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.

The Application Audit Process - A Guide for Information Security Professionals

This paper is meant to be a guide for IT professionals, whose applications are audited, either by an internal or external IS audit. It provides a basic understanding of the IS Audit process. It is also meant as an aid for auditors to facilitate the audit process by communicating audit terms and objectives. The document takes the reader through the different control points of an application audit: Administration, Input, Processing, Outputs, Logical Security, Disaster Recover Plan, Change Management, User Support, Genera...

Copyright SANS Institute

Author Retains Full Rights

AD

Investigate Insider Threats
Protect your company against corporate IP Theft
Learn More
SpectorSoft

The Application Audit Process - A Guide for Information Security Professionals

GIAC Security Essentials
Certification (GSEC)
Practical Assignment
Version 1.4c

Option 1 - Research on Topics
in Information Security

Submitted by: Robert Hein
Submitted on: 10/31/2004

© SANS Institute 2005, Author retains full rights.

Table of Contents

Abstract 1
Introduction 2
Application Audit 2
  Administration 3
  Inputs, Processing, Outputs 4
  Logical Security 5
  Disaster Recovery Plan 6
  User Support 7
  Change Management 8
  General Controls 9
  Third Party Services 10
Conclusion 10
References 11

© SANS Institute 2005, Author retains full rights.

Abstract

This paper is meant to be a guide for IT professionals, whose applications are audited, either by an internal or external IS audit. It provides a basic understanding of the IS Audit process. It is also meant as an aid for auditors to facilitate the audit process by communicating audit terms and objectives. The document takes the reader through the different control points of an application audit: Administration, Input, Processing, Outputs, Logical Security, Disaster Recover Plan, Change Management, User Support, General, and Third Party Suppliers.

The paper specifies the documentation that the IS auditor will be looking for at each process to ensure controls are in place. It should be readily apparent to the reader that the IS Auditor and Information Security Professional are really both pursuing the same goals but through different terminology. IS audit wants "control" whereas Information Security pursues "security". They are, in essence and practice, the same thing.

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2005 Author retains full rights.

Introduction

Legislative, economic, and organizational pressures are forcing their way into the historically unencumbered Information Technology (IT) department. Information security professionals are pushed to the breaking point with new and more complex challenges. Organizations are looking towards their internal and/or external audit departments to reign in the challenges. In the current business climate, it is essential that IT professionals understand the process of Information Systems (IS) Audit and the concepts of risk and control.

We should first define the two important concepts of risk (business risk) and control (internal control) as they are used in this paper.

Business Risk – "any event or action that stops an organization from achieving its goals or business objectives." (Gallegos et al. 386).

Internal Control – The University of Delaware's Internal Audit Department website defines internal control as "a process, effected by an entity's board of trustees, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives"

IS Auditing involves providing independent evaluations of an organization's policies, procedures, standards, measures, and practices for safeguarding electronic information from loss, damage, unintended disclosure, or denial of availability. IS audit provides management with an assessment of whether there exists sufficient controls to mitigate an organization's risk. The application audit is an assessment whose scope focuses on a narrow but business critical process or application.

Application Audit

An application audit is a specific audit of one application. For example, an audit of an excel spreadsheet with embedded macros used to analyze data and generate reports could be considered an Application Audit. Application Audits can also pertain to a business process that heavily relies on various information technology systems. An example would be the payroll process of a company, which may span across several different servers, databases, operating systems, applications, etc. Application audits can also be of a more technical nature like of a PBX or a single data warehouse.

These audits can be done as the system is developed, at post-implementation, or on a regularly scheduled basis (annually, every 5 years, etc.). Whichever stage of audit review is being carried out, the IS Auditor is looking for assurance that the application provides an adequate degree of control over the data being processed. The level of control expected for a particular application is dependent on the degree of risk involved in the incorrect or unauthorized processing of that data (Oliphant).

© SANS Institute 2005 Author retains full rights.

An Application Audit, should, at a minimum determine the existence of controls in the following areas:

1. Administration
2. Inputs, Processing, Outputs
3. Logical Security
4. Disaster Recovery Plan
5. Change Management
6. User Support
7. Third Party Services

Administration

The administration of the application is probably the most important area of the application audit review. This is because this area focuses on the overall ownership and accountability of the business to the application. Without adequate controls around the administration of an application, all the other areas are more than likely inadequate and cannot assure that controls are in place and risks are mitigated.

An IT manager, or business owner, should ensure that roles and responsibilities are clearly defined, and documented, for each individual on their team. This documentation should be sufficient evidence to demonstrate that an effective organizational structure is in place. This means, at a minimum, organization charts are available and current. Several software companies that offer enterprise wide, organizational chart software. These software tools can greatly facilitate the process.

Organizational charts and roles and responsibilities documentation are not only helpful to information system auditors, but the company as a whole. They offer managers a better understanding of their business, as well as being an excellent training tool for new associates.

An auditor will most likely request job descriptions for application developers, the business owners, and any production support groups. It is essential to determine if application business ownership and custodianship responsibilities are clearly established. Controls should be in place to ensure that segregation of duties exists between business owners, developers, and operational support. Specifically, responsibilities for application development, change approval, and application access authorization need to be segregated. Neil Jackson, business manager, internal audits, E*TRADE Financial, in an interview with Ed Hurley, Assistant News Assistant for SearchSecurity, states that “The most difficult issue is the evaluation of how system access and system and application privileges are properly segregated to impose an effective system of control. For example, there should be a way to restrict a system's administrator from performing specific application transactions.” (Hurley).

© SANS Institute 2005 Author retains full rights.

Any legal or regulatory compliance issues, around the application, should be stated and addressed. The change management methodology employed by the company should identify these regulatory and compliance issues. It is important to ensure that a representative of the company's legal and/or compliance department is consulted during the development and implementation of system changes. Any changes to the application could move a system out of compliance with laws that it had previously addressed.

Performance metrics should be defined and key processes around these metrics should be monitored. Service Level Agreements (SLAs) should be required between each business customer that is dependent on the application for any aspect of their business function. The SLAs should be documented, up to date, and be appropriately monitored. The auditor will review the SLA to ensure that it meets set standards such as defining what service levels will be used and exactly how they will be measured as well as aligning the supplier's incentives with the customer's objectives through service level credits and termination rights (Peterson).

Inputs, Processing, Outputs

In this area, the auditor will be looking for evidence of data preparation procedures, reconciliation processes, handling requirements, etc. Auditors will need to obtain evidence that controls over manual processes such as user data preparation procedures are in place. It is essential that manual inputs are complete and appropriately authorized prior to being processed by the application.

Be prepared for an auditor to ask to review business processes around the creation of transactions that will be input into the system. A typical audit practice is to pull a sample of these transactions and ensure they are properly authorized and the authorization is documented. The auditor could also request a sample of source documents and ensure that they are appropriately secured and retained. Using Computer Assisted Auditing Techniques (CAATs), an auditor can recalculate and validate the accuracy and completeness of key system calculations which occur during processing. IT professionals being audited should be prepared to have their applications and systems tested in such a way that all processing is reviewed. There should be ample evidence that input controls, error processing, and output validation are designed into the application. The majority of licensed CAATs software can perform a very thorough audit of these controls.

In terms of outputs, the auditor will be seeking documentation that defines the handling requirements of reports or other hard-copied documents produced by the application. This documentation should include the retention requirements (how long this documentation needs to be secured and maintained) and the distribution procedures (who has permission to see the output, and how they are

© SANS Institute 2005 Author retains full rights.

to ensure its security). Finally it should also include information disposal / destruction procedures. As Geoffrey James states in his article, “Get auditors to help you understand when to cache it and when to trash it”.

The auditor may request a listing of all system generated reports to determine the owner and business use. From these reports they will validate the need and effectiveness of current reports. The auditor will determine whether these user reports are marked with the appropriate security classification according to the organization’s information protection standard, if applicable.

Balancing and reconciliation (control totals) should be in place to determine that the desired output is obtained for each application process. Audit trails should be utilized and processes in place to review them so that errors can be found and corrected, improper processing can be pinpointed, and any malicious actions during processing can be caught. The auditor will determine if control totals from key reports are traceable to upstream or downstream systems in order to follow the application process in a logical manner. These reports must be available to prove adequate control over the inputs and outputs.

Logical Security

Application audits usually involve in-depth evaluation of logical security for the application. This review is done on top of the logical security review performed as part of the infrastructure review which looks at the enterprise wide systems (UNIX, Mainframe, LANs, Databases, etc.).

The auditors will need to have your application user ID administration process documented and evidence that it is being followed. There needs to be specific processes around new user ID administration. The documentation around user ID administration should also detail the ongoing maintenance processes such as access updates and deletions, who is responsible to administer the access, and who needs to approve it.

A typical test would involve the auditor receiving from the organization’s Human Resource department a list of new employees and transfers to the department within a set time period. The auditor would then select a sample of users added to the system over the same time period and verify that creation of the account was appropriately authorized by the appropriate personnel (supervisor, manager, application owner, etc.) They will also verify that the access provided to the application ID is limited to the access requested on the authorization form.

It is considered a best practice to use access profiles rather than ad hoc access to applications and systems. The auditor will thus ensure that profiles are being used and verify that each user ID in the application is linked to a specific application profile. If there is an ID that is linked to more than one profile, the auditor will confirm that there is no improper segregation of duties among the granted profiles.

© SANS Institute 2005 Author retains full rights.

A likely test would be for the auditor to select a sample of current users of the application and printout their access rights. They would then review these printouts with each user's business management to ensure the access is appropriate. This is an excellent way to ensure that the ongoing maintenance processes are effective. This being said, the IT and business owners should initiate their own security review of the application on a periodic basis to ensure that it is effective. If IT can provide audit documentation of these reviews, this gives the auditor confidence that there are sufficient controls around the entire process.

The auditor will almost surely request the application's security configuration. In this context, the configuration should, at a minimum, illustrate the application's:

- Number of allowable unsuccessful log-on attempts
- Minimum Password Length
- Password Expiration
- Password Re-use ability

The auditor will then assess, based on the organization's security policy, or on external best practices, whether this configuration is adequate to protect the application from malicious or fraudulent intent.

The organization should have security surveillance procedures documented at a company wide level. The auditor would need to provided access tracking / logging reports to ensure that audit trails are generated, and properly reviewed, according to the security surveillance procedures. Any violation and security activity reporting should be in existence and provided to the auditor.

Disaster Recovery Plan

In his article "Holistic Approach is Key to Network and IT Recovery and Security Success", Damian Walch states that "Post September 11th, companies have seen the terms "security," "cyber-security" and "disaster recovery" uttered in the same breath. They've begun to appreciate the notion that security and business continuity could be aligned in several ways." Auditors are particularly aware of the need for an adequate and performable disaster recovery plan (DRP) that will provide confidence that the application can be recovered in a reasonable amount of time after a disaster.

To determine whether the DRP can provide this confidence, the auditor will request the backup guidelines and processes documentation. The auditor will ask for offsite storage guidelines and processes and review the current procedures to determine their adequacy. Offsite storage contingency should be written out and SLAs with the offsite storage vendors, if applicable, should be provided to the auditor. Through review of this documentation and discussions with management, they can form an opinion on whether the necessary control points are in place to mitigate the effects of a potential disaster.

© SANS Institute 2005 Author retains full rights.

In terms of the actual DRP, there needs to be evidence that a plan requirements identification process exists. This process should be documented, involve the appropriate business and IT representatives, and be a regularly scheduled event. The identification process will also be reviewed by the auditor to ensure that all necessary assumptions have been made (site available with running electricity, servers up, etc.) and that no requirement has been overlooked.

The most important evidence of control, the DRP itself, should specify the different stages (initial, interim, and return to normal) of the disaster and their accompanying steps. These stages should clearly document the roles and responsibilities of all involved. The specific locations, personnel, phone numbers, etc. will more than likely be checked by the auditor for their accuracy and timeliness.

A plan maintenance process should be in place which provides for changes to the plan when anything that affects the application has been changed. The DRP should be up to date, accurate, and doable. This process should be either periodic (biannually) or based on certain events (new releases). Any meeting minutes or documentation that comes from this process should be provided to the auditor.

It is essential that DRP training processes are in place. The auditor is at liberty to ask any staff involved with the application, what their specific roles and responsibilities during a disaster are, and then match their responses to what the DRP itself states. The training should be documented and readily available in each associate's personnel file. Training documentation and events should also be recorded and properly stored so that they are readily accessible by the auditor.

The surest evaluation of the adequacy of the DRP is documentation of the recovery testing that is performed. The testing process must be defined and implemented for the plan. Subsequently, the DRP must be updated to reflect any deficiency determined in the test results. The auditor will form an opinion on whether the test process sufficiently determines whether the plan will work in an actual disaster, and how reliable the test plans assumptions are. From there, the auditor can then determine if the test results are sufficient to ensure that the DRP could bring back the application in a time and manner that would prevent any significant or unnecessary business interruptions.

User Support

One of the most overlooked aspects, of any application, is whether there exists adequate end user support in order to control risk. Auditors will be looking for evidence that user documentation around the application, in the form of user manuals, online help, etc., is readily available and up to date. If the application

© SANS Institute 2005 Author retains full rights.

was developed within the organization or has aspects of it that were, there should be a document update process that is documented and followed.

There should be processes in place, used by management, to identify any training needs. For example, a process to monitor productivity in terms of the application should be in place. From this process, management could determine if a lack of adequate training is the cause for decreasing productivity. Along these lines, the auditor will expect to see that any issues that users have with the application are tracked and an escalation process is in place. If a user requests an enhancement, there should be a process to validate the need and address with the user the feasibility and/or timetable for the enhancement to be implemented.

Most large organizations are moving towards centralized help centers for their end users. Weber states that support staff "must have a high level of interpersonal skills so that they can interact effectively with users" (314). It is likely that the auditor will contact the support staff and assess their ability to effectively solve any problems that arise in, or around, the application.

Change Management

A page on Tripwire's website states "Change management and operational stability go hand in hand". No IS auditor in today's business climate could refute that statement. IT professionals need to understand the basic concept that all changes to an application must go through a formal, standardized process. The auditor is first going to ensure that this process is documented and being followed.

That cornerstone of an effective change management system is that all changes are documented, whether they are break fixes, enhancements, or major revisions (releases). It is essential that any change to the application is first initiated by a request that is reviewed and approved by the appropriate associates. The documentation around the change management process needs to specifically call out who can request changes, who can approve changes, and who can move these changes into production. The auditor is looking to ensure that these three roles are not held by the same people.

Beyond the approval process, the auditor will be looking for evidence that an assessment of the impact of the change has been completed. Any issues from this assessment must be addressed through a back-out plan for the specific change. Performance and security impact reviews will also be requested to show that the consequences of the change have been looked at in a manner sufficient to control the risk of the change.

An emergency change process must also be in place to handle the situations where the normal approval process will take to long in order to sufficiently meet the business requirements placed on the application. This process should

© SANS Institute 2005 Author retains full rights.

document want constitutes an “emergency” as well as demand a more detailed approval process after the emergency change has been implemented. This is done to ensure that the change does not detrimentally affect the business objectives. The auditor will review these documents and probably request a sample of recent changes, including emergency changes, to ensure that the proper approval was obtained and process followed.

All changes to the application should be logged, tracked and properly documented in some centralized system. There are many change management software products available on the market today. The auditor should have access to the system, and can provide an opinion on whether the system is effective in tracking the changes.

IS Auditors will certainly request documentation around the testing of these changes as well as for the testing process itself. Regression testing is an important aspect of control around the application that auditors especially like to see. This type of testing shows that the application’s influence on other business processes is being monitored effectively.

Auditors will test to ensure that programmers/developers cannot make changes to the production version of source code and that separate test environments exist so that development, test, QA, staging environments, and production are all logically segregated. Furthermore, auditors will look for evidence that Source/object code are synchronized with production code and that a Software release process is documented and in place. There should be ample evidence, provided to the auditor, that code is managed effectively.

Approved test plans should be available for the auditor’s review and have backing documentation that the approval was done by the appropriate individual(s). User sign-offs after testing will also be verified. The documentation around the change itself, including test plans, user sign-offs, walkthroughs, etc. should be stored in an appropriately secure area.

General Controls

Outside of the application itself, there are processes, standards, systems, etc. that could have an effect on the application. Auditors define these as “infrastructure” or “General” controls. These can include:
- System Administration / Operations
- Organizational Logical Security
- Physical Security
- Organizational Disaster Recovery Plans
- Organizational Change control processes
- License control processes
- Virus control procedures

© SANS Institute 2005 Author retains full rights.

It is during this process that the auditor will review the controls over the operating systems (UNIX, Linux, Windows, Novell, etc.), databases (Oracle, Access, etc.), and hardware (PCs, Mainframes, etc.). The review will be very “high level” and performed in such a way to rely on other audits of these specific systems within the organization, to determine that the application being audited is not placed at risk as a result of inadequacies within these areas. The physical security component is generally just a checklist to ensure that assets are protected through sprinkler systems, alarms, security guards, “deadman” doors, etc.

Third Party Services

The auditor will look at the controls around any third party services that are required to meet business objectives for the application or system. It is important that a relationship manager role is present for the third party and that this individual or group is in constant contact with the third party. Auditors will request the contract with the vendor and review to ensure that: it follows company procedures, was reviewed and signed off by legal, and is current.

The auditors will be seeking a valuable tool known as a SAS 70 evaluation. The SAS 70 stands for Statement on Auditing Standards No. 70, and is an auditing standard developed by the American Institute of Certified Public Accountants (AICPA). According to the “About SAS 70” website, the “SAS No. 70 is the authoritative guidance that allows service organizations to disclose their control activities and processes to their customers and their customers' auditors in a uniform reporting format. A SAS 70 examination signifies that a service organization has had its control objectives and control activities examined by an independent accounting and auditing firm. A formal report including the auditor's opinion ("Service Auditor's Report") is issued to the service organization at the conclusion of a SAS 70 examination.”

Beyond the SAS 70, the auditor will be looking for evidence that a service level agreement framework is in place and its metrics are reviewed. Furthermore, evidence that periodic reviews of SLAs and contracts are performed will be requested. Appropriate non-disclosure agreements and monitoring / reporting processes should be in place and continuity of services requirements should be defined.

Conclusion

In the shadow of world terrorism and corporate scandals, IS auditors are fast becoming a mainstay in the IT department. New legislation and competitive global economics almost guarantee that organizations will want to be sure that they have the controls in place to mitigate internal and external risks. Information security professionals can readily understand that the application audit presented in this paper simply outlines the controls that they are themselves attempting through security. It is essential that IT and audit work together in organizations to better understand the concepts of risk and control and ensure that the business objectives are met in an effective and appropriate manner.

© SANS Institute 2005 Author retains full rights.

References

"About SAS 70." sas70.com. 2004. 13 Oct 2004 <http://www.sas70.com/about.htm>

"Best Practices The Key to Risk Reduction, Control, and Operational Stability." Tripwire.com. 2004. Tripwire, Inc. 13 Oct 2004 <http://www.tripwiresecurity.com/practices/index.cfm>

Gallegos, Frederick, Sandra Allen-Senft, and Daniel P. Manson. Information Technology Control and Audit. Washington, D.C.: Auerbach /CRC Press LLC, June 1999.

Hurley, Ed. "Auditor: There's nothing to fear." Search Security.com. 8 April 2002. Tech Target. 17 Aug. 2004 <http://searchsecurity.techtarget.com/qna/0,289202,sid14_gci815576,00.html>.

Internal Audit Department. Dept. home page. University of Delaware. 4 Oct. 2004 <http://www.udel.edu/Treasurer/intcntrldef.html>.

James, Geoffrey. "The Auditors Are Coming...the Auditors Are Coming...And That Could Be Good News for You." CIO Magazine. 4 April 2003. 21 Oct 2004 <http://www.cio.com/archive/041503/audit.html>.

Le Grand, Charles. "Pressures Changing the Audit Profession." theiia.org. 1 June 2002. IT Audit. 11 Oct. 2004 <http://www.theiia.org/itaudit/index.cfm?fuseaction=forum&fid=451>.

Oliphant, Alan. "An Introduction to Computer Auditing - part 6." theiia.org. Vol. 2, April 1, 1999. IT Audit. 17 Aug. 2004 <http://www.theiia.org/itaudit/index.cfm?fuseaction=forum&fid=192>.

Palmquist, Scott. "Decrypt the Keys to Wireless Security." Wireless Systems Design. April 2004. Penton Media. 8 Oct. 2004 <http://www.wsdmag.com/Articles/Index.cfm?ArticleID=7917&pg=2>.

Peterson, Brad et al. "Ten Key Questions for Developing Effective Service Level Agreements." Outsourcing Center. 21 October 2001. Everest Partners, L.P. 07 Oct. 2004 <http://www.outsourcing-best-practices.com/ten.html>.

Walch, Damian. "Holistic Approach is Key to Network and IT Recovery and Security Success." Disaster-Resource.com 2004. 11 Aug. 2004 < http://www.disaster-resource.com/articles/03p_064.shtml>.

© SANS Institute 2005 Author retains full rights.

Weber, Ron. Information systems control and audit. Upper Saddle River, NJ : Prentice Hall, 1999.

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2005 Author retains full rights.

Last Updated: September 5th, 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
SANS Tallinn 2015	Tallinn, EE	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Baltimore 2015	Baltimore, MDUS	Sep 21, 2015 - Sep 26, 2015	Live Event
Data Breach Investigation Summit & Training	Dallas, TXUS	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Perth 2015	Perth, AU	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 Seattle 2015	Seattle, WAUS	Oct 05, 2015 - Oct 10, 2015	Live Event
SANS DFIR Prague 2015	Prague, CZ	Oct 05, 2015 - Oct 17, 2015	Live Event
SOS: SANS October Singapore 2015	Singapore, SG	Oct 12, 2015 - Oct 24, 2015	Live Event
SANS Tysons Corner 2015	Tysons Corner, VAUS	Oct 12, 2015 - Oct 17, 2015	Live Event
SANS Gulf Region 2015	Dubai, AE	Oct 17, 2015 - Oct 29, 2015	Live Event
SANS Tokyo Autumn 2015	Tokyo, JP	Oct 19, 2015 - Oct 31, 2015	Live Event
SANS Cyber Defense San Diego 2015	San Diego, CAUS	Oct 19, 2015 - Oct 24, 2015	Live Event
SANS Sydney 2015	Sydney, AU	Nov 09, 2015 - Nov 21, 2015	Live Event
SANS South Florida 2015	Fort Lauderdale, FLUS	Nov 09, 2015 - Nov 14, 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
Security Leadership Summit & Training	Dallas, TXUS	Dec 03, 2015 - Dec 10, 2015	Live Event
SANS Milan 2015	OnlineIT	Sep 07, 2015 - Sep 12, 2015	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced