL: http://www.ofm.wa.gov/policy/icckIfa.htm

"RU Secure – Security Checklist", Rutgers The State University of New Jersey, October 2004
URL: http://rusecure.rutgers.edu/sec_plan/checklist.php

"SuperScan", Foundstone, October 2004
URL:
http://www.foundstone.com/index.htm?subnav=resources/navigation.htm&subcontent=/resources/freetools.htm

"Port Numbers", Internet Assigned Numbers Authority (IANA), October 2004
URL: http://www.iana.org/assignments/port-numbers

"Microsoft Baseline Security Analyzer", Microsoft Inc., October 2004
http://www.microsoft.com/technet/security/tools/mbsahome.mspx

"Disabling Network Services on UNIX", System and Network Security, University of California, Berkeley, October 2004
URL: http://security.berkeley.edu:2002/MinStds/Disabling-Unix.html

"UNIX/Linux Security Best Practices", University of Virginia, Information Technology and Communication Division, October 2004
URL: http://www.itc.virginia.edu/unixsys/sec/

"Common UNIX Services to Disable", York University, October 2004
URL: http://infosec.yorku.ca/Administrators/UNIX_disable.html

Ricky M. Magalhaes, "Understanding Windows Logging", Windows Security.com, July 2004
URL:
http://www.windowsecurity.com/articles/Understanding_Windows_Logging.html

Dr. Nikolai Bezroukov, "Log Analysis and Auditing", Softpanorama, October 2004,
URL:
http://www.softpanorama.org/Logs/log_auditing.shtml#Recommended%20Links

"Hardcopy Pro", DeskSoft, October 2004
URL: http://www.desksoft.com/HardCopy.htm

Vanessa Antoine, Raymond Bongiorni, Anthony Borza, Patricia Bosmajian, Daniel Duesterhaus, Michael Dransfield, Brian Eppinger, Kevin Gallicchio, James Houser, Andrew Kim, Phyllis Lee, Tom Miller, David Opitz, Florence Richburg, Michael Wiacek, Mark Wilson, Neal Ziring, "Router Security Configuration Guide", Version 1.1, (Ft. Meade, MD: National Security Agency, Router Security Guidance Activity of the System and Network Attack Center (SNAC), September 2002)
URL: http://nsa2.www.conxion.com/cisco/guides/cis-2.pdf

"Dumpsec", SomarSoft Utilities, October 2004
URL: http://www.somarsoft.com/somarsoft_main.htm

"Router Audit Tool (RAT)", The Center for Internet Security, September 2004
URL: http://www.cisecurity.org/bench_cisco.html

Peter Benie, "SUN Patch Reporter", University of Cambridge, October 2004
URL: http://www-uxsup.csx.cam.ac.uk/~pjb1008/project/patchsun/

"General Recordkeeping Requirements", Texas Workforce, September 2004
URL:
http://www.twc.state.tx.us/news/efte/general_recordkeeping_requirements.html

"John the Ripper" Openwall Project, October 2004
URL: http://www.openwall.com/john/

"Default Password List", Phenoelit, March 2005
URL: http://www.phenoelit.de/dpl/dpl.html

Andy Cuff, "Database Vulnerability Scanners" Computer Network Defense Ltd, Talisker Security Wizardry, March 2005
URL: http://www.networkintrusion.co.uk/database.htm

Pete Finnigan, "Oracle Security Papers", PeteFinnigan.com, March 2005
URL: http://www.petefinnigan.com/orasec.htm

Ame Vidstrom, "SQLdict", Ntsecurity.nu, March 2005
URL: http://ntsecurity.nu/toolbox/sqldict/

"NGSSQuirreL for SQL Server (evaluation version)", Next Generation Security Software Ltd., March 2005
URL: https://www1.ngssoftware.com/?Action=Logon

*Please note: Throughout the document, the author used fictional names of businesses to illustrate points. Oscar happens to be the author's pug dog and Edison happens to be the author's cat.