GIAC Enterprises

Risk Assessment and Security Procedure Policies

Paul Jankowski

Information Security Officer Practical
Version: 1.2 (January 13, 2003)

Table of Contents

1. Assignment 1 – Describe GIAC Enterprises

1.0 Abstract

The following is a practical assignment intended to demonstrate my understanding of the GIAC Information Security Officer course. I created a fictional company, GIAC Enterprises. I identified the top security risks to the organization and provided appropriate policies and procedures to mitigate those risks.

1.1 Mission of GIAC Enterprises

GIAC Enterprises will be the preferred provider of health carrier services for businesses and individuals in the communities we serve.

1.2 Description of GIAC Enterprises

GIAC Enterprises is a health insurance carrier for businesses in the Midwest. We currently employ 500 employees. GIAC is a Third Party Administrator for Self-Funded Employee Benefit Plans.

GIAC is located in Reno, Nevada and has been in the employee benefit service business since 1992 providing clients with superior claim administration services. GIAC has access to a select number of preferred stop-loss markets and offers a variety of services. GIAC has a professional and experienced staff with state-of-the-art equipment to provide the services necessary to implement and maintain a successful employee benefits program.

GIAC administers benefit plans for 265 companies covering 200,000 to 250,000 people throughout the United States. GIAC offers the following services:

Medical, Dental, Disability, and Vision Claim Administration
Medical Case Management and Utilization Review
Full-Service Sales and Marketing
Billing and Eligibility Administration
HIPAA and COBRA Administration
Flexible Benefits Administration
Consulting Services to Health Care Coalitions/Initiatives

1.3 IT Infrastructure

GIAC Enterprise has created a strong alliance with key players in the computer industry. Those players are IBM, Cisco, Microsoft and Dell. GIAC's philosophy is that standardization and familiarity is an additional component to security.

All servers and workstations are Dell computers. Each server and workstation is created from a standard image to meet the strict guidelines and standards set by the National Security Agency and other recognized organizations.

Hardware Configuration: Desktop

Dell Optiplex GS260
Intel Pentium 4, 2.0GHz/400MHz front side bus, 512K advanced transfer cache, 512Mb memory, 20GB hard drive, 3.5" Floppy drive, integrated 100Mb ethernet adapter, and 17" color monitor.

Hardware Configuration: Server

Dell PowerEdge 460
Intel Pentium 4, 2.0GHz/400MHz front side bus, 512K advanced transfer cache, 8GB memory, 73GB hard drive RAID 5 array, 3.5" Floppy drive, integrated 100Mb ethernet adapter, and 17" color monitor. DLT VS80 tape drive is used for daily backups.

The tape rotation consists of ten tapes for each server. Five tapes for each day of the week and the other five for each Saturday of the month. The five Saturday tapes are labeled one through five and rotated based on which week of the month it is to backup. Each tape is labeled with the server name and day it is to be used on. All tapes are kept off site and are rotated by a certified and bonded courier. The off-site location is sixty miles from GIAC at a records retention center. The tapes are kept in a locked case. There are six cases, one for each day of the week and Saturday.

Two people manage the inventory of backup tapes. If an engineer needs a tape for recovering a file, they must fill out a form showing the date, the engineer requesting the tape and provide a reason why the tape is needed. This is done with one of the inventory personnel, who is then responsible to make sure the tape is replaced within a reasonable amount of time.

All network devices, switches, and routers are Cisco products. The redundant firewall is a Cisco Pix firewall that allows for the filtering of all inbound and outbound traffic. This is what is termed a single point of entry. All Internet traffic goes through this firewall to ensure GIAC is not exposed to hackers. All ports on the firewall are turned off, except the ports necessary for business operations.

The firewall is configured to direct all SMTP traffic to the FTP server. The FTP server then scans the email using Network Associate's WebShield SMTP antivirus software. Any infected emails are cleaned or quarantined and all clean/non-infected email is forwarded to the Exchange Server. Outgoing mail follows the same process in reverse. Outgoing emails go from the Exchange server to the FTP server where they are scanned and sent out for delivery.

The PIX firewall has conduits between the FTP server and outside customer NAT address. Conduits define what type of connections are allowed to an inside host and are always required when a lower security host is connecting to a higher security host.

The conduits allow the source host access to the destination host using the specific protocol and port, which makes the defined connection very secure.

For this reason, the term conduit is used to describe the path between the two devices. Cisco Secure TACACS is used for FTP customers to authenticate through the firewall. This application allows customers to send their employee data files into GIAC Enterprises for processing.

The DMZ consists of a FTP server, an external Web server, and the Momentum file transfer system. Cisco Secure TACACS server is used to authenticate any FTP users into the DMZ for file transmissions through Cisco Secure's database. No internal traffic is allowed into the DMZ unless a conduit is established for that device. Currently two conduits exist from the FTP and Momentum servers to the SQL Database server inside the network. The PIX directs external https traffic to the secure web server (Momentum), http traffic to the external web server, and external FTP traffic to the FTP server.

The FTP server also functions as a SMTP server for GIAC and resides inside the network. This server has IIS 4.0, service pack 6a, to communicate with the Secure Web (Momentum) server.

The “external” web server is only for an established company presence on the Internet. There is no connection between the internal network and the external web server. The web server runs IIS 4.0 with service pack 6a.

The main file transfer server is the Momentum Intelligent Network Gateway. It serves as a point of contact between customers and GIAC’s employees on the internal network. This server has IIS 4.0, service pack 6a, with 128-bit encryption to ensure high level security to customers using Momentum’s Secure Web product. The Momentum server will be described in more detail in the next section.

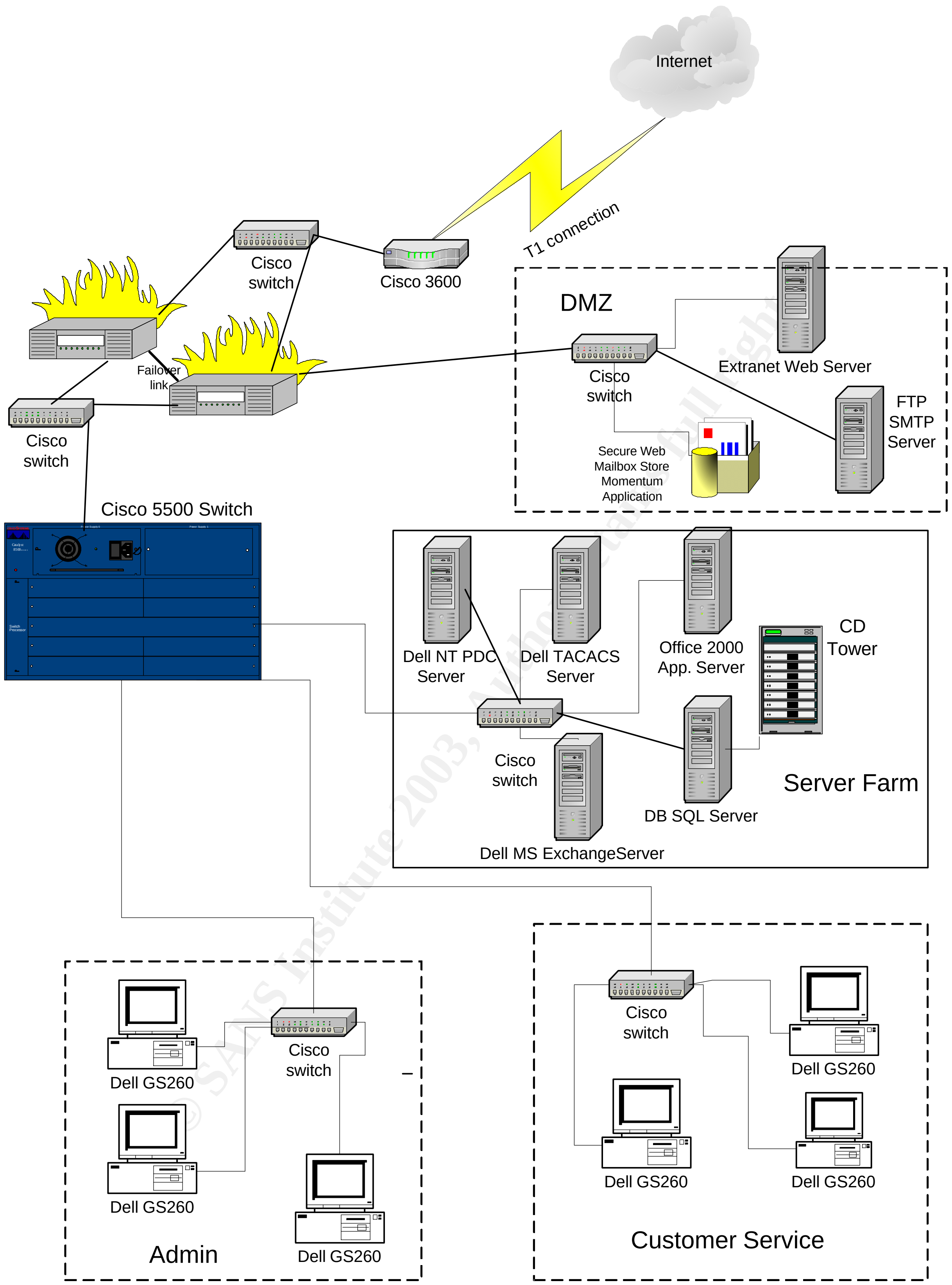
The internal network is an untrusted single domain environment. All software used on the network is Microsoft, with few exceptions. All servers run Microsoft's NT 4.0 server with service pack 6a and Network Associate's NetShield antivirus software.

The data base server is an SQL server with service pack 7. This server receives the data from the files received by the FTP and Momentum servers and processes the data. GIAC employee’s interface with the SQL server to update client records. Updated records and reports are sent back to the FTP and Momentum servers for customers to retrieve.

TACACS server is based on the GIAC standard NT Server platform and resides inside the network. Cisco Secure ACS Release 3.0(2) Build 5 is the cisco device monitoring application installed on this server. It supports several methods of authorization, authentication, accounting and reporting of each cisco device. The TACACS server allows only authorized personnel to make configuration changes of updates to the Cisco devices. A Senior Network Engineer reviews the logs generated from this server on a daily basis.

The mail server is Microsoft Exchange version 5.5 with service pack 4 and Network Associate's GroupShield antivirus software.

All workstations run Microsoft's Windows NT Workstation 4.0 with Microsoft Outlook 98 mail client. The business applications are from the Office 2000 suite with service pack 2 and Network Associate's VirusScan antivirus software. GIAC has implemented a policy based network that locks down desktops so users only have access to network drives and application menus they have rights to.


Internet
T1 connection
Cisco switch
Cisco 3600
Failover link
Cisco switch
Cisco 5500 Switch
DMZ
Cisco switch
Extranet Web Server
FTP SMTP Server
Secure Web Mailbox Store Momentum Application
Dell NT PDC Server
Dell TACACS Server
Office 2000 App. Server
CD Tower
Cisco switch
DB SQL Server
Server Farm
Dell MS ExchangeServer
Dell GS260
Cisco switch
Dell GS260
Admin
Dell GS260
Cisco switch
Dell GS260
Dell GS260
Dell GS260
Customer Service

1.4 Business Operations

Communication to and from outside business partners through the Internet is crucial to the day to day operations of GIAC Enterprises.

GIAC sends and receives all its data between its customers through FTP or secure web connections. Both servers have a directory that the customer connects directly to, based on their customer profile. The customer drops off data files with changes to their selected insurance providers. Employee status changes (full time to part-time or vice versa), turnover, or employees selecting a new insurance provider would be included in the data files.

GIAC Enterprise's "Crown Jewels" is the combined data, or information that resides on the SQL server. This information is received from vendors or insurance companies and the customers. Aetna, Mutual of Omaha, and CIGNA are examples of vendor or insurance companies represented by GIAC. JC Penny, Ford Motor Company and IBM and their employees are examples of the customers that subscribe to GIAC services.

The data on the Secure Web (Momentum) server and the FTP server only reside there for a very small amount of time, as that data is either passed onto the SQL server or it is passed onto the customer.
The format of the employee data file contains the company ID, insurer ID, employee number, name, address, social security number and plan number (to identify the insurance provider).

FTP Connection
As we all know FTP has been viewed as an insecure protocol by virtue of clear text data transfer. To address this issue, GIAC has instituted the following security procedures for its customers:

- **Static NAT IP address** GIAC only allows static NAT IP addresses through the firewall. The purpose is to only allow communication between GIAC's PIX firewall and the customer's firewall. An example of this security in action would be if a terminated employee from a customer's site were to attempt to send a fake file from outside of his company's firewall he would be unable to breach GIAC's firewall.

Double authentication Once the customer's static NAT IP address is allowed through GIAC's firewall the customer is required to authenticate through two servers: Cisco TACACS and the FTP server. All FTP customers first authenticate through TACACS, which is a server that, as a Windows NT service, controls the authentication, authorization and accounting of users accessing GIAC's network ("Overview of Cisco") all FTP activity and accounts for. It tracks all successful and unsuccessful logon attempts by outside users and has the ability to lock out accounts based on these unsuccessful logon attempts. Once the customer is authenticated through TACACS, they are then required to authenticate through the local FTP server. Once in, the customer is logged into its own FTP root directory that they only have access to. The customer directories are setup as hidden to prevent a savvy user to browse other customer directories. Even if a customer knew another customer's directory name they would be unable to browse within it due to their customer specific directory permissions.

Secure Web Connection

The other file transfer solution is through SSL file transfers over the internet through Momentum's Secure Web product. The customer uses their preferred browser of choice to establish a connection to the Momentum server. The Momentum server uses Microsoft IIS and is secured with a 128-bit encryption certificate through VeriSign established Certificate Authority software. This allows file uploads and downloads via HTTPS with a web browser. HTTP file transfers are not allowed. The only similarity to FTP security is that only the customer's static NAT IP address is allowed through the firewall.

Once the NAT IP address is allowed through the firewall the customer logs into the local Momentum server, located inside a DMZ. The customer is then logged into their own hidden directory where they may upload or download files.

Distinguishing Customer Files

The Momentum server has an automated application process that has been developed to scan for files in the customer directories on both the FTP and Momentum servers. With the high volume of inbound and outbound files each file must be identified properly.

Momentum's software requires a unique profile ID for each customer file. For inbound traffic, customers are given a file layout that requires them to add a header record that contains a unique segment Momentum software scans to identify the file and direct it to the correct profile. The profile is then setup to migrate the file to an internal directory for processing.

Outbound files also require a profile that requires the header record containing the unique segment to be recognized by Momentum. Once identified, Momentum will process the file and place it in the appropriate customer directory for the customer to pick up via FTP or Secure Web.

Customer communication is done by phone, or by email. GIAC only interacts with the subscriber insurance company or the customer. There is no direct contact with the individual policyholder.

Assignment 2 – Identify Risks

2.1 Data Integrity Breach

Although firewall logs are monitored regularly, a window of opportunity exists during which a network compromise would be undetected. Detection, response and containment are unpredictable without appropriate tools and procedures. An effective tool to identify and address potential intrusions or inappropriate use of data assets will improve GIAC's ability to contain and respond to unauthorized intrusion attempts from external or internal sources.

2.1.1 Observation

GIAC does not utilize an Intrusion Detection System to detect and notify on inappropriate or malicious activity from the Internet, nor do they have documented Incident Response Containment Procedures to adequately react to these situations. Currently, an informal process is in place to identify, respond, control and recover from incidents. However, a formal policy has not been developed or approved by management.

2.1.2 Impact

Without intrusion detection, an attack may go unnoticed for days only to be discovered by accident. The *Crown Jewels*, which is the information that resides on the SQL server, could be compromised or completely destroyed. Without an intrusion detection system, and documented incident response and incident escalation policies and procedures, GIAC is at risk of losing the ability to properly contain and recover from an incident. Without knowing when the integrity breach took place, the backup tapes maybe ineffective to recover from the intrusion. Such an occurrence may lead to loss of data and even a loss of reputation. Either occurrence could lead to the instability of the company as a whole.

2.1.3 Recommendation

Develop an intrusion detection system to include the implementation of both host and network based intrusion detection systems. The host-based systems should be deployed on critical servers in the network and will assist with the detection of unauthorized changes to files and directory structure. Network based intrusion detection sensors should be strategically placed throughout the network in an effort to monitor and protect GIAC Enterprises' most important IT assets.

Cisco Intrusion Detection System (IDS) would provide GIAC's desired security through the following techniques through its IDS Host Sensor product:

- stateful pattern recognition
- protocol parsing

- heuristic detection
- anomaly detection.

These techniques guard against hackers' unauthorized intrusions, Internet worms, bandwidth attacks, etc. Protection against such attacks significantly reduces downtime and protects GIAC's *crown jewels* by detecting and stopping malicious activity.

An intrusion detection system would be ineffective without an incident response and incident escalation policy and procedures. If a security breach is found, GIAC's IT staff must know what to do and when to do it. This policy should cover six specific areas: planning, identification, containment, eradication, recovery and follow-up. Each of these areas should include specific tasks that must be accomplished and procedures that should be followed to insure that the business functionality is recovered, the vulnerability that led to the incident is properly identified and patched, and that proper evidence is gathered to insure that the case, if prosecuted, is supported.

2.2 Ineffective Risk Mitigation

As businesses venture into electronic commerce, the need for secure networks is greater than ever before. Unfortunately, this increased investment does not appear to be mitigating the number or cost of incidents from either internal or external sources. An attempt to determine what threats exist, their likelihood, and the consequences or potential loss must be determined in a formalized fashion.

2.2.1 Observation

There are numerous controls GIAC IT professionals have implemented to safeguard electronic information, but without understanding what risks truly face them, they have only created a false sense of security. Few organizations invest in proper risk assessment before implementing controls. GIAC has spent and continues to spend a large amount of money and resources towards the security measures already put in place. GIAC does not have a formal Risk Assessment Policy. Without a formal process, GIAC will never know how to protect their assets.

2.2.2 Impact

The consequences of not knowing where to direct resources to mitigate risks can be profound. Not only are some threats overlooked, but also resources and budgets are misapplied to threats that do not exist or have minimal impact. Threats to information assets are not limited to technological weaknesses. Physical controls, business and operational processes, telecommunications, and employee awareness all play vital roles. Not all threats are malicious. Accidents, errors of omission, and natural disasters are equally likely threats requiring consideration.

2.2.3 Recommendation

A formalized Risk Assessment Policy needs to be established. Risk assessments only provide a snapshot of vulnerabilities in an ever changing, dynamic system. Therefore, risk assessments must be part of an ongoing process re-evaluating old vulnerabilities and identifying new ones. Only after actual threats and vulnerabilities are understood can policy and risk management decisions be implemented. A "Risk Assessment" is the analysis of the likelihood of loss due to a particular threat against a specific asset in relation to any safeguards to determine vulnerabilities. This would provide a direction for GIAC to take in securing their infrastructure and assets.

2.3 Unsecured file transfer

Controlled File Transfer Protocol (FTP) access from the Internet is allowed for select business clients and third parties. FTP is an unsecured protocol by design and even though the usage is controlled with access to only select IP addresses or subnets, it is still a risk given the ability of IP address spoofing or session hacking.

2.3.1 Observation

FTP protocol transfers the data in "clear" text format. The security in place for FTP file transfers consists of dedicated IP usernames and passwords. Distinct usernames and passwords are required by both Cisco's TACACS server and by the FTP server. These passwords also contain special characters.

2.3.2 Impact

If a hack were successful into the FTP server, the hacker would have access to highly confidential information. All of this information is protected under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). HIPAA performs the following:

- limits the use and release of individually identifiable health information
- gives patients the right to access their medical records
- restricts most disclosure of health information to the minimum needed for the intended purpose
- establishes safeguards and restrictions regarding disclosure of records for certain public responsibilities, such as public health, research and law enforcement ("The Health").

2.3.3 Recommendation

For GIAC customers with FTP access, they could be converted to the Secure Web server services or if their volume was large enough, a dedicated conduit could be established for them. PGP Enterprise 8.0 software would be used for generating data encryption keys for encrypting and decrypting the data. The conduit would secure the

FTP traffic by offering an encrypted tunnel for the data to be transmitted between GIAC and its customers.

Since these broadband Internet services are 24/7, they can leave individual machines open to intrusion. This leaves both the client and the corporate network at risk. In order to prevent hackers from hacking a session for use as an entryway to
GIAC's internal network, it is critical that security solutions are established end-to-end ("End-to-End").

3. Assignment 3 – Evaluate and Develop Security Policy

The following policy is based upon a SANS sample policy company

3.1 Sample Security 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

3.2 Policy Evaluation

This policy may suit the sample company's needs from an overall perspective, but it is too general to fulfill all the requirements of the company's Risk Assessment policy. It does a fairly reasonable job with the statements, the responsibility, and the action on issues identified. The policy is very easy to understand and reads very well. Overall it is a good first step as much of the detail is left out. A Risk Assessment policy does need stated objectives to help further guide the policy and this is a key component that is not in the sample policy.

Purpose – One-sentence states that risk assessments will be conducted to determine vulnerability and initiate remediation. While being very brief and to the point, the purpose does not state how this policy supports the overall security policy implemented by GIAC. The purpose also fails to inform us why it is being established. The purpose of "determining vulnerability and initiating remediation" is vague and could be explained with more detail so one reading this statement would have a better understanding of the purpose.

Scope – Once again the scope is a statement that is very brief and to the point. It fails to adequately define the extent of the policy, as it simply states "any entity". The scope does make reference to Third Party Agreements, which I believe is crucial in a Risk Assessment policy. How Third Party Agreements are handled need not be defined here, but direction to where to find it should be provided.

Policy - The policy is well written and does explain the policy as it is written, but fails to specifically define who is responsible for the policy. The responsibility is being left to the department responsible for that system and the company as a whole. This responsibility needs to be directly appointed to an individual who is of high rank within the organization. The policy does identify what needs to be done but it does not identify how often it needs to be done.

Enforcement – This section is a one-line statement that serves the purpose of the policy.

Definitions – This section is a plus to any reader of the policy. I believe this helps one better understand the intentions of the author.

7.0 Revision History – This section should be included in any policy, so one can accurately track the growth of the policy over its life, as it applies to the company. Knowing **when**, **who**, and **why** changes were made can help with future administrative decisions.

3.3 Revised GIAC Enterprises Information Security Risk Assessment Policy

1.0 Purpose

This Information Security Risk Assessment Policy implements and supports GIAC's Information Security Policies. The purpose of this policy statement is to outline the objectives and scope of GIAC's information security risk assessment process. GIAC is responsible for ensuring the integrity, confidentiality, and availability of critical information pertaining to the corporation and its customers, while minimizing the impact of security procedures and policies upon business productivity.

2.0 Objectives

The objectives of the risk assessment process are to:

- Periodically evaluate vulnerabilities and threats that have the potential to affect the integrity, confidentiality, legal liability, and availability of information and systems.
- Ensure that appropriate safeguards and controls are in place by periodically evaluating existing measures for adequacy.
- Provide a basis for maintaining an appropriate information security program.

3.0 Scope

The information security risk assessment policy covers technical, physical, and administrative processes that relate to the entry, processing, transmission, storage and retrieval of corporate and customer information. The policy focuses on the internal information systems and processes of GIAC, with limited references to third party service providers (i.e., outsourcers). Specific guidelines for overseeing service providers' security and risk assessment processes are outlined in GIAC's Information Security Program (see Section on Baseline Controls for Third Party Service Providers).

4.0 Policy

The execution, implementation, and maintenance of the information security risk assessment policy is the responsibility of the Director of Information Technology, who will oversee the procedures and guidelines outlined below. The results of the risk assessment will be used to ensure the continued adequacy and continuous improvement of GIAC's information security program.

The information security risk assessment process will be conducted at least annually; however, certain steps in the process will occur at more frequent intervals, as outlined in the procedures. The full process, or certain steps, may also be conducted in response to material changes in technology, information sensitivity, threats, business strategies, legal liability, and customer information systems.

5.0 Enforcement

The Information Security Officer will conduct a periodic risk assessment review of the overall information systems environment, current policies, procedures, guidelines and standards and all incidents of non-compliance. Any employee found to have violated any part of this policy will be subject to the disciplinary action based on the severity of the violation. Disciplinary action maybe a written warning placed in their permanent employment record up to and including termination of employment.

6.0 Terms and Definitions

Risk: Those factors that could affect confidentiality, availability, and integrity of GIAC's key information assets and systems.

Risk assessment: the process of identifying vulnerabilities and threats, prioritizing sensitive assets for protection, and identifying appropriate safeguards.

Threat: an event, or agent, with the potential to cause unauthorized access, modification, disclosure or destruction of information resources, applications or systems.

Vulnerability: a weakness in a system, application, infrastructure, control or design flaw that can be exploited to violate system integrity.

7.0 Revision History

Assignment 4 - Develop Security Procedures

GIAC's risk assessment process is based upon the framework outlined in Special Publication 800-30, "Risk Management Guide for Information Technology Systems," issued by the National Institute for Standards and Technology (NIST). The process outlined in the NIST guide has been customized for GIAC to include the following activities:

Step 1 – Information and data classification
Step 2 – Threat analysis
Step 3 – Vulnerability assessment

Step 4 – Impact analysis
Step 5 – Control evaluation
Step 6 – Risk determination
Step 7 – Results documentation

Each step is discussed in detail below and references are made to related GIAC documents and policy statements, as applicable.

5.1 Step 1 – Information and Data Classification

GIAC's risk assessment process considers the criticality and sensitivity of information assets in the evaluation of vulnerabilities, threats, and compensating controls. Reference is made to GIAC's Information and Data Classification Policy, which outlines criteria for categorizing information as confidential, sensitive, or public. Based on its classification, information is accorded certain treatment in terms of access controls, storage, internal and external transmission, and disposal/destruction. The sensitivity and criticality of information is considered in the risk assessment process during the impact analysis and risk determination phases. While noted as Step 1 in the risk assessment process, GIAC's information classification policy is ongoing (e.g., classifications are based on the nature of the information as it exists, not assigned at a particular point in time.) However, the classification process is considered a pre-requisite to conducting a risk assessment of information security, particularly in estimating the impact of vulnerability/threat combinations and evaluating controls, and determining residual risk.

5.2 Step 2 – Threat Analysis

The objective of GIAC's threat analysis process is to identify and evaluate potential agents of harm that may exploit existing vulnerabilities in controls or processes, and thereby impact information security. GIAC's threat analysis methodology involves identifying general categories of all foreseeable internal and external threats, evaluating the potential impact that the threat could have on GIAC's information security, and determining the likelihood that the event may occur. A summary of the analysis may be presented in a form similar to the Sample Form "Threat Analysis Summary" (see sample form on page 22). Ratings are assigned based on the foreseeable likelihood of occurrence and business impact.

The threat analysis will be conducted annually and coordinated by the ITS Department. The purpose of the annual evaluation is to determine whether certain threats have changed in terms of their likelihood of occurrence and their potential impact. GIAC recognizes that as technology and internal or external circumstances change, threats to information security will also require reassessment. The results of the analysis will be considered, in combination with the results of GIAC's vulnerability assessment, to determine the potential impact.

5.3 Step 3 – Vulnerability Assessment

The objective of GIAC's vulnerability assessment is to identify and evaluate weaknesses, gaps, deficiencies in controls or processes that may impact information security. GIAC's vulnerability assessment practices are categorized into three areas: technical, administrative, and physical. Each area is addressed by a combination of practices and techniques designed to identify potential vulnerabilities, which are described below.

5.3.1 Technical Vulnerability Assessment Practices

The following practices are conducted to identify and evaluate vulnerabilities that pertain to technical processes and controls, including automated systems, GIAC's network, connections to partners' networks, and connections to the Internet.

Network Security Assessments

Objective: Obtain an independent (third party) assessment of network security.
Scope: Assessment of network vulnerabilities (Internet and systems penetration test) and evaluation of existing controls (network assessment).
Frequency: Internet and systems penetration tests - annually; network assessment – annually.
Oversight Responsibility: Audit Department.
Output: Summary report that identifies and prioritizes weaknesses and gaps.
Other Criteria:

- Qualified third party firms will be used to conduct the assessments on a rotating basis (no consecutive engagements).
- GIAC senior management will review reports.
- Tracking reports will be created to monitor progress in addressing outstanding items (See Section 5.5, Step 5).

Internal System and Network Monitoring

Objective: Identify potential vulnerabilities in GIAC systems and monitor availability using scanning software and other automated tools (e.g., virus scanning, and intrusion detection).
Scope: Internal networks, systems, and workstations.
Frequency: Depending on the nature of the tool, scans may be conducted daily, weekly, or at other intervals, as appropriate.
Oversight Responsibility: Director of Information Technology or designee.
Output: Log reports and test results will be reviewed and summarized as appropriate, relevant metrics will be forwarded to GIAC management and the Audit Committee periodically.
Other Criteria

- Only authorized associates in the ITS department may perform vulnerability tests on GIAC systems.
- Only authorized and approved testing programs and tools may be used.

Technical Security Assessments of Third Party Service Providers

Objective: Ensure that service providers' security programs are comprehensive and adequate to meet the confidentiality, integrity, and availability requirements for GIAC's information.
Scope: Critical service provider relationships (i.e., relationships where either (1) the service provider handles sensitive customer information, (2) the service provided is essential to GIAC's core operations, or (3) GIAC is significantly dependent on the provider due to its unique offerings or the terms of the relationship).
Frequency: Critical service providers will be evaluated at least annually (refer to GIAC's Information Security Program, Section on Third Party Service Providers).
Oversight Responsibility: Director of Information Technology.
Output: Summaries of vendor security reviews will be maintained in the respective service provider's files.
Other Criteria:

- Service providers must supply current, independent security assessment reports per the terms of their contract/service level agreement with GIAC.

Expert Consultations

Objective: To ensure that GIAC IT staff stays up to date on important security developments and to determine where adjustments are needed in policies and practices.
Scope: Technology and information security related issues.
Frequency: Consultations will occur on an "as needed" basis.
Oversight Responsibility: Director of Information Technology.
Output: Summary reports or memoranda, depending on the significance of the topic and recommended action, the summary may be distributed to GIAC management.
Other Criteria: None.

5.3.2 Administrative Vulnerability Assessment Practices

The following practices are conducted to identify and evaluate vulnerabilities that pertain to administrative processes and controls, such as service provider/vendor oversight, compliance with GIAC security policies, and internal controls related to security (e.g., segregation of duties, log reviews, assignment of authorization rights).

Automated Control Checks Developed and Administered by ITS[1]

Objective: Monitor compliance with internal policies and practices.
Scope: Network and system use by GIAC associates (e.g., account activity and status, access privileges, etc.).

[1] These activities consist of a combination of internally developed programs and techniques to test system controls, including employees' adherence to policy (e.g., appropriate password strength, legitimacy of active account status, etc.). ITS runs these programs periodically and generates lists of exceptions for follow-up.

Frequency: The frequency of tests vary from daily activity summaries to ad hoc reports that are generated only when they are triggered by a specific event.
Oversight Responsibility: Director of Information Technology.
Output: Summary activity reports and event logs.
Other Criteria: Tracking reports will be created to monitor progress in addressing significant items (See Section 5.5, Step 5).

Reviews by GIAC Internal Audit

Objective: Evaluate adequacy of internal controls and administrative processes.
Scope: Compliance with GIAC internal policies (e.g., appropriate separation of duties, dual control, etc.).
Frequency: Reviews are conducted at least annually, with some areas reviewed during interim internal audit examinations.
Oversight Responsibility: Audit Department.
Output: The results of the review are included in documentation. They provide an evaluation of the adequacy of internal controls and adherence to policies.
Other Criteria: None.

5.3.3 Physical Vulnerability Assessment Practices

The following practices are conducted to identify and evaluate vulnerabilities that pertain to physical processes and controls (e.g., access to facilities and equipment).

Internal Reviews

Objective: To obtain an assessment of physical security practices, two types of reviews are conducted: (1) Physical security of documents, records, equipment, and facilities, and (2) Physical security over computers and peripherals.
Scope: Both types of reviews are designed to confirm compliance with security policies and guidelines.
Frequency: Reviews of security over documents, records, equipment, and facilities consist of branch office "self-assessments" and periodic evaluations by the Corporate Security Group and/or the Corporate Facilities Group. Reviews of computers and peripherals consist of "spot checks" and scheduled visits resulting from equipment changes at the respective site locations.
Oversight Responsibility: The review of physical security over documents, records, equipment, and facilities is conducted by the Corporate Security Group and/or Corporate Facilities Group. The review of physical security over computers and peripherals is conducted by ITS and/or the Corporate Security Group.
Output: Summary reports are provided that identify and prioritize weaknesses and gaps.
Other Criteria:

- Reports will be reviewed by GIAC senior management.
- Tracking reports will be created to monitor progress in addressing outstanding items (See Section 5.5, Step 5).

The results of the above vulnerability assessment processes will be considered, in combination with the results of the threat analysis, in the impact analysis and the control evaluation, described in steps 4 and 5, below.

5.4 Step 4 – Impact Analysis

The purpose of the impact analysis is to combine the results of the threat analysis with the vulnerability assessment to determine the potential harm that might result from a security exploit. Therefore, when reviewing the recommendations and/or exception items identified in the technical, administrative, and physical vulnerability assessments described in Step 3, GIAC will consider the likelihood and impact associated with various threat sources. The results of the Threat Analysis will be referenced to determine the impact and risk associated with identified vulnerabilities. This determination will be recorded on the Control Evaluation and Risk Determination Form discussed in Step 5 below.

5.5 Step 5 – Control Evaluation

Based on the results of periodic vulnerability assessments addressing technical, administrative, and physical systems and processes, GIAC will evaluate existing controls for adequacy and make enhancements, as needed. Upon completion of the various technical, administrative, and physical vulnerability assessments referenced in Step 3, the impact analysis will assist in prioritizing the findings (e.g., exception items) identified in the review. The impact analysis will aid in allocating efforts and resources to areas where vulnerability and threat pairs are determined to have the greatest potential impact on the confidentiality, integrity, and availability of information.

Material findings of the review will then be logged on a tracking report similar to the Sample Form "Control Evaluation and Risk Determination" (see sample form on page 24). A determination of the risk related to the identified exception item is recorded on the form in addition to the recommended action plan for remediation. Additional information related to plans for implementing or enhancing controls is also indicated on the form (e.g., responsibility and due date). Follow-up action will be monitored by management through the distribution and review of these tracking forms. Responsibility for completing the Control Evaluation and Risk Determination Form, including the determination of risk associated with an exception item, is assigned by the Director of Information Technology, with input from the Audit Department.

5.6 Step 6 – Risk Determination

Risk determination occurs at several stages of the process outlined in this document. General risk associated with identified threats is evaluated in the threat analysis (Step 2) and ratings are assigned based on the perceived likelihood of the threat and its potential impact. A risk determination is also made during the impact assessment (Step 4) when vulnerabilities and threats are considered in combination. The evaluation of controls (Step 5) also involves risk determination, as the results of vulnerability assessments are prioritized and mitigating controls are implemented based upon perceived risk.

Risk determinations are documented at each of the steps noted above, and GIAC management is informed of the decisions through the distribution of tracking reports and periodic summaries of vulnerability assessment results.

5.7 Step 7 – Results Documentation

Key documents associated with GIAC's risk assessment process include:

- Annual Threat Analysis
- Results of vulnerability assessments conducted by internal or external personnel
- Control Evaluation and Risk Determination Form

THREAT ANALYSIS SUMMARY

Threat Category/Source	Ratings	
	(1) Likelihood	**(2) Impact/ Significance**
Current insider (employee, contractor, partner) *Consider the potential for abuse of confidential information, sabotage, harassment, bribery, extortion, identify theft, fraud, data corruption/alteration, unauthorized transactions, etc.*		
Former insider *Consider the potential for abuse of confidential information, sabotage, harassment, bribery, extortion, identify theft, fraud, data corruption/alteration, unauthorized transactions, etc.*		
Hacker/cracker *Consider the potential for unauthorized access, intrusion, Data theft, data destruction, identity theft, financial frauds Information bribery/extortion, spoofing, impersonation, etc.*		
Malicious code (virus, Trojan horse, etc.) *Consider the potential for data loss or corruption, denial/disruption of service, damage to systems and hardware, etc.*		
Competitor *Consider the potential for abuse of confidential information, sabotage, theft of trade secrets, etc.*		
Terrorist *Consider the potential for data loss or corruption, denial/disruption of service, damage to systems and hardware, etc.*		
Natural Disaster (Snow/ice storm, fire, flood) *Consider the potential for denial/disruption of service, loss or corruption of data, harm or inconvenience to staff, damage to hardware/facilities, lack of access to facilities, etc.*		

Ratings are assigned based on:

(1) Likelihood: Determined based upon consideration of the following categories:
Remote – Event may only occur in exceptional circumstances.
Unlikely – Event could occur at some time.
Moderate – Event should occur at some time.
Likely – Event will probably occur in most circumstances.
Almost Certain - Event is expected to occur in most circumstances.

(2) Impact/Significance: Determined based upon consideration of the following categories:
Insignificant - Negligible consequences.
Minor - Minor consequences, damage, and/or loss.
Moderate - Significant consequences, damage, and/or loss.
Major - Serious consequences, damage, and/or loss.
Catastrophic - Worst case consequences; severe and lasting damage and/or loss.

CONTROL EVALUATION AND RISK DETERMINATION

CONTROL EVALUATION AND RISK DETERMINATION

Exception Item/ Recommendation (1)	Risk Factor (2)	GIAC Action Plan (3)	Responsibility and Due Date (4)	Current Status
Security Maintenance Local administrator account passwords, which allow unlimited access to device management functions, are rarely changed as most administration is accomplished with a domain administrator login. The administrator password should be changed in line with GIAC's standard password policy.	High	A procedure will be developed whereby local administrator account passwords for all servers will be changed according to AB-Corp's domain administrator account maintenance policy.	Information Security Officer October 2003	The process to change the local administrator passwords will be performed through scripts that are in the process of being developed by IT.

NOTES:

(1) Exception items are identified in the vulnerability assessment process and represent the results of independent tests of technical, administrative and physical controls.
(2) Risk factors are determined based on the nature of the vulnerability, the likelihood that a threat source may exploit the vulnerability, and the impact that would result from such an exploit. Risk factors are determined as High, Medium, and Low.
(3) GIAC's Action Plan includes the implementation of recommended controls (or control enhancements) as determined in the control evaluation process.
(4) Designated individuals and/or team(s) who will be responsible for implementing the new or enhanced controls.

5. References

"End-to-End Security for Remote VPN." Information Week 1 Nov. 2002: 2

Cisco IDS Host Sensors. Cisco Systems. 10 Dec. 2002 http://www.cisco.com/en/US/products/hw/vpndevc/ps976/index.html)

Cisco Intrusion Detection System. Cisco Systems. 19 Dec. 2002 http://www.cisco.com/en/US/products/sw/secursw/ps2113/index.html

PG Enterprise 8.0, http://www.pgp.com/display.php?pageID=74

The Health Insurance Portability and Accountability Act of 1996 (HIPAA). 15 October 2002. Centers for Medicare & Medicaid Services. 13 Dec. 2002 http://www.cms.gov/hipaa

Overview of CiscoSecure ACS 2.4 for Windows NT Server. Cisco Systems. http://www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/csacs4nt/csnt24/csnt24ug/ch1.pdf