Global Information Assurance Certification Paper

GIAC GOVERNMENT AGENCY:

Brian C. Dufour

Information Security Officer Training

SANS GISO Practical Assignment Version 1.3

In Partial Fulfillment of the GIAC/GISO Certification

Abstract

This research paper is for the partial fulfillment of the GIAC/ GISO certification. The organization is a fictional agency within a cabinet level department of the Federal Government that manages the corporate level Budget and Accounting system used by the agencies within the Department. The paper covers the business operations of the agency, its IT infrastructure, and the risk that the organization faces to its business operations and the information it is responsible for securing. There is also an evaluation of security policy that focuses on one of the risks identified and a revision of that policy. Procedures are also created to implement the policy.

ASSIGNMENT ONE

Description of GIAC Agency

The GIAC Agency is part of a larger government department of the United States Federal Government called DIAC. Its mission is to manage the corporate level Budget and Accounting financial management system for the entire DIAC Department and provide customer support to the four agencies within the Department who use the financial system. Federal accounting encompasses not only regular accounting entries from transactions, but also budget accounting because the budget is recorded on the books at the beginning of every fiscal year. These agencies' offices are located throughout the continental United States. The agencies in DIAC that use the financial management application pay GIAC out of their own appropriations. GIAC relies on revenue from the use of this system to fund its operations. Currently the GIAC is only serving DIAC but in the future it would like to develop and implement other financial systems to service other departments of the Federal Government.

The financial system was developed, implemented and is administered and maintained at the GIAC site in South Alabama. There are 87 employees who work for GIAC at the site. These include software developers, database administrators, system engineers, and accountants to provide support to users of the system, a security access administration group, and a Quality Assurance (QA) team to test all software before it enters production. In order to ensure that the agency is compliant with Federal mandates and guidelines on Information Security the Senior Executive of GIAC appointed two employees to be the Information System Security Managers.

Information Technology (IT) Infrastructure of GIAC Agency

Described below is the IT infrastructure and what GIAC does to secure that infrastructure (See Appendix A for diagram). The goal of GIAC in protecting its information resources is to ensure the Confidentiality, Integrity and Availability of its information that its clients rely on and that other agencies within the Executive Branch, such as the Office and Management and Budget (OMB), need to have to report to Congress. The responsibility to protect this financial information is also a legal one.

The Computer Security Act of 1987, The Privacy Act of 1974, and OMB Circular A-130 provide mandates and guidance on what has to be done to secure Federal information systems. Circular A-130 calls for, "adequate security", which means, "security commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of information."

The Budget and Accounting system is the financial management system that the agencies within DIAC use is housed on an IBM mainframe. It uses OS/ 390 version 2.10 as the operating system. It is written in COBOL and uses DB2 as the database. The security software that is used on the mainframe is RACF.

GIAC has two Hewlett Packard Proliant DL 360 servers that are used for its application that produces financial statements for the reporting purposes of DIAC. These servers are running Windows 2000 for servers. One is the application server the other is the Oracle database server. Data is downloaded from the mainframe and placed into the database. The servers are using McAfee ant-virus software.

GIAC has a web based Customer Service software application that is used to collect problem tickets put in by users of the financial management system. The customer agencies load a client for the software onto their workstations at their site. GIAC provides the CD's for this to the agency. This software runs on a Dell PowerEdge 6600 server running Windows 2000 Advanced Server. It also runs McAfee anti-virus software.

In the GIAC DMZ the GIAC Web server is running Apache HTTP Sever version 1.3. The web server has information relating to the mission of the GIAC organization as well as information for users of the Budget and Accounting system about changes to the system or to the accounting operations. Users are allowed to request documentation on the different parts of the system, but such documentation will only be sent to a valid government address of the agency making the request. The e-mail gateway is also in the DMZ using McAfee anti-virus software. There is also an external DNS server in the DMZ.

All workstations are using Windows 2000 Professional with the Microsoft Office 2000 sweet of systems. McAfee anti-virus software is used to scan for viruses. The network administrators push down updates to the desktops. They are scanned automatically when users logon to the system.

The remote users of the GIAC systems connect through a Virtual Private Network (VPN). The VPN server is located outside the firewall at the border router. The VPN is configured to block traffic among the various sites when the VPN fails.

The firewall used is a Check Point firewall. It is configured to provide Network Address Translation for traffic leaving the GIAC site.

The router is a CISCO High Capacity router providing border protection.

The switches used are Cisco Catalyst 6000.

The Intrusion Detection System is the latest version of SHADOW, version 1.8.

GIAC keeps its systems update to date with the latest patches, services packs, and any emergency fixes. The network administrators and the system engineers for the mainframe have this responsibility with the Security Program Managers providing oversight of this. When a server or application is placed into service a checklist to harden the system is supposed to be used. The last Risk Assessment of any of the GIAC systems was four years ago.

The building that GIAC is housed in is a secure government site. Guards contracted out to GIAC protect the building. All personnel are required to have badge identification to enter the building and are required to have them visible at all times. The mainframe and the servers are housed in a windowless room in the building that is climate controlled and has a fire suppression system. Cameras monitor it and only authorized personnel are allowed into the room. Users must use an access card to enter the computer room.

All the systems and the network are backed up nightly and all tapes are removed to a secure off site location. GIAC is located in South Alabama and has to worry about Hurricanes during the months from June to November. GIAC has put together a Disaster Recovery Plan and team to go to another site in the event the GIAC site is down. This plan is tested once a year.

Business Operations

The GIAC agency developed and implemented a financial management system to be used by the agencies within DIAC to provide the Department with a common Budget and Accounting system. This would provide the financial managers with uniform accounting standards to follow and provide a way for the Department to measure the performance of its overall budget. The use of one system developed by GIAC has also saved DIAC money. The time and money saved from having to consolidate the information from the old budget and accounting systems from the individual agencies within DIAC has been substantial. The development of the system in-house also saved money and provided the users with a system that would serve the needs of a Government agency. GIAC views itself as a agency providing a vital customer service to the agencies within DIAC and it must do everything to provide the best service and the most secure systems for its users.

The financial management system encompasses several different modules. These include such functions as accounts payable and receivable, property and asset management, a procurement module for acquiring goods and services, the budget accounting module, a general ledger module and a disbursement module that makes payments to vendors. Data entry clerks input data from source documents directly into the system for processing at the various agency locations. The agencies also have staff

people such as accountants, property and procurement officers, budget officers, and users who certify payments out of the system who also use the system on a daily basis. On an average day GIAC has about 900 users touching the system.

Access to the different modules and the functions within that module is controlled by the application. The security functions can allow a user to only scan data in the system, input data, or actually update documents in the system and have the system process them. The data can also be locked down to where a user in one agency will not see the data of another agency. When a user requires access to the system a request is made by the agency Security Officer who handles access request for the Budget and Accounting system. The request is reviewed for the proper signatures and if everything is correct the user is placed in the system. These Security Officers in the agencies are given a *Budget and Accounting System Security Guide* by GIAC to help them perform this function.

The data in the Budget and Accounting system comes from the daily transactions that the agencies have in the course of their business. The data entry clerks input information from bills, vouchers and other source documents into the system. The accountants review the data and make adjustments as needed. The Budget Officers keep an eye on the budgets to ensure that the agency does not exceed its spending authority. The Property and Procurement personnel keep track of the assets of the agency and handle purchasing for the their agency. A nightly processing cycle is run every night to keep the information timely. There is a lot of data produced in the system, as it is the entire DIAC Department using it.

GIAC also uses the functional side of the system for its budget and accounting, but must also bear the burden of keeping the technical side of the system running and secure. The system engineers are responsible for the proper functioning of the IBM Mainframe computer. They are given very high-level access as system engineers and their knowledge is very important to the GIAC agency. There is a policy of rotating the duties of the engineers but it has not been enforced the last couple of years.

The software developers handle the maintenance of the Budget and Accounting system and develop upgrades and enhancements as user requirements change over time. The Development system is logically isolated from the Quality Assurance (QA) environments and the Production environments on the mainframe. Once the code is written it is tested in development and then moved to the QA team who performs testing independent of the developers. The QA team writes its own scenarios for this. Production access is not granted to the developers or the members of the QA team to the Budget and Accounting system.

The database administrators are responsible for maintaining the DB2 databases that the system uses. Their access is also very high-level to the Development, QA and the Production environments. They perform routine maintenance to keep the databases finely tuned to ensure the highest level of performance for the customers.

The accountants in customer support are the GIAC employees who are allowed into the Production system to view all the data of the agencies. They are granted access by the agency Security Administrators after a request has been sent to them by the GIAC Security Access Group. Scan access is the only level that they are allowed to have. They use this access to respond to tickets placed into the Customer Support System. Once a problem is fixed they respond either by phone call to the user or e-mail. This group also makes sure the documentation on the web server is up to date and that request for manuals get to the right people.

They also use the Financial Statements application to produce the statements that DIAC uses to report to OMB and Treasury. The statements are produced monthly, quarterly and annually and e-mailed to DIAC headquarters and then distributed to the proper recipients. The accountants are also granted read access to the files on the mainframe that are produced by the Budget and Accounting system and then downloaded to the Financial Statements database. This is done to check the source file in case there are data elements missing.

The Security Access Group grants access to the mainframe, the network and the applications. They also are responsible for monitoring the IDS and Firewall and reviewing the logs from the mainframe security software. The two employees appointed Information System Security Managers are part of this group. Their job is to provide oversight to the security of the entire GIAC organization.

The Budget and Accounting system is the crown jewels of GIAC. The information on this system is the proprietary financial information needed to run the entire department and the security for it is the responsibility of GIAC. The loss of the confidentiality, integrity, and availability of this financial data would harm GIAC and the Department as whole. It could impact budget request, violate certain laws such as the Prompt Pay Act if vendors could not receive there money on a timely basis, harm small business who rely on contracts with GIAC and other agencies in the Department, and invite Congressional inquiries. There is also information that is covered under the Privacy Act of 1974. This system does the payroll accounting for the department and information such as Social Security Numbers and banking information is a part of the data. Information on individual citizens must be protected as a matter of the law. GIAC executives are legally liable if information is compromised and harm results from it. In the post 9-11 world there is increasing pressure to have government operations continue in the event of a disaster, both natural and man made. GIAC must be able to meet the new demands imposed by this change in the environment.

There would be a loss of confidence in GIAC if it could not live up to the responsibility of keeping the Budget and Accounting system, its main source of revenue to fund its operations, secure and available to its customers.

ASSIGNMENT 2

GIAC Areas of Risk

It is important for an organization that manages sensitive information and information technology assets to know the risk that those systems face. The public and private sector have become permanently attached to the hardware and software that provide the information they require to run their business and satisfy the needs of their customer. GIAC is no exception to this. Below three risk that GIAC faces are discussed.

Risk 1

The first area of risk to GIAC's crown jewels is the unauthorized alteration of data and unauthorized access to data in the Budget and Accounting system by employees. This could happen in a few ways.

- One is that a Security Administrator could grant the wrong level of access to a user either by mistake or with criminal intent to commit fraud.
- A developer could write a program to make payments to themselves, or a system engineer or database administrator could delete or manipulate data by accident or on purpose.
- An accountant could alter data to cover up mistakes or fraud.
- A user with the wrong access could view personal information of employees such as Social Security Numbers, bank account numbers, or salaries of individuals.

This risk is a concern to GIAC because the Confidentiality and Integrity of the data is very critical to the entire Department. There are billions of dollars that are appropriated to the Department and the potential for fraud, waste and abuse is too great to ignore. GIAC is entrusted with making sure that this information stays accurate and secure. This is how it operates and pays its employees.

The consequences of the above risk are many. The first is the loss of taxpayer money due to a mistake because a user had access they were not supposed to have, abused the access they did have, or through theft of government funds through fraud. This would no doubt invite Congressional and media inquiries into the Department and cause the removal of GIAC executives. If the integrity of the information were suspect this would cause financial reporting to be false or misleading to Congress and lead to budget reduction or unnecessary increases to it. The loss of data confidentiality could bring serious legal ramifications to employees and executives of GIAC. If vendor bids are released it could disrupt the process of how the government obtains goods and services that are of a high quality and give the taxpayer the best for their money. Any of this would destroy the confidence of GIAC customers and force the Department to look for a new system and organization to process their financial information.
GIAC can take the following steps to mitigate this risk:

- Train the Security Administrators in the proper way to grant access in the system. This training should be given on a yearly basis to refresh them.
- Every month a report of the users of the system and their access levels should be produced and reviewed by managers in the agencies. Any users who have

changed job function or have left should have their access changed or deleted. Once the report is completed it should be certified by the agency administrator and sent to GIAC's Information System Security Managers.
- Review access levels to ensure that separation of duties is enforced in the application.
- Enforce the policy of rotating the system engineers and rotate the database administrators on the database they work on.
- Extensive background checks should be made of all employees and include criminal and credit history checks.
- Ensure that there is proper training for all users of the system for their particular job duties.
- Remind all employees of the legal consequences of fraud and theft in annual awareness programs.
- GIAC Information System Security Managers should make surprise audits of the agencies to review the procedures of the Security Administrators.
- Create a Configuration Management Process that includes code reviews.

Risk 2

There is the threat to GIAC's site due to natural disaster or terrorism.
The GIAC site is located in south Alabama about 45 miles from the Gulf of Mexico. This area has experienced many tropical storms, hurricanes and tornadoes over the years. GIAC is also a government site that could be targeted by terrorist, both foreign and domestic.

There is always the threat from tropical systems during hurricane season. Louisiana was hit by a tropical storm and a hurricane within a week of each other in 2002. A major storm could destroy all the assets of the GIAC agency in just a few hours, cause flooding and structural damage, or knock out power to the site indefinitely. September 11 and Oklahoma City showed how far terrorist are willing to go to achieve their goals. While it is not as visible as a national monument or a well-known government building, the GIAC site still has the potential to be attacked by terrorist. GIAC must plan for either one of these scenarios or any other type of disaster that would interrupt business operations.

GIAC is concerned about this because without the proper planning for such an event it could cease to exist as an entity and the loss would be catastrophic to DIAC. Even a short disruption in customer service could cause customer agencies to find another organization to perform the functions that GIAC does for them. Financial information must be timely and accurate to make proper decisions. GIAC must plan to be able to avoid any long term down time no matter what the disaster.

The consequences of this risk could be:
- The loss of life. Lawsuits would be possible it GIAC did not take the proper steps to deal with this risk.
- The loss of millions of dollars in computer hardware and software.

- Loss of business for GIAC. Government agencies have more options than they did years ago. GIAC provides a service that could be replicated by another government agency or by the private sector. If GIAC is unable to give its customers the comfort of being able to get back online quickly, they will leave and go elsewhere.
- Employee morale falling if the shutdown leads to furloughs.
- Employees may leave for another job if a prolonged shut down occurs. Talented people will not sit around and wait for GIAC to rebuild while they try to make ends meet. Once GIAC is back up it could be without the people who kept it running before the disaster.

GIAC can take steps to mitigate this risk. They are:

- Perform a threat assessment of GIAC. According to Michael Miora in the *Computer Security Handbook*, "Threat assessment is the foundation for discovery of threats, and their possible levels of impact," (Miroa, *Computer Security Handbook,* p. 43-2)
- Conduct the Disaster Recovery test more than once a year to ensure backups are working.
- Perform annual reviews of the site where tapes are stored for recovery operations.
- Perform a Business Impact Assessment to determine to see how long GIAC can be down before a serious impact is felt.
- Develop a Business Continuity Plan and test at least twice a year.
- Store critical system documentation off site and the Disaster Recovery and Business Continuity Plans off site.

Risk 3

GIAC faces a risk because the Risk Assessments of its systems and security program are outdated. The last one was done four years ago. Security breaks down over time and technology evolves rapidly creating new risk and new threats. Failing to know the risk to your systems is unacceptable for an agency with a mission such as GIAC's.

GIAC must be aware of the risk facing its systems and very concerned about them. There are inherent risks in a financial system that must be eliminated, mitigated, transferred or accepted. If GIAC does not know and understand these risks, as well as the other risks associated with operating information systems in today's computer environment, it will have a hard time proving due diligence on its part if a threat were exploited and some kind of harm resulted.

The consequences from failing to have regular Risk Assessments done on systems and the overall security program can lead to an overall breakdown of security. According to the National Institute of Standards and Technology (NIST) Special Publication 800-12, "Risk management is the process of assessing risk, taking steps to reduce risk to an acceptable level and maintaining that level of risk." If GIAC does not do this then the

potential exploitation of the risks to its systems could have devastating repercussions to the agency if it fails to manage those risks. The customers have to trust and have confidence that GIAC is providing a safe computing environment to process and store their information. The reputation of the agency is important if it wants to attract other non-DIAC customers to use its Budget and Accounting system package.

GIAC can mitigate this risk by doing the following:

- Institute a strict policy that calls for a Risk Assessment on all the systems under the management of GIAC and its overall Information Security Program. The policy will say how often an assessment is required.
- Create a Risk Management Board made up of managers, security personnel and IT personnel to review the risks assessments and have the power to take appropriate measures to mitigate those risks.
- In the awareness program for executives include the importance of Risk Management and the consequences without one for GIAC.

ASSIGNMENT 3

Evaluation of Security Policy

This policy for Risk Assessments was taken from the SANS Security Policy Project web site. The policy is in appendix B and can be found at the following link: http://www.sans.org/resources/policies/Risk_Assessment_Policy.doc

This policy relates to GIAC's lack of policy on performing risk assessments on its systems and its overall security program.

Purpose

The purpose of the policy is clear in that it states that it gives the power to conduct risk assessments to the Information Security staff and the responsibility to them to remedy the findings that are found to be a threat. This shows the organization recognizes the need to perform these assessments and is putting in writing that recognition.

The policy is lacking in a giving a specific time when to do these assessments. The use of the word periodic is too vague. OMB guidelines require a risk assessment every three years or when there is a major modification made to the system (see Circular A-130). GIAC as an agency in the Federal Government falls under this regulation. The policy should state this in its purpose. It also allows the Information Security team to do the assessments, but an assessment should be overall and they should be included in it. That is why the assessment team should be independent of the organization.

Background

The policy does not contain a background section. The background should go into why this policy is needed to let the reader know the importance having up to date risk assessments. This can be accomplished in the purpose section. This section is optional to GIAC.

Scope

The scope of the policy is clear and broad on what systems, procedures and what organizations can have risk assessments performed on them. This allows the organization to assess the systems it interconnects with to provide a degree of security with that connection. It also allows a company like GIAC to assess the security administration at the agencies that use the Budget and Accounting system.

Policy Statement

The policy statement is good at specifying the responsibility of the employees who are responsible of the systems that will be assessed. They are expected to cooperate in both the actual risk assessment and the remediation process after the assessment. This should be in writing because it provides a measure of accountability for managers and their employees.

The policy statement does not explain why the policy will help the organization with its risk management. There is no reasoning in the policy statement to help the reader understand the ramifications if the organization does not perform this function. GIAC business depends on providing a secure computing environment and assessing the risk to those systems and environment and mitigating them is a vital part of agency policy.

Responsibility

There is no section in the policy that spells out the responsibility of persons for this policy. However, in the purpose and policy statements sections the responsibility of who is supposed to do the risk assessments and the responsibility of the employees is spelled out for the reader. It might be wise to place a section with this subject to make things easier for the reader so they can understand any part they must play in the policy's implementation.

Action

The policy does not have an action section. There is nothing in the policy that says when it should go into effect. It does not define the time when a decision should be made to perform a Risk Assessment. This is needed so that the responsible persons will know when to make this decision to be in compliance with the policy.

The policy is a good starting point for GIAC. It is realistic and a policy that can be implemented. The enforcement section is a good way to drive home the importance of the policy. The definitions help add clarity to it and help the reader who may be new to the job.

Policy Revision

GIAC Risk Assessment Policy

Purpose

The purpose of this policy is to ensure that independent risk assessments are conducted on the information systems under the management of GIAC and on its overall Information Security Program to keep them up to date. Federal regulations require risk assessments be performed on information technology systems under the control of Federal agencies every three years or when a major modification has been made to the system. GIAC will adhere to this regulation. GIAC must maintain an acceptable level of risk to the information assets under its management to avoid violating laws and regulations of the United States and protect the information of its customers.

Scope

The independent risk assessments shall include all of the information systems under the management of the GIAC Agency and GIAC's Information Security Program. The information technology systems risk assessments will include all applications, hardware, software, telecommunications, networks and their processes. The program risk assessment will include all policy, procedures, and how they are administered to manage the overall all Information Security Program of GIAC.

Policy Statement

GIAC has been entrusted with processing the financial information of the DIAC Department. In order to maintain the confidentiality, integrity and availability of that information so managers can make informed financial decisions GIAC will assess the risks to the systems that process this information and the systems that support them every three years or if a major modification is made to them. GIAC will also review every two years its Information Security Program to make sure that policy and procedures are followed and that they enhance the security posture. Information security breaks down over time with the changes in technology and keeping risk assessments up to date helps manage the risk to GIAC's systems. Once the assessments are completed the GIAC Risk Management Board will review the findings and will take appropriate measures to mitigate the risks that are at an unacceptable level. GIAC expects every employee to provide their full cooperation when the assessment teams are conducting the risk assessments.

Responsibility

The chief GIAC Information System Program Manager and their deputy are responsible for seeing that this policy is enforced and for making revisions as needed. They will also manage the contracts with the independent assessment teams.

The chief Information System Program Manager in consultation with the Senior Executive of GIAC will choose the members of the Risk Management Board.

The managers of the various departments in GIAC are responsible for seeing that all their employees cooperate with the assessment teams.

The Risk Management Board will be responsible for reviewing the findings of the assessments and then developing a Plan of Action and Milestones to mitigate the risk to an acceptable level.

Action

This policy will be in effect the beginning October 1, 2003

All assessments for the information technology systems and for the security program will be completed by September 30, 2004. Once this is complete and all information systems have an up to date risk assessment a review will be done to determine if any changes to the systems will cause the need of another risk assessment or the system can wait until the end of the three years.

The Risk Management Board will be put together and chartered by January 1, 2004.

Develop Security Procedures

Once GIAC has brought its risk assessments up to date it will be much easier to adhere to the Risk Assessment Policy. Since that policy calls for a risk assessment on information systems every three years or when a major modification is done a procedure will have to be put into place to review a system modification to determine if it is major and will affect security and will therefore trigger a new risk assessment. Major modifications may include but are not limited to such changes as a operating system upgrade, a new release of software or moving an application from one platform to another (i.e., mainframe to a UNIX system).

What actions should be carried out for this procedure?

- All GIAC information systems that will undergo a major modification during the fiscal year will submit the proposed change to the Information System Program Manager's office for formal review.

- The Information System Program Manager's office will have 30 days to respond to the proposal on whether it is a major modification.
- If it is determined to be a change that requires a new independent risk assessment the department that submitted the request will be notified. The change will not be allowed to go into production until a risk assessment has been completed and any risk identified will be mitigated. The department will work in conjunction with the Information System Program Manger's Office to obtain the contract for the risk assessment.
- If the change does not require a new risk assessment then the department is notified and may proceed with the implementation of the change.

Why are these actions important?

This process must be in place to provide a control over the management of the GIAC's information resources. The organization must know when a change will occur to its systems so it can be sure that all measures are taken to account for risks to the system and all necessary countermeasures are taken to mitigate those risks. It will also keep GIAC in compliance with Federal regulations.

Who is responsible for carrying out the actions in this procedure?

The departments that will be making a change to the system or systems under their management are responsible for submitting the formal proposal to the Information System Program Managers Office for review. They must provide a detailed analysis of the proposed change that will include what they believe the impact to security will be.

The Information Security Program Manager is responsible for reviewing the analysis of the change and provides its own analysis on the impact to security. The Information Security Program Manger is the final authority on whether the change requires a new independent risk assessment.

When should the actions be taken?

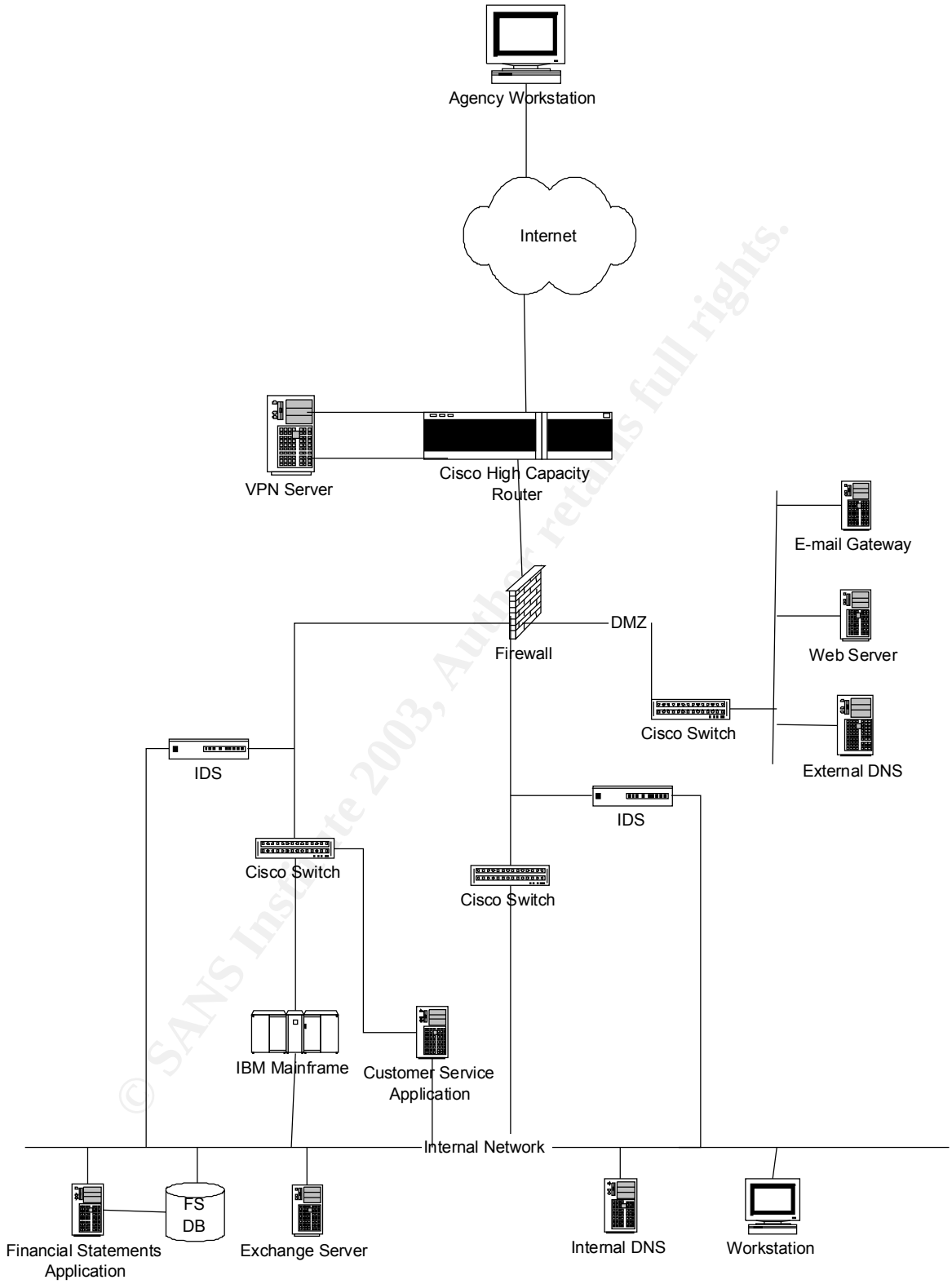
The proposal for a modification should be submitted to the Information Security Program Manager once the department knows what the change will be. That means the hardware or software change has been decided and how that change will take place has been made formal and the analysis on the impact to security has been completed.

The Information Security Program Manager will review the proposed change and conduct its own impact to security and respond to the department making the request in 30 days. If a risk assessment is needed a contract will be put in place to bring in an assessment team from outside the organization.

How is this procedure checked?

This procedure is part of the internal controls of the GIAC Agency. It is subject to audits by the DIAC Office of the Inspector General, risk assessments of the Information Security Program, and by any outside audit such as the General Accounting Office.

Appendix A



Appendix B

Risk Assessment Policy

1.0 Purpose
To empower InfoSec to perform periodic information security risk assessments (RAs) for the purpose of determining areas of vulnerability, and to initiate appropriate remediation.

2.0 Scope
Risk assessments can be conducted on any entity within <Company Name> or any outside entity that has signed a *Third Party Agreement* with <Company Name>. RAs can be conducted on any information system, to include applications, servers, and networks, and any process or procedure by which these systems are administered and/or maintained.

3.0 Policy
The execution, development and implementation of remediation programs is the joint responsibility of InfoSec and the department responsible for the systems area being assessed. Employees are expected to cooperate fully with any RA being conducted on systems for which they are held accountable. Employees are further expected to work with the InfoSec Risk Assessment Team in the development of a remediation plan.

4.0 Risk Assessment Process
For additional information, go to the Risk Assessment Process.

5.0 Enforcement
Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6.0 Definitions

Terms	**Definitions**
Entity	Any business unit, department, group, or third party, internal or external to <Company Name>, responsible for maintaining <Company Name> assets.
Risk	Those factors that could affect confidentiality, availability, and integrity of <Company Name>'s key information assets and systems. InfoSec is responsible for ensuring the integrity, confidentiality, and availability of critical information and computing assets, while minimizing the impact of security procedures and policies upon business productivity.

7.0 Revision History

References

Miroa, Michael. “Computer Security Handbook.” Edited by Bosworth, Seymour. Kabay M.E. New York, John Wiley and Sons. 2002. 43-2

Office of Management and Budget. “Management of Federal Information Resources. OMB Circular A-130.

National Institute of Standards and Technology. “Special Publication 800-12: An Introduction to Computer Security: The NIST Handbook. October 1995. 59

http://www.sans.org/resources/policies/Risk_Assessment_Policy.doc