Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Post Acquisition Audit in 30 Days

This paper will focus on how to establish a successful post acquisition audit and to ensure the key areas of risk are identified and reviewed. Although multiple areas of risk will be introduced which may include financial, legal, political, or economic, the emphasis will be around information security risks.

Copyright SANS Institute
Author Retains Full Rights

AD

© SANS Institute 2009, Author retains full rights.

Post Acquisition Audit in 30 Days

GSNA Gold Certification

Author: Brad Ruppert, bradruppert@gmail.com

Adviser: Jim Purcell

Accepted: May 3rd 2009

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

Contents

1. Abstract 4

2. Overview 4

3. Scope 5

4. Aligning with professional standards 5

5. Where to Start 7

6. Establish Stakeholders 8

7. Defining the Audit Scope and Objectives 8

8. Roles and Responsibilities 10

9. Developing the Audit Timeline 13

10. Documenting the Audit Work Program 14

11. Developing the Document Request List 24

12. High-level Steps to Executing the Audit 26

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

13. Conducting the Audit 29

14. Documenting the Observations 29

15. Developing the Audit Report 30

16. Closing out the Audit 31

17. Conclusion 32

18. References 34

Figures

Figure 1: Roles and Responsibilities 12

Figure 2: Audit Timeline 13

Figure 3: Sample Work Program 24

Figure 4: Sample Document Request List 26

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

1. Abstract

This paper will discuss the steps required to develop a high level risk-based post acquisition IT audit and means of conducting the audit in less than 30 days. Acquisitions are a common occurrence in any major corporation and it is imperative that an audit of the acquired business be conducted immediately following integration with the existing information systems. The post acquisition audit will help to identify any high risks areas specific to the newly acquired business, integration issues, or variances with existing information technology policies. The goal will be to provide an IT auditor with the initial framework to prepare a post acquisition audit and conduct it in an efficient and timely manner.

2. Overview

The key to performing a successful post acquisition audit starts by having a good understanding of the business, its current risks, knowing who the key stakeholders are, and having a defined set of deliverables. Knowing the business means having an understanding of revenue generating processes, management style, management hierarchy, business industry, company infrastructure, and internal / external influences. Understanding current risks will require knowledge of applicable laws and regulations, the business's financial standing, economic and environmental influences, and security risks specific to company assets.

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

Knowing the key stakeholders will be important when defining scope, objectives, and timeline of the audit which will ultimately be used when agreeing to the project deliverables.

3. Scope

This paper will focus on how to establish a successful post acquisition audit and to ensure the key areas of risk are identified and reviewed. Although multiple areas of risk will be introduced which may include financial, legal, political, or economic, the emphasis will be around information security risks. Technologies mentioned in this paper may not be the best solution for every organization depending on the size, budget, and flavor of systems being supported. The degree of difficulty required to establish a successful post acquisition audit will depend on the size of the company, number of employees, number of systems, locations of systems, and vendor types. The basic principles of this paper can be applied to any company looking to complete a post acquisition audit.

4. Aligning with professional standards

Organizations typically rely upon various IT solutions to meet their specific business requirements. Once these solutions are in production, post-implementation reviews are carried out by auditors to assess the effectiveness and efficiency of the solutions. These audits will

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

also review the implementation and initiate actions to improve the solution and serve as a learning tool for the future. The Control Objectives for Information and related Technology (COBIT) is a set of best practices that provides managers, auditors, and IT users with a set of generally accepted measures, indicators, and processes to assist with providing appropriate IT governance. In a post-acquisition audit, the first review after the implementation of an IT solution, the following processes are most relevant:

"—Define the Information Architecture
—Define the IT organization and relationship
—Manage the IT investment
—Ensure Compliance with External Requirements
—Assess risks
—Manage projects
—Manage quality
—Identify automated solutions
—Acquire and maintain application software
—Acquire and maintain technology infrastructure
—Install and accredit systems
—Manage changes
—Educate and Train Users
—Manage Data
—Monitor the processes
—Assess Internal Control Adequacy
—Obtain Independent Assurance
—Provide for Independent Audit" (ISACA, 2005)

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

5. Where to Start

Finding the right approach to a post acquisition audit begins by examining all the steps involved with the process. Some of the most important steps include: identifying stakeholders, outlining the scope and objectives, reviewing business requirements, understanding of roles and responsibilities, gathering policy and procedures, and agreeing to specific audit timelines. Identifying the goals of a post acquisition audit establishes objectives and outlines milestones, which is important throughout the audit process. Understanding roles and responsibilities ensures accountability, provides direction, and helps coordinate auditing efforts. Awareness and communication, the cornerstones of a successful audit program, are products of the lead auditor and his or her team. Obtaining policies and procedures creates a holistic view, clarifies objectives, defines roles and responsibilities, provides instruction, and outlines compliance. The details of what/where/when/how should be captured in the policies and procedure documentation to eliminate confusion, establish routine, provide guidance, and to enable practices to be auditable. Establishing the audit timelines is important not only to the auditor but also the key stakeholders. The lead auditor will need to formally communicate the proposed audit process, time spent planning, estimated time conducting fieldwork, and time for closing the audit and providing deliverables. Using the templates and techniques detailed throughout this paper should provide a solid foundation for conducting a post-acquisition audit in 30 days.

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

6. Establish Stakeholders

Establishing the key stakeholders of the post-acquisition audit is the first step to organizing and coordinating the audit. The stakeholders will be members of executive staff that oversee the high level finances, risk, technology, and operations of the business. It will be important to identify and communicate the audit plan with the stakeholders both at the corporate level and that of the newly acquired business. Involving them in the initial planning will help to ensure adequate resources are allocated to helping the lead auditor during fieldwork but also to ensure there is the appropriate level of awareness should issues arise from audit observations. Executive management is not fond of surprises and typically prefers to know about an audit and potential issues well in advance.

7. Defining the Audit Scope and Objectives

Given the time allotted to complete the audit, the next step will be to identify the objectives and determine an applicable scope. The objectives should align with the high level business objectives of the company by ensuring controls are in place to protect the most important assets. If information is the most important asset the auditor will want to understand the data lifecycle and ensure mechanisms are in place to protect the confidentiality, integrity, and availability of this information. If people are the most important asset the auditor will want to

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

ensure controls exist to protect the employee's physical security, interests (benefits, salary), relationship within their group, and their ability to grow within the company. Identifying what is "in scope" should be based on importance to the business, compliance to laws or regulations, whether the area has been reviewed in the past by an independent external auditor, and what its current risk is to the company based on the business impact analysis. It will also be important to decide what is not "in scope" so there is a clear understanding of what is to be reviewed and what is to be excluded. Typically shared services like HR or finance might be excluded if they intend to be provided by corporate. Areas of IT that might be excluded would be email or VoIP services if the acquired company were to be added to existing corporate systems. Areas that planned to be phased out, depending on the timeline, may also potentially be excluded.

Discussions with the stakeholders should help to identify which IT systems and processes the company relies on the most. The highest revenue generating or revenue supporting systems along with primary infrastructure should be the main areas of initial focus. Client facing or business-to-business applications will most likely fall into these categories and should be given the most attention. Another means of prioritizing audit scope can be to examine the data flow and determine what areas or processes are within the control of the acquired business versus what areas have be transferred to third-parties to support. Ensuring

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

contracts and service levels agreements are being actively managed may reduce the need to audit these other areas.

8. Roles and Responsibilities

After identifying the objectives and scope of the audit, it is important to identify key roles and responsibilities of the auditees. Knowing the organizational lines of responsibility and management's hierarchical structure will ensure the auditor is interfacing with the appropriate subject matter experts and those that have the authority to make high level risk mitigating decisions. The auditor should then attempt to identify system or data owners and the associated custodians of that asset. The system/data owner will be the executive business or IT manager who is familiar with the business processes associated with that asset and can intelligently make decisions that affect changes to it. The system/data custodian is the administrator that handles day-to-day operations and implementation of changes to the asset. Understanding these roles will help the auditor differentiate between what the business processes are intended to be versus what actual process are currently employed. Performing the audit will identify the gaps between expected business deliverables and actual business deliverables.

Incorporating executive management into the audit process is just as important as

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

conducting the fieldwork with the subject matter experts. Without executive management approval, the auditor may not be given the authority, access, or resources needed to conduct the fieldwork. Obtaining approval from the top down will ensure that adequate time of the subject matter experts is dedicated to working with the auditor. Despite this, the auditor must be sensitive to the needs of the employees as they have ongoing work that still needs to be completed along with helping the auditor.

While not all post acquisition audits will be exactly the same, there will be some common high level roles and responsibilities for all audits. These roles may include: lead auditor, audit team, key stakeholder, mid-level management, and subject matter experts. The lead auditor is the primary coordinator of the audit which may be support by additional resources as part of the audit team. The key stakeholder is typically a senior executive of that business unit or area being audited. Mid-level management is comprised of the directors and managers which will help coordinate discussions about business processes and procedures. The subject matter experts will the technical engineers and administrators responsible for implementation of systems and networks. The details of these roles, responsibilities, and potential job title are defined in the figure below:

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

Role	Responsibility	Job Title
Lead Auditor	Coordinates with executive management, mid-level management, subject matter experts and audit team. Works with management and audit team to establish audit objectives, scope, and timeline. Will coordinate periodic status reports to management based on fieldwork conducted. Ultimately responsible for completing audit report and delivery to management.	Auditor Expert
Audit Team	Works with the lead auditor to develop scope and objectives. Interfaces with subject matter experts and system administrators to gather artifacts during fieldwork. Documents observations, associated risks, and provides input to the audit report.	IT Auditor
Key Stakeholder	Meets with the lead auditor and executive staff to formally approve the audit scope, objectives, and timelines. Coordinates with mid-level management to ensure resources are dedicated to working with the auditors. Will take ownership of remediation requirements based on outcome of audit report.	Chief Information Officer
Mid-level Management	Considered to be system/data owners. Receives guidance from key stakeholder to support the auditors and provides them the internal resources needed to complete fieldwork. Will facilitate communications between auditors and other teams throughout the organization. May provide recommended corrective actions based on audit observations and risks identified during fieldwork.	Director of Business/IT Operations
Subject Matter Experts	Considered to be system/data custodians. Works with the audit team to demonstrate day-to-day activities and processes. Provides reports, logs, artifacts, or the access required for auditors to conduct fieldwork.	System Administrator or Network Engineer

Figure 1: Roles and Responsibilities

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

9. Developing the Audit Timeline

An audit should be treated as if it were a project. It will have a defined scope, objective, and timeline just like a project. Ensuring that the audit progresses according to schedule is ultimately the responsibility of the lead auditor and can be a key component to the success of the audit. Below is an example of an audit timeline and component stages.

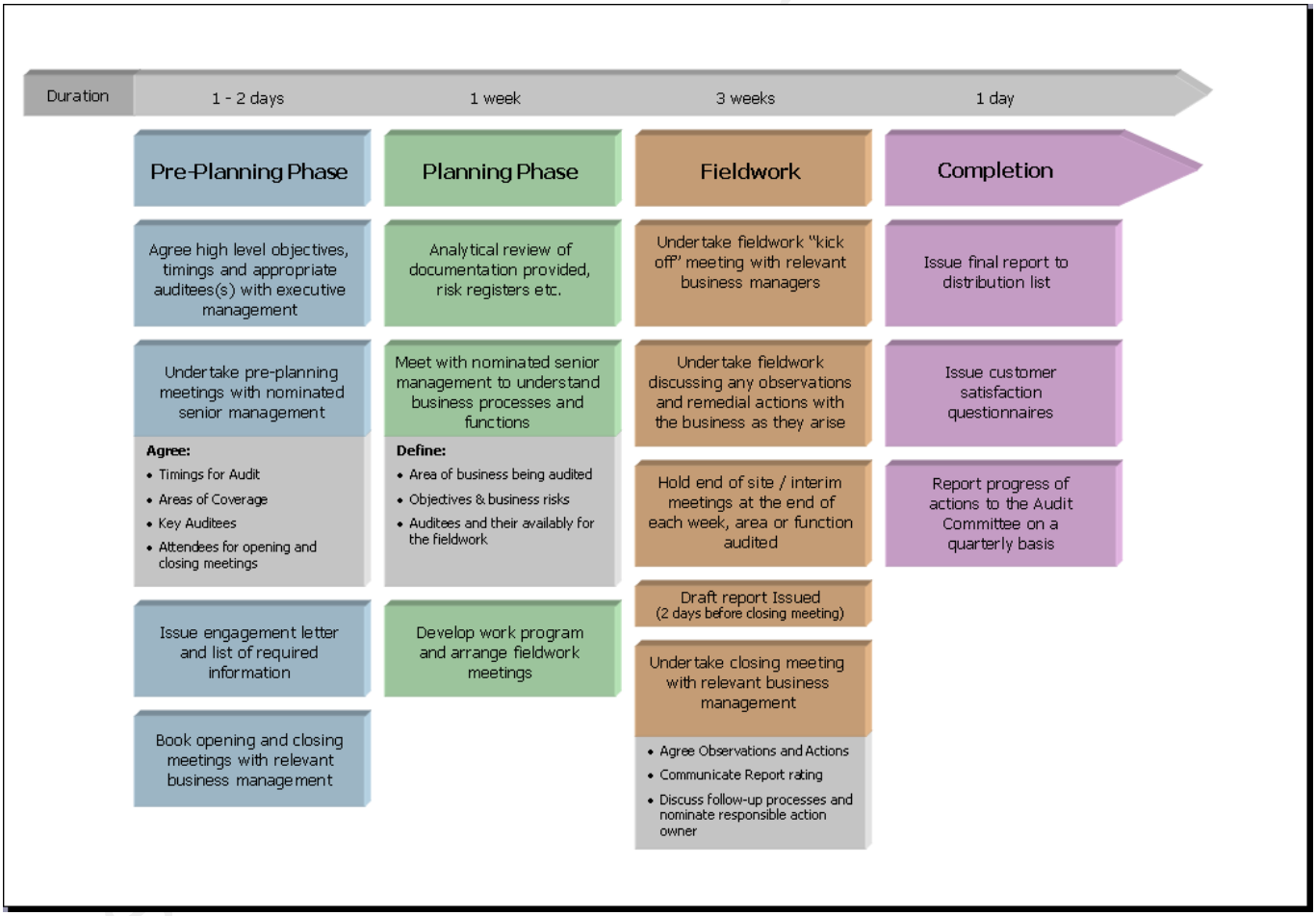

Figure 2: Audit Timeline

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

10. Documenting the Audit Work Program

Following the Project Management Institute's guidelines, each process will have an input, tools and techniques, and an output. Creating the audit work program will require input provided by enterprise environmental factors and organization process assets. Tools and techniques will be provided by the audit team members in the form of expert judgment. The output will be the documented audit work program.

Examples of enterprise environmental factors that can influence an audit would be:

- *"Organizational or company culture and structure*
- *Governmental or industry standards - elements such as regulatory standards and regulations (for instance, doctors must be licensed to practice medicine on people or pets), quality standards (International Standards Organization standards, for example), product standards, and workmanship standards.*
- *Infrastructure - the organization's facilities and capital equipment.*
- *Human resources - existing staff's skills and knowledge.*
- *Personnel administration - guidelines for hiring and firing, training, and employee performance reviews.*
- *Organization's work authorization system - how the work of the project is authorized.*
- *Marketplace conditions - supply-and-demand theory applies here along with economic and financial factors.*
- *Stakeholder risk tolerance - the level of risk stakeholders are willing to take on." (Heldman, 2007)*

The Guide to the Project Management Body of Knowledge expands on this by stating:

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

"*Virtually all projects are planned and implemented in a social, economic, and environmental context, and have intended and unintended positive and/or negative impacts. The project team should consider the project in its cultural, social, international, political, and physical environmental contexts.*

- ***Cultural and social environment**. The team needs to understand how the project affects people and how people affect the project. This may require an understanding of aspects of the economic, demographic, educational, ethical, ethnic, religious, and other characteristics of the people whom the project affects or who may have an interest in the project. The project manager should also examine the organizational culture and determine whether project management is recognized as a valid role with accountability and authority for managing the project.*
- ***International and political environment.** Some team members may need to be familiar with the applicable international, national, regional, and local laws and customs, as well as the political climate that could affect the project. Other international factors to consider are time-zone differences, national and regional holidays, travel requirements for fact-to-face meetings, and the logistics of teleconferencing.*
- ***Physical environment.** If the project will affect its physical surroundings, some team members should be knowledgeable about the local economy and physical geography that could affect the project or be affected by the project."(Project Management Institute, 2004)*

Organizational process assets are the organization's policies, procedures, standards, guidelines, plans, and approaches for conducting work. This would include Information Security Policies, Human Resource Policies, Physical Security Policies, and IT operating procedures. All these documents will be important to use as a baseline for auditing against. Organizational process assets would also include previous audits or work papers conducted by the Internal

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

Audit team that could be used as a template for future audits. These provide a starting point and can provide reference of previous audit risks, historical information, key contacts, and sample work programs.

Below is an example of a sample work program, developed by the author, which addresses twelve high level control objectives focused on Information Security risks. These areas include: security policy, security governance, asset classification, operating system controls, physical security, application security, change management, quality management, business continuity planning, network security, secure information exchange, and access controls. While this is not an exhaustive list of all areas of risk, it can be used as a foundation for an IT auditor.

Control Objective 1 – Determine if information security policies exist, are aligned with global policies, and are effectively communicated to staff.		**Risks – Lack of adequate information security policies / procedures poses a risk to the confidentiality, integrity, and availability of sensitive data. Without policy it is difficult to assign responsibility, ensure accountability, and to enforce compliance to a standard.**	
Ref	**High Level**	**Detailed Level**	**Record of Work Done**
1.1	Determine if information security policies and procedures exist	1. Request a copy of information security policies and procedures. 2. Compare local policies against global policies and ensure they are properly aligned with corporate strategy.	
1.2	Ensure information security policies are effectively communicated	1. Discuss with management their strategy for communicating security policy 2. Review new-hire security training programs and how they ensure compliance 3. Discuss how changes to the policy are reviewed and communicated to employees 4. Interview employees from different business divisions to assess their security awareness levels with regard to policy (i.e. – where is the policy,	

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

Control Objective 1 – Determine if information security policies exist, are aligned with global policies, and are effectively communicated to staff.		**Risks – Lack of adequate information security policies/procedures poses a risk to the confidentiality, integrity, and availability of sensitive data. Without policy it is difficult to assign responsibility, ensure accountability, and to enforce compliance to a standard.**	
Ref	**High Level**	**Detailed Level**	**Record of Work Done**
		what sections apply to their business if any, who do they escalate security issues to)	
1.3	Determine if information security policies are regularly reviewed to account for changes to the business or regulations	1. Discuss with management their strategy for reviewing the security policy 2. Request artifacts from any annual or semi-annual reviews of the policy 3. Discuss version control or how they maintain changes	

Control Objective 2 – Determine if information security is effectively managed and supported at the business unit level.		**Risks – Lack of information security management at the business level presents a risk of disclosure, alteration, or destruction of sensitive assets. Information Security Management should be aware of security risks and be able to effectively communicate these to the business.**	
Ref	**High Level**	**Detailed Level**	**Record of Work Done**
2.1	Determine if management has a commitment to information security	1. Request organizational charts or roles/responsibilities of employees to determine whether management demonstrates active support for security measures within the organization. 2. Identify individuals with explicit assignment and acknowledgement of information security responsibilities.	
2.2	Ensure information security risks are documented and addressed for all new lines of business or programs	1. Request copies of risk assessments conducted by information security teams that address confidentiality, integrity, and availability of systems.	
2.3	Determine if external security reviews are conducted	1. Discuss with management their strategy for external security reviews 2. Request artifacts from external security reviews or vulnerability assessments	

Control Objective 3 – Determine if information assets are appropriately classified and protected.		**Risks – Sensitive data may be inadequately protected from disclosure, alteration, or destruction.**	
Ref	**High Level**	**Detailed Level**	**Record of Work Done**
3.1	Determine if an inventory of assets has been effectively conducted	1. Discuss with management their means of inventorying and classifying assets. 2. Determine how often assets are collected, documented, reconciled and by who	

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

Control Objective 3 – Determine if information assets are appropriately classified and protected.		**Risks – Sensitive data may be inadequately protected from disclosure, alteration, or destruction.**	
Ref	**High Level**	**Detailed Level**	**Record of Work Done**
3.2	Identify what controls exist to protect sensitive assets	1. Document the physical controls that exist to protect sensitive assets 2. Document the technical controls that exist to protect sensitive assets 3. Are data owners and data custodians clearly defined have their roles been separated	

Control Objective 4 – Evaluate operating system controls to ensure acceptable use and adequate protection of company assets.		**Risks – Failure to have an adequate operating system controls can present a risk of data disclosure.**	
Ref	**High Level**	**Detailed Level**	**Record of Work Done**
4.1	Ensure acceptable use policies are defined and communicated to employees	1. Request copies of acceptable use policies and procedures for internal users 2. Discuss auditing controls for monitoring of acceptable use	
4.2	Ensure protection of the hard disk in the event of loss or compromise	1. Discuss with management the controls around protecting data on company laptops 2. Review any risk assessments performed on non-protected systems	

Control Objective 5 – Determine if physical security controls are properly documented and communicated to staff.		**Risks – Harm may come to employees or physical assets unprepared for a disaster.**	
Ref	**High Level**	**Detailed Level**	**Record of Work Done**
5.1	Determine if physical security controls are defined to address environmental risks.	1. Request physical security policies and procedures. 2. Request disaster recovery plans and business continuity plans to see if they are incorporated. 3. What controls exist to protect company hardware	
5.2	Determine if employees are aware of security controls.	1. Interview employees to see what their awareness levels are with regard to physical security policies.	
5.3	Determine if separation exists between public and private areas	1. What controls exist to separate delivery and loading areas from private access areas	
5.4	Determine if hardware maintenance policies exist	1. What controls have been implemented to ensure availability of systems	

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

Control Objective 6 – Determine if application security controls exist to prevent data leakage.		**Risks – Potential for disclosure, alteration, or destruction of intellectual property/information assets or reputational damage.**	
Ref	**High Level**	**Detailed Level**	**Record of Work Done**
6.1	Verify that application along with updates have gone through a risk review.	1. Examine risk review policies and procedures and obtain review evaluations. Determine if security risk, third-party risk, business risk, implementation risk and operating risk are taken into account. 2. Identify authorization or signoff authority of risk	
6.2	Verify that implementation complies with documented security controls.	1. Work with engineers and security architects to walk through infrastructure and ensure compliance with security standards. 2. Interview management to discuss and detail security risks and how they are mitigated. Especially with regard to confidentiality and data integrity.	
6. 3	Verify that a security assessment and post implementation review was completed.	1. Request security assessment documentation from security engineers which should include test cases and output from tests. 2. Identify if there are any outstanding risks based on assessments and discuss the follow-up actions that took place with management.	
6.4	Verify ongoing security monitoring and assessments are taking place.	1. Discuss with management ongoing security strategy. 2. Ensure appropriate security tools and processes are in place for to prevent injection of malicious code.	
6.5	Validate external security controls around application	1. Run through some cursory tests of the externally facing application. 2. Request results from application security scans, stress tests, etc. 3. Test for SQL Injection, Cross-site Scripting, Buffer Overflow, and Unicode exploits.	
6.6	Validate internal security controls around remote access	1. Work with developers to ensure proper input validation take place on all application interfaces 2. Examine error handling procedures to ensure proper encapsulation of error messages separating development from production error messages	
6.7	Ensure development teams have application security training	1. Ensure management has an application security strategy in place and that it aligns with corporate policy 2. Identify what external resources (books, websites, training, conferences, etc) are used for application security awareness 3. Request a list of employees that have completed application security training	

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

Control Objective 7 - Determine if application enhancements have gone through change management.		**Risks - Failure to follow change management procedures may result in unauthorized changes to production environments. This could adversely affect the functionality or security of the application.**	
Ref	**High Level**	**Detailed Level**	**Record of Work Done**
7.1	Determine if the application has gone through a defined Software Development Life Cycle (SDLC).	1. Obtain SDLC procedures and expected deliverables 2. Obtain business case documentation with cost-benefit analysis 3. Obtain Business Requirements Document (BRD), System Requirements Document (SRD) 4. Interview management responsible for designing and implementing to ensure proper approval and signoff provided	
7.2	Verify existence of Change Management (CM) program and ensure adherence to CM procedures.	1. Obtain Change Management Program documentation 2. Obtain evidence that demonstrates request, approval, development, QA, staging, and production release changes. 3. Interview management responsible for designing and implementing Remote Access to ensure proper approval and signoff provided 4. Ensure proper segregation of duties exists between project authorization and design/development	

Control Objective 8 – Determine if SLAs, metrics, and Quality of Service (QoS) are documented, measured, and monitored along with escalation procedures.		**Risks - Availability issues could arise if capacity is exceeded prior to detection. Business sponsor may not be receiving adequate uptime or support due to latency issues going undetected**	
Ref	**High Level**	**Detailed Level**	**Record of Work Done**
8.1	Verify that service level agreements have been defined, are actively monitored and reported to management.	1. Request copies of SLAs from management and monitoring strategy. 2. Request reports from activity monitoring and capacity monitoring. 3. Identify if service level comply with initial agreements. 4. Interview management to determine how reports and logs are communicated back to business.	
8.2	Ensure service level escalation procedure exists.	1. Discuss with management escalation procedure and request documented processes. 2. Obtain evidence of previous instances of escalation through a ticket tracking system or status reports.	

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

Control Objective 8 – Determine if SLAs, metrics, and Quality of Service (QoS) are documented, measured, and monitored along with escalation procedures.		**Risks - Availability issues could arise if capacity is exceeded prior to detection. Business sponsor may not be receiving adequate uptime or support due to latency issues going undetected**	
Ref	**High Level**	**Detailed Level**	**Record of Work Done**
8.3	Determine if quality of service reports are conducted.	1. Request copies of Quality of Service (QoS) surveys and procedures for administering and reporting. 2. Discuss with management the process of evaluating QoS reports and action items from reports.	

Control Objective 9 – Confirm that a business continuity plan exists to support business critical functions.		**Risks – Failure to provide adequate backup systems in the event of a disaster poses a risk to the business operations, communication and functionality.**	
Ref	**High Level**	**Detailed Level**	**Record of Work Done**
9.1	Verify that a high-level business continuity plan has been documented to address critical functionality.	1. Request copy of high-level Business Continuity Plans (BCP). 2. Request copy of Business Impact Analysis. 3. Request copy of Disaster Recovery Plan.	
9.2	Ensure the BCP addresses all major business processes and has been communicated to appropriate management and staff.	1. Conduct interviews with senior management to ensure all critical business functions are covered in the BCP. 2. Conduct interviews with middle management to ensure awareness and understanding of plan exists. 3. Review strategy to ensure adequate remote access capabilities exist to support ongoing business	
9.3	Ensure BCP addresses all critical employee routines and functions	1. Conduct interviews with senior management to ensure all critical employee functions are covered in the BCP. 2. Conduct interviews with middle management to ensure awareness and understanding of plan exists	
9.4	Ensure a backup strategy exists	1. Request evidence of a backup strategy that includes both critical systems, employee desktops, and employee functions 2. Request test cases, test results, or scheduled tests	
9.5	Ensure BCP is routinely reviewed for accuracy and has been tested	1. Request evidence of BCP review or meeting minutes from evaluation. 2. Request test cases, test results, or scheduled tests.	

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

Control Objective 10 – Evaluate the network security controls to ensure adequate management of network devices and protection of data transmission.		**Risks – Failure to properly secure network devices or data being transmitted over the network poses a threat of disclosure, alteration, or destruction of information assets.**	
Ref	**High Level**	**Detailed Level**	**Record of Work Done**
10.1	Verify that new network implementations go through a risk review	1. Examine risk review policies and procedures and obtain review evaluations. Determine if security risk, third-party risk, business risk, implementation risk and operating risk are taken into account. 2. Identify authorization or signoff authority of risk	
10.2	Verify that implementation complies with documented security controls	1. Work with engineers and security architects to walk through network infrastructure and ensure compliance with security standards. 2. Interview management to discuss and detail security risks and how they are mitigated. Especially with regard to confidentiality and data integrity.	
10.3	Verify that a security assessment and post implementation review was completed	1. Request security assessment documentation from security engineers which should include test cases and output from tests. 2. Identify if there are any outstanding risks based on assessments and discuss the follow-up actions that took place with management.	
10.4	Verify ongoing security monitoring and assessments are taking place	1. Discuss with management ongoing network security strategy. 2. Ensure appropriate security tools and processes are in place for virus checking and intrusion detection	
10.5	Validate external security controls	1. Work with Security Operations Center to identify and isolate IP segments for external mapping 2. Run tests with a port mapping tool such as nmap to validate open ports on external firewalls. Discuss exceptions or findings with network security groups 3. Work with telecom groups to identify phone blocks owned by company for external mapping 4. Run tests with war dialing software such as Ton-Loc or THC-Scan to identify existing modems. Discuss exceptions or findings with network security groups.	
10.6	Validate internal security controls	1. Discuss with management any outbound filters that take place at the network level 2. Document how internal events are monitored and logged 3. Document how anomalous activities are logged and escalated 4. Request IDS reports that include signatures for	

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

Control Objective 10 – Evaluate the network security controls to ensure adequate management of network devices and protection of data transmission.		**Risks – Failure to properly secure network devices or data being transmitted over the network poses a threat of disclosure, alteration, or destruction of information assets.**	
Ref	**High Level**	**Detailed Level**	**Record of Work Done**
		anomalous behavior 5. Request border router and firewall configuration files to be run against a parser like Nipper or RAT (Router Auditing Tool). Review results with management.	

Control Objective 11 – Evaluate the exchange of sensitive information to ensure it is protected against disclosure.		**Risks – Failure to properly secure data in transit poses a risk of disclosure in the event the data is intercepted.**	
Ref	**High Level**	**Detailed Level**	**Record of Work Done**
11.1	Ensure sensitive data transmitted between Experian and an external party is properly secured.	1. Identify business processes (physical and electronic) that deal with transmitting and receiving sensitive data between clients and business partners 2. Discuss any security controls that may be used to encrypt or otherwise protect data from the risk of disclosure by an unauthorized party	
11.2	Identify any exchange agreements between Experian and external parties	1. Request copies of exchange agreements or policies specifying sensitive data handling 2. Work with management to ensure current practices meet requirements	

Control Objective 12 – Evaluate access controls around internal systems to ensure protection of company assets.		**Risks – Failure to have an effective access control program poses a risk of unauthorized access to sensitive company assets.**	
Ref	**High Level**	**Detailed Level**	**Record of Work Done**
12.1	Ensure access control policies and procedures have been defined for internally systems.	1. Request copies of access control policies and procedures for internal systems 2. Ensure a separation of duties exists between system developers, system administrators, system users, and reporting analysts	
12.2	Ensure a user lifecycle process had been developed	1. Request copies of user onboarding, transfer, and removal process 2. Request audit logs to verify transfers and terminations match with system changes	
12.3	Ensure controls exist to prevent unauthorized access to internal systems	1. Discuss with management the authentication mechanism used to control access and ensure it aligns with security policies 2. Discuss session timeout controls and password management	

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

Control Objective 12 – Evaluate access controls around internal systems to ensure protection of company assets.		**Risks – Failure to have an effective access control program poses a risk of unauthorized access to sensitive company assets.**	
Ref	**High Level**	**Detailed Level**	**Record of Work Done**
12.4	Ensure controls exist around remote access to internal systems	1. Discuss with management all remote access capabilities to internal systems or networks 2. Ensure risk assessments have been conducted on these remote access technologies and that they align with security policy 3. Discuss authentication mechanisms used to control access 4. Identify with management the controls to store user provisioning of remote access software / hardware	

Figure 3: Sample Work Program

11. Developing the Document Request List

During the planning stage the audit team will want to develop a document request list to be the initial step of information gathering from the auditees. This will provide some guidance to the auditees as to the areas that will be examined and should include requests for policies, procedures, demonstration of work performed, and controls for protecting company assets. This document is meant to be used as a checklist that is sent to executive management immediately following the formal engagement letter. The engagement letter will be the official notification that the audit is to proceed and to provide some high level background about the audit process, timeline, and deliverables. Most internal audit teams have a template engagement letter that is used for all audits, and only the attributes are changed. An example of a document request list specific to a post-acquisition audit is provided below.

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

Memorandum

To: [*Name of Primary Stakeholder*]
From: [*Name of Lead Auditor*]
Date:
Re: [*Audit Title*]

Reference: Document Request List

General
Organizational Chart
Annual Plan/Forecast
List of facilities
Business Continuity Plan
List of pending legal matters
Employee List (name and address)

Policies and Procedures
Information Security Policies
Human Resources/Hiring Policies
Physical Safety Procedures
Acceptable Use Policies

Human Resources
Employee turnover statistics

Business
List of business partners/customers/3rd party vendors
Business/Data flow diagrams
Outline of all services and product offerings

Information Technology/Information Security
Physical Security Controls (locks, badges, cameras, guards, segregation by job function, etc.)
Data Center Physical and Environmental Controls Overview
Asset Management (hardware, software, owner, custodian)
Network diagrams
List of Supported Applications (function, summary, owner, custodian, users, platform, OS, system dependencies, business dependencies, accessibility [internal/external])
List of End-user computing files (spreadsheets, ad-hoc databases, etc)
Virus and Malware Protection

IT Policies/Procedures
Change Management
Information Security Awareness Training
Password Policy (workstations, servers, network devices, applications, database)
Incident Handling and Escalation Procedures

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

Patch Management (servers, workstations, network devices)
System Development Life Cycle (SDLC) Procedures
Data Retention / Destruction
Data Classification / Protection (data at rest/data in motion)
Event Monitoring and Log Collection (network, host)
Operations Monitoring
System and Data Backup
System Configuration, Benchmarking, and Security Hardening
Wireless Usage

IT Reports
Network Event Monitoring Logs
Application Monitoring Logs (user access accountability)
System Maintenance/Monitoring Reports
System and Physical Security Incident Reports (previous 6 months)
Security Reports for all key systems/applications (user name and access level)
Workstation and Server Patching Reports
Business Continuity Test Results
Quality Assurance and Operational Readiness Tests of Applications
Application Risk Assessments
Network and System Vulnerability Assessments
System Benchmarking Certification Results

Please forward all questions and concerns to the lead auditor listed below:

[Contact Information of Lead Auditor]

Figure 4: Sample Document Request List

12. High-level Steps to Executing the Audit

The execution of a post-acquisition audit can be similar to the execution of a post-implementation audit. The lead auditor will want to examine stated objectives, business case,

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

cost-benefit analysis, business requirements documents, detailed design documents, testing procedures, and implementation details. When reviewing any IT solutions within the newly acquired company, the auditor will need to ensure that controls are in place to protect the confidentiality, integrity, and availability of the data and system itself. One means of providing this assurance is to audit the solution against professional standards like the COBIT control objectives. The effect of noncompliance to these standards should be analyzed and included in the audit report. Below are some guidelines for conducting a post acquisition audit provided by the Information Systems Audit and Control Association (ISACA):

1. *"A post-implementation review should be scheduled at a reasonable time after the IT solution has been implemented. Typical periods can range from four weeks to six months, depending upon the type of solution and its environment.*
2. *A post-implementation review is intended to be an assessment and review of the final working IT solution. Ideally, there should have been at least one full implementation and reporting cycle completed to perform a proper review. The review should not be performed while still dealing with initial issues and teething troubles, or while still training, and educating users. However, where possible, the review should be performed while the opportunity remains to incorporate final improvements to derive optimum benefit from the IT solution.*
3. *Review procedures should include the study of available documentation (such as business case, business requirements including business controls, feasibility study, system, operational and user documentation, progress reports, minutes of meetings, cost/benefit reports, testing and training plans), discussions with stakeholders, hands-on experimentation and familiarization with the IT solution, observation and inquiry of business and project personnel, and examination of operational and control documentation.*
4. *Appropriate resources to carry out the post-implementation review should be identified and allocated, and the performance of the review should be planned in conjunction with relevant auditee personnel.*
5. *Agreement should be reached regarding the format, content, audience and timing, where possible, of reporting the results of the post-implementation review.*

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

6. *The stated objectives of the IT solution, costs and benefits should be studied in detail. The extent of achievement of the objectives and actual costs and benefits should be evaluated together with the processes and systems used to capture, monitor and report performance, costs and benefits. As part of this exercise, the productivity/performance improvements delivered by the IT solution should also be studied. Suitable measurement criteria should be used in this context. The cost and/or time overrun, if any, should be analyzed by reference to their causes and their effects. Controllable and uncontrollable causes should be identified separately.*

7. *The process followed for defining and implementing the IT solution should be evaluated with reference to its appropriateness, as well as its effectiveness.*

8. *The adequacy and effectiveness of education and training provided to users and staff supporting the IT solution should be reviewed.*

9. *The reports of any prior reviews performed either internally or by external reviewers on a pre-implementation basis or concurrently with the implementation process should be studied, and the status of recommendations and actions taken verified.*

10. *Since the post-implementation review is examining an IT solution, in general, the IT solution should satisfy appropriate COBIT control objectives. The extent of compliance with relevant control objectives and the effect of noncompliance should be analyzed and reported. Further, critical success factors, key goal indicators, key performance indicators and maturity model benchmarks from COBIT Management Guidelines should be adapted as appropriate for the IT solution and implementation process being reviewed.*

11. *Appropriate management trails should be maintained for the data gathered, analysis made, inferences arrived at as well as corrective actions recommended.*

12. *The extent of compliance with statutory and regulatory requirements and organizational policies and standards of the IT solution and implementation process should be reviewed.*

13. *Where appropriate, automated testing tools and CAATs may be used to test relevant aspects of the IT solution.*

14. *The review should highlight risks and issues for necessary corrective action, together with opportunities for improvement in controls or increased effectiveness of the implementation process.*

15. *Reported findings, conclusions and recommendations should be based on an objective analysis and interpretation of the information and evidence obtained during the post-implementation review.*" (ISACA, 2005)

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

13. Conducting the Audit

Performing the actual fieldwork might seem like a daunting task but can be quite manageable if broken up into smaller pieces and scheduled in advance. The lead auditor should spend the planning week reading through policies and procedures and to schedule meetings throughout the following two weeks of fieldwork with each subject matter expert. He or she should also coordinate with mid-level management to have summary meetings at least twice a week; preferably once in the middle and once at the end of each week. It is also important to provide a summary of these meetings via email to executive management to keep them abreast of any potential major issues should they arise. Communication is the most important component to any audit and helps eliminate confusion and ensure there are no surprises. This also helps to manage expectations and provide executive management with status updates of the audit.

14. Documenting the Observations

During the audit fieldwork, observations may be identified that demonstrate variances between documented policies or procedures and the actual business processes performed. These observations should be documented in written form and discussed with the auditees. It is possible that the policies or procedures were written before actual work began or that they are

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

no longer current. This should be discussed with management to determine if the process needs to be modified to conform to the documented procedures or perhaps the documentation needs to be updated to reflect the actual work being performed. It will be important to involve management in these discussions because they will ultimately own the responsibility for managing these changes and ensuring ongoing conformance to written policies and procedures.

15. Developing the Audit Report

The audit report is typically a high level document to be distributed to executive management that summarizes the scope, objectives, findings and associated risks, as well as remediation actions, owners and timelines. The report will not include all the details of the fieldwork but rather a short synapses of what the key issues are and what mitigating actions have been agreed to and by whom. The report should provide an executive summary toward the beginning, followed by a one page description of each observation, risk, severity rating, mitigation statement, action owner, and time needed to correct the issue. The report should identify the areas reviewed during the audit as well as any areas excluded and any reasoning behind such decisions. The report should also include an appendix which describes how the risks were categorized and how the severity ratings were concluded based on probability and

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

impact estimates.

After the fieldwork has been concluded, the audit team should work toward finalizing the audit findings, risks, remediation plans, and time required to implement corrections into the final report. This should be a collaborative effort with the auditees and mid-level management to agree to the accuracy of the observations and the risks identified. Although risk severity can often be a subjective analysis, the observations or issues identified and the potential risks from these issues should be based on facts gathered during fieldwork. This draft report should be distributed to executive management two to three days prior to the official closeout meeting to provide adequate time for review.

16. Closing out the Audit

A closeout meeting should be scheduled well in advance to ensure executive management is available to attend as well as mid-level management. Typically this meeting request should be sent out during the planning week to mark the closing of the audit, one week after fieldwork has concluded. The closeout meeting should be more of a formality providing a quick summary of observations and agreed actions and not necessarily an open forum for discussion. Executive management's time is precious and therefore it is best practice to ensure that any open items of discussion surrounding the report should be handled prior to the closeout

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

meeting. Having bi-weekly meetings with mid-level management and subject matter experts during fieldwork helps to facilitate awareness and draw consensus on open issues. Copying executive management on an email that summarizes these bi-weekly meetings will inform them that progress is being made and corrective actions have been agreed to.

The closeout meeting should be at most one hour long, and should include a brief summary of the scope, objectives, findings and agreed actions. The auditees should be thanked for their time and support provided to the audit team and each auditor should briefly summarize each high level observation along with management's agreed corrective action. There will be a small window for discussion with executive management over the agreed actions and general risk based on the observation noted in the report, but this should be kept to a minimum. Should executive management want to continue discussions these should be channeled for another meeting considering all items have been thoroughly discussed previously with mid-level management and subject matter experts. Ensuring any follow-up discussions are more of an exception rather than the rule will be the responsibility of the lead auditor and his or her ability to communicate the audit findings well in advance.

17. Conclusion

Conducting a post-acquisition audit in 30 days can easily be accomplished given the

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

proper planning, support from executive management, and having the necessary communication skills. Breaking the larger tasks into smaller units and scheduling meetings well in advance will also provide a great deal of assistance to the success and efficiency of the audit. Conforming to industry standards like COBIT, and utilizing prior audit templates will also simplify the creation of work papers and ensure a more thorough review is conducted. Keeping upper management involved in the audit findings and soliciting their advice for corrective actions will ensure adequate awareness of risks to the business and that remediation action address a holistic approach.

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

18. References

Heldman, Kim (2007). *Project Management Professional Study Guide*. Indianapolis, Indiana: Wiley Publishing.

Project Management Institute (2004). *A Guide to the Project Management Body of Knowledge.* Newton Square, Pennsylvania: Project Management Institute, Inc.

Information Systems Audit and Control Association (2005). *Control Objectives for Information and related Technology (COBIT).* Rolling Meadows, Illinois: ISACA

© SANS Institute 2009, Author retains full rights.

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

Last Updated: September 2nd, 2015

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Crystal City 2015	Crystal City, VAUS	Sep 08, 2015 - Sep 13, 2015	Live Event
SANS Network Security 2015	Las Vegas, NVUS	Sep 12, 2015 - Sep 21, 2015	Live Event
SANS Seoul 2015	Seoul, KR	Sep 14, 2015 - Sep 19, 2015	Live Event
Data Breach Investigation Summit & Training	Dallas, TXUS	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Baltimore 2015	Baltimore, MDUS	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Perth 2015	Perth, AU	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Tallinn 2015	Tallinn, EE	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS ICS Amsterdam 2015	Amsterdam, NL	Sep 22, 2015 - Sep 28, 2015	Live Event
SANS Bangalore 2015	Bangalore, IN	Sep 28, 2015 - Oct 17, 2015	Live Event
SANS DFIR Prague 2015	Prague, CZ	Oct 05, 2015 - Oct 17, 2015	Live Event
SANS Seattle 2015	Seattle, WAUS	Oct 05, 2015 - Oct 10, 2015	Live Event
SANS Tysons Corner 2015	Tysons Corner, VAUS	Oct 12, 2015 - Oct 17, 2015	Live Event
SOS: SANS October Singapore 2015	Singapore, SG	Oct 12, 2015 - Oct 24, 2015	Live Event
SANS Gulf Region 2015	Dubai, AE	Oct 17, 2015 - Oct 29, 2015	Live Event
SANS Cyber Defense San Diego 2015	San Diego, CAUS	Oct 19, 2015 - Oct 24, 2015	Live Event
SANS Tokyo Autumn 2015	Tokyo, JP	Oct 19, 2015 - Oct 31, 2015	Live Event
SANS South Florida 2015	Fort Lauderdale, FLUS	Nov 09, 2015 - Nov 14, 2015	Live Event
SANS Sydney 2015	Sydney, AU	Nov 09, 2015 - Nov 21, 2015	Live Event
SANS London 2015	London, GB	Nov 14, 2015 - Nov 23, 2015	Live Event
Pen Test Hackfest Summit & Training	Alexandria, VAUS	Nov 16, 2015 - Nov 23, 2015	Live Event
SANS Hyderabad 2015	Hyderabad, IN	Nov 24, 2015 - Dec 04, 2015	Live Event
SANS Cape Town 2015	Cape Town, ZA	Nov 30, 2015 - Dec 05, 2015	Live Event
SANS San Francisco 2015	San Francisco, CAUS	Nov 30, 2015 - Dec 05, 2015	Live Event
SANS Milan 2015	OnlineIT	Sep 07, 2015 - Sep 12, 2015	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced