Global Information Assurance Certification Paper

Information Technology General Controls – A Top-Down Audit Approach
GIAC GSEC Practical Assignment Version 1.4b
Michael Roberts
March 16, 2004

Abstract
Information Technology General Controls may seem like an abstract idea to some. However, the existence of these controls is what helps ensure the security, confidentiality, availability and integrity of corporate data and is therefore an integral part of the overall business.

General controls are not limited to those discussed below, however, these should be the focus when considering how the Information Technology (I.T.) processes support the business. The following discusses three overall information technology general controls: access control, change management, and operations. Each general control may be reviewed individually, though the entire control environment should be considered when evaluating effectiveness of these controls.

For each section, typical well-controlled environments are outlined. These are the controls that should be considered and evaluated when an auditor is performing a review. In some cases, a 'specialist' may be required to perform an adequate assessment of controls. The specialist is typically an individual with in-depth knowledge and experience in one particular area. Based on the complexity of the environment, this individual should be incorporated into the review if the auditor's skill set does not match that of which is being reviewed.

Access Control
"Security audits frequently expose the presence of obsolete user identifications that can be exploited, often maliciously, to gain legitimate access into corporate networks." [1] As the data and knowledge capital are crucial to the existence and success of any company, the securing of these valuable assets should be made a top priority. Most companies consider their data secure, but as an auditor, the following should be evaluated.

There are three aspects of access control that need to be considered: physical, logical and external logical access. Each of the three sections will detail typical controls within each process and briefly touch on their evaluation from an auditor's perspective.

Physical Access
"…Combining physical and information security brings physical security into the security information management application domain with the promise of greater integration across the enterprise with network, systems and storage management." [2]

Though physical security may have been a secondary concern for many companies during year's past, it has increasingly become an area of focus.

When analyzing the physical security of any company, there is both the "physical" aspect of the building (i.e. exterior doors, alarms, cameras etc.) to take into consideration, as well as the processes that are in place to grant, restrict and terminate access to the building(s) and its secured areas (i.e. data center, control room, etc.).

To conduct an adequate and efficient evaluation of how physical access is controlled, one must first perform a "walkthrough" of the building and secured areas within the building. This typically can be best facilitated when led by an authorized individual, usually a supervisor or manager that has job responsibilities relating to the physical access of the building. While on this walkthrough, the following should be observed and evaluated for the building in general as well as the data center or any other secured areas:

- Exterior Doors/All Entrances and Exits
- Access Control Devices (i.e. Swipe Card readers)
- Security/Alarm System
- Cameras/Motion Detectors (i.e. "Access Indicators")
- Environmental Controls (i.e. Fire and Flood protection, Natural Disaster, etc.)
- Emergency Procedures
- Back-up Power Supply
- Policies and Procedures/Physical Access Handbook

After the walkthrough has been completed and specific questions relating to observations have been answered, the processes that allow and disallow access to the building and its secured areas should be investigated.

As with any process, it first needs to be understood and documented clearly. Supporting documenting such as policies and procedures should be obtained and reviewed. If these policies and procedures are communicated or are available for all employees, this should be noted as well. Typically, in a well-controlled environment, an authorized individual must use a formalized physical access request form to request access to the building and/or its secured areas. The request is generally then setup by an appropriate individual, and a picture ID should be given to the employee. The request form would then be either imaged or saved as is and cataloged to preserve the audit trail. Changes in access should be performed in a similar manner, though a new ID however, would obviously not be necessary for every change in access. Also, terminations should be communicated to the appropriate individual on a prompt basis. This may be performed by the business (functional) area, or by the Human Resources department. As long as its clearly defined by the business, either one would suffice.

Finally, an actual evaluation of current employee access should be performed. Based on the size and complexity of the company, a sample of users may be evaluated based on for example, job title and function. Inquiries of questionable access should be raised to management and any breakdowns in the physical access setup process should be communicated as well. Of note, this evaluation should occur on a regular basis to increase control.

When auditing, the procedures as detailed above are a minimum of what should be in place in order for controls within the physical access process to be considered "effectively operating".

Logical Access

Though physical access may seem trivial to some degree as it is tangible and in plain-view on a daily basis, logical access and the associated proces ses may be considered a bit more elusive. Though there are many different kinds of logical access (i.e. Operating System, Database, Application, etc.) with various levels for each one (i.e. 'Superuser', 'root', etc.), one solid process can generally be im plemented that covers all possible access.

However, one process for all types and levels of access is generally not enforced. Companies tend to focus on end -user or application -level access, but the other types, typically those that are more high -powered and generally reserved for Information Technology (I.T.) personnel, may go left unchecked. A standard, controlled request for application -level access typically is as follows:

- A manager, supervisor or otherwise authorized individual documents (explicitly by application) the request on a 'user access r equest form'.
- The form is sent to the help desk or other segregated (functionall y) area in which the setup in access is performed.
- The newly setup employee is emailed his/her user name and password indicating that the setup has been completed.
- The user would then login, and would then be prompted to change his/her password.
- Terminations are communicated timely via a standard form and access is appropriately removed.

The above process can generally be consid ered "controlled" for the application-level logical access process. However, when evaluating the logical access process, it is not sufficient to only consider this level of access. Though many users may rely on this access for their everyday job function , there are other more powerful users that should be of concern as well.

The process in place for granting users to any of the following should be considered within scope when evaluating the logical access process:

- Operating System Level
- Database Level
- Fire wall
- Routers
- Intrusion Detection System
- VPN/Remote Access
- Telephony System
- Any other system/application in which access to business resources is granted

Though the user base for the above entities is usually relatively small, the access request process should not deviate from the one formerly outlined.

Additionally, when performing a review of the logical access process, other control points should be considered and evaluated. This should include assessing policies and procedures around the logical access process and how these are communicated to all employees, evaluating password controls for all systems and applications, and inquiring about reporting and monitoring (logging) of events (i.e. security breeches) and the ensuing review of these events.

External Logical Access

An extension of logical access as defined above that has become much more relevant in the recent past is known as external logical access. This type of access refers to the general public (those that have Internet access) and their ability to access a company's website and other corporate systems that may interface with the Internet. Though many companies have made strides to increase the security of their web presence, there are constantly new threats that must be considered. A current hot topic and concern for many companies is the security of their web application(s). "Web applications invite public access to an organisation's most sensitive data. Customer information, transaction information and even proprietary corporate data can be accessed through web applications." [3]

Based on the business and how a company utilizes the Internet, a scope of review that entails one of the following methods should in most cases be performed to assess exposure.

Currently, there are three methods that are used to assess the security and vulnerabilities of a company's web presence. The first is known as "black-box testing" and involves an external 'attack' using many standard techniques that a hacker might employ. Such techniques typically lead to well-known vulnerabilities and allow companies to quickly and systematically correct this unwanted exposure. Downfalls of this approach include the fact that it's a point in time assessment and that despite many vulnerabilities being exposed, some may go without discovery based on the scope and timing of the review.

The second method of assessing vulnerabilities from an external logical access perspective is known as "white-box testing". This method of review involves the detailed analysis of a specific web application and the code it is written in. This technique does not however take other considerations such as server configuration or interfacing systems.

The last and most telling method of external logical access assessment is known as "gray-box testing". This form of testing essentially combines both black-box and white-box testing techniques in order to gain the most complete picture of a companies Internet presence and associate risks. [4]

Though the in-depth scope of how external logical access is reviewed is beyond this paper, it should not be overlooked when evaluating the general controls within an I.T. environment. A specialist that understands both the

methodology and technology should perform an adequate review and assessment of a company's web presence.

Access control is critical in maintaining the security and confidentiality of data and knowledge capital. The three areas as outlined above should not be overlooked when evaluating the overall security of an environment.

Change Management

Change management consists both of software and hardware or infrastructure change management. These processes should not be thought of as mutually exclusive as each may have an impact on one another. From implementing a large piece of software on an inadequate server, to the decommissioning of a production machine, these processes will at some point impede on each other.

Both types of change management have a large impact on a company and if not performed in a controlled manner, can pose serious risk. Of the two, software change management or "program change" is typically more of a concern to an auditor and though highly important in maintaining the integrity and confidentiality of data, hardware change management should not be overlooked.

The first portion of this section will focus on software change management, how it's typically performed when done so in a controlled manner, and areas of greatest concern for an auditor while the second will focus on hardware change management.

Software Change Management

"Even the most reliable hardware is useless if software changes are implemented poorly…software's availability is most at risk when it's being changed."[5] Typically, there are several steps within the software change management process and therefore, several areas in which the process has the potential to breakdown or lack control. It is therefore important when analyzing the process that all controls are taken into consideration on a whole as opposed to being looked at individually.

In a company that has a well-controlled software change management process, the following controls would most likely be in place and operating effectively:

- Software change management procedures exist and are clearly documented and understood by all parties involved in the process.
- Requests are initiated by and approved (functional as well I.T. personnel) by authorized individuals.
- A minimum of two logically separate environments exists (typically known as 'Test' and 'Production').
- All changes are coded outside of Production.
- All changes are tested, normally referred to as integration testing, prior to being moved to Production.
- Changes are approved and documented (electronic or hard copy) by authorized personnel prior to being moved into Production – Typically

this would be either supervisor or manager level but could also be director or higher if the change has a significant impact on the business.

- Individuals who develop or code the change should not have access to move the change into production as this should be done by designated individuals, not other programmers, in order to preserve segregation of duties.
- Once placed into production, end-user acceptance testing is performed and a signoff is obtained once the user is satisfied that the change is working as requested.
- Emergency software change management procedures should be documented with the standard software change management procedures and should closely follow the standard process including adherence to the outlined controls above

Based on these controls, there are several considerations that need to be addressed. The following will briefly discuss the way some companies may handle (or should handle) software and logical environment differences.

First, many environments may have change management software implemented. Mainframe environments may uses packages such as *ChangeMan*® or *Panvalet*® while Microsoft predominant environments may incorporate *MS Visual SourceSafe*®.[6] These software packages may have inherent functionality built in and may control access to some degree, however, each of the above controls should not be overlooked if an environment is utilizing a change management package. As with any software, poor implementation or poor understanding of the software may reduce its effectiveness in controlling the environment.

Another consideration with regard to software change management is "configurable" changes. These changes typically are for applications and usually are with regard to a setting, a report change (i.e. a field may be added or deleted) or even the application of patch. From the literal definition, a company may not consider these actual software changes, as they do not involve a coding change. However, from an auditor's perspective, these should be considered changes and should follow the same controlled process as all other changes. The reason being is that though source code may not directly be modified, functionality of the application itself is being changed.

All systems and applications critical to the business fall within the realm of software change management and therefore should follow a controlled process. Specifically, this process should cover changes to not only applications and operating systems, but databases, firewalls, routers, Intrusion Detection Systems, etc.

Finally, it is important to note that all considerations based on individual environments and how the software change management process functions should be clearly documented in formalized procedures.

Hardware Change Management
Though sometimes an afterthought, hardware change management impacts the I.T. environment in a substantial manner. Hardware changes may range from a variety of events including: routine maintenance, server shutdowns, new equipment implementation and obsolete equipment decommission.

As with the software change management process, controls should be in place to maintain the integrity of data and also to reduce the risk of lost or unrecoverable data. For a company that is utilizing an effective hardware change management process, the following controls should be in place and working as designed:

- Hardware change management procedures exist and are clearly documented and understood by all parties involved in the process.
- Requests are documented and approved by authorized individuals.
- The request should detail the change management plan and should approximate the impact and risk to the business.
- Hardware changes should first be performed in a "test" environment and stress-tested. If the hardware fails in this environment, it will near certainly fail in the production environment. [7]
- After the change has been completed, a post-evaluation should be performed and documented by both I.T. personnel and a small number of end users (if impacted by the change).

As is the case with the software change management process, there are several considerations that a company must address based on their individual environment. The most important of these considerations should be based on policies and procedures.

As the hardware change management process can be considered more subjective that other I.T. processes, formalized policies and procedures should be detailed enough so that very little is left to interpretation. When an auditor reviews these procedures for adequacy, the following should be clearly stated:

- The process for assigning risk should be defined, including the different levels of risk.
- The change management plan that is required for all changes should be given set parameters of detail required.

Consisting both of software and hardware changes, the Change Management Process has a significant impact on the rest of the business. Controls within this process help maintain confidentiality and integrity of data while also allowing for better management of the process itself.

Operations
Unlike Access Control and Change Management, Operations is far more abstract in nature and therefore more difficult to audit. As a good portion of what is included within this category is forward thinking, being able to conclude on the overall effectiveness of Operations becomes rather complex.

Though complicated and less straightforward in nature, the importance of Operations and controls within the processes should not be neglected.

The following will outline the areas typically included within the Operations realm, discuss what an auditor would in general look for when auditing, and then briefly touch on the difficulties that an auditor may come across when evaluating effectiveness.

Disaster Recovery Planning

Disaster Recovery Planning (DRP) is an area that has moved to the forefront on many companies' priority list. Disaster Recovery Planning, usually linked to Business Continuity Planning (BCP), should be clearly defined and understood by the business prior to undertaking the large task in developing the plan itself. Defined, Disaster Recovery Planning is the process by which a company undertakes procedures to resume normal operation of the Information Technology function in the event that a disaster disrupts this function, or part of it, making it unavailable. All companies should recognize, "Information is a corporate asset. Records containing information necessary to restore functions affected by an incident or disaster must be protected."[8]

As downtime or loss of data will adversely impact any company, a lack of advanced planning raises the risk associated with such an event.[9] A well-designed plan that is documented and kept up to date as well as tested on a regular basis, should at a minimum include the following:

- The identification of the critical recovery period in which networks, servers, applications, etc. are given a priority and time frame in which each must be recovered.
- An updated, ongoing agreement to use an alternative processing site other than the current site.
- Documented escalation plan should exist and include the names of the decision-making personnel
    - This plan should clearly define each level of escalation and the severity and impact on the business.
    - Also, all relevant contact information of key individuals should be included.
- Documented procedures for all I.T. and functional personnel to follow in order to establish the resumption of business.
- An up to date listing of backup files needed to recover systems and applications as well as ensuing instructions for personnel to follow in order to recover and resume business.
- A service level agreement with vendors that guarantees replacement of critical hardware and equipment within a specified period of time.

Another area of importance within Disaster Recovery planning is with respect to the backup and recovery of critical data and all interfacing systems. As the integrity of data is essential for businesses to operate successfully, this process should be documented and included within the disaster recovery procedures. Typically, these procedures should at a minimum, include the following:

- A backup of schedule of all significant data as well as interfacing systems
- Updated hard copy documentation of all system software, configurations, patch-levels, and potentially source and object code
- Detailed procedures of how backups should be performed for all critical systems
- An off-site storage plan in which it is detailed as to the frequency of offsite rotation of DVD's, CD's, or tapes and how the media is stored and categorized.

At a minimum, the Disaster Recovery Plan should be tested annually to ensure the plan is working as designed. A formalized DRP that is detailed, complete in nature, and tested on a regular basis, should limit the amount of downtime in the event of a disaster.

The procedures above, which are typical when adequate Disaster Recovery Planning is being performed, should be reviewed and assessed for reasonableness. As the only way that the plan can sufficiently be evaluated is based on testing, all testing documentation performed by the company should be retained. If testing documentation is lacking or if testing itself is not being performed, it is far more difficult to evaluate the completeness and effectiveness of the DRP and it would not be prudent for an auditor to conclude on the plan itself without subsequent detailed procedures. These procedures would typically involve bringing in a specialist with adequate experience to evaluate the plan. However, this still may not be enough for one to be comfortable that a plan would be even sufficient in the event that it is necessary. Auditor judgment, based on experience, should be used in this instance.

Business Continuity Planning

A Business Continuity Plan should be in place that covers all critical business processes. The plan should extend beyond the Disaster Recovery Plan and provide detail as to how critical business processes will continue to operate if the facilitating technology is unavailable. An analysis by the company needs to be performed in which business processes are analyzed, given priority in relation to each other, and documented. An analysis of this type will require participation by many different functional areas within the company as business continuity is an overall business issue, not only an IT one.[10] At a minimum, the following activities should be undertaken by the business:

- Develop and document procedures for all major processes and corresponding information flow
- Conduct a business impact assessment to determine the impact of a disruption
- Assess the risk of a disruption on an ongoing, regular basis
- Develop a strategy for recovery
    - This should include identifying the recovery period for each critical process and determining the timeframe in which recovery of these critical functions must occur before the organization's ability to continue is in question.

- Also, detailed processes of how these functions will be carried out when computer operations are unavailable should be made priority.
- Maintain an up to date detailed listing of equipment u sed and corresponding user manuals.
- Assess the risk of a disruption on an ongoing, regular basis.

As is the case with Disaster Recovery Planning, an adequate Business Continuity Plan should be reviewed and assessed for reasonableness. Also, the best way to evaluate a Business Continuity Plan is by reviewing testing documentation as typically retained by the company. Lack of testing documentation would result in the incorporation of a BCP specialist and the ensuing evaluation. This may or may not be suff icient, and in this case well, professional auditor judgment should be used to determine if an opinion could be given on the plan.

Production Control

Though not always incorporated into the Operations category, production control, or job scheduling, shoul d be considered when reviewing companies Information Technology General Controls. Production Control is most prevalent in mainframe environments, and refers to scheduled and unscheduled 'jobs' that are run on a regular (or irregular if related to and unsc heduled job) basis. As production control is most often seen in the mainframe environment, we will assume this environment when discussing the control environment.

The risk associated with production control involves what the 'jobs' are actually doing. Most importantly, these jobs may perform regular updates of data. Some data may not be considered critical to the company, however, other data may directly relate to a critical process. As such, uncoordinated or poorly controlled job scheduling may lea d to systematic errors and inevitably downtime.[11] It would imprudent to overlook the access security and change management processes that relate to production control. Combine this assessment (as previously outlined) with the type of data and information that is being transacted through production control, and a risk factor should be evaluated. Based on this risk, an auditor should determine if further inquiry and evaluation of the actual process should be performed.

Overall Assessment

As discussed throu ghout, there are several control points within each process that can potentially have a significant impact on a business if not implemented or operating effectively. From an auditor's perspective, experience and knowledge of how to look for and evaluate t he many controls that may or may not be in place is key to performing an assessment of Infor mation Technology General Controls. Finally, when an evaluation is performed, all controls that make up each process need to be considered. Contro ls should not be considered mutually exclusive, as only a comprehensive view of the control environment will allow for a thorough and accurate assessment to be performed.

Reference:

[1] Malik, Bill. " Information security policy: Answering to the board of d irectors." Computerworld. 18 Sept. 2003. URL: http://www.computerworld.com/securitytopics/security/story/0,10801,84767,00.htm l (16 Mar. 2004).

[2] Willoughby, Mark. " Bridging the divide: Information security meets physical security." Computerworld. 28 May 2003. URL: http://www.computerworld.com/security topics/security/story/0,10801,81589,00.html (16 Mar. 2004).

[3] Wood, Peter. "Web Application Hacking: Exposing Your Backend." 11 Nov. 2003. URL: http://www.net -security.org/article.php?id=599 (15 Mar. 2004).

[4] Hemler, Joseph, Andrew Nairn and Kerry Rollins. "What's in Your Web Root? An Introduction to Grey Box Web Application Security Testing." (8 Aug. 2003).

[5] Schlieben, Paul. "Streamline Your Change Management Process" 1 Sept . 2000. URL: http://www.iseriesnet work.com/resources/artarchiv e/index.cfm?fuseaction=vi ewarticle&CO C ontentID=8096 (16 Mar. 2004).

[6] *ChangeMan* is a registered trademark of Serena while *Panvelat* is a registered trademark of Computer Associates and *MS Visual SourceSafe* is a registered trademark of Microsoft.

[7] Humphrey Watts, S. "Five reasons why projects fail." Computerworld. 20 May 2002. URL: http://www.computerworld.com/developmenttopics/development/story/0,10801,71209,00.html (16 Mar. 2004).

[8] Stremple, Rosalie and Michael F. Martone. "Disas ters Come in All Sizes" *InfoPro*. March 2000.

[9] Apicella, Mario. " Disaster recovery taken to heart." InfoWorld. 25 Feb. 2003. URL: http://www.computerworld.c om/hardwaretopics/storage/story/0,10801,78804,00.html (16 Mar 2004).

[10] Sanborn, Stephanie. "Considering Continuity". InfoWorld. 29 Mar. 2002. URL: http://archive.i nfoworld.com/articles/fe/xml/02/04/01/020401febccase.xml (16 Mar 2004).

[11] Stedman, Craig. "Don't Forget About ROI." Computerworld. 22 Apr. 2002. URL: http://www. computerworld.com/databasetopics/data/story/0,10801,70389,00.html (16 March 2004).