

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Assignment:
GISO Basic Practical Assignment (v1.3)

Company:
GIAC Enterprises

Title:

"Locking Down the Enterprise Jewels"

© SANS Institute 2003, Author retains full rights.

By: Enrique "Rick" Perez
On: July 17th, 2003

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Table of Contents: **Page#**

Table of Contents…… 2

Abstract Summary…… 3

Organization Overview…… 3

IT Infrastructure…… 5

Network Diagram Prior to Remediation…… 8

Business Operations…… 9

Area of Risk # 1…… 12

Area of Risk #2…… 15

Area of Risk #3…… 19

Evaluate Security Policy…… 21

Revise Security Policy…… 23

Develop Security Procedures…… 26

Appendix Section …… 30

Appendix A. Security Assessment Request Form…… 31

Appendix B. Statement Of Work…… 32

Appendix C. Security Assessment Issues List…… 33

Appendix D. Final Information Security Assessment…… 34

Appendix E. Exception Request Form…… 35

Appendix F. Information Classification Policy…… 37

Appendix G. Risk # 1 Best Practices To Be Implemented…… 39

Appendix H. Risk # 2 Best Practices To Be Implemented…… 41

Appendix I. Risk# 3 Best Practices to Be implemented…… 44

References…… 45

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Abstract Summary:

The following document provides the reader a clear picture of the business objectives and infrastructure of GIAC Enterprises. Additionally, It identifies potential security risks with the current organization's infrastructure as they relate to potential security threats documented by well known industry organizations, such as, SANS, SEI CERT/CC, CSI, etc. and what mitigating steps will be implemented to address the identified risks. The document will try to emphasize that in order to protect your network from attacks; you must be able to protect your assets from external and internal users. Furthermore, it will show that solutions must work in unison where one security measure covers a gap left by another or acts as a backup mechanism in the event primary shield is penetrated. In conclusion, the document will show that a layered security approach combined with preventive measures, detection mechanisms and security policies provides GIAC Enterprises a "Defense in Depth Strategy" to stay par with the *Black Hat Community*.

ASSIGNMENT #1:

Organization Overview:

The GIAC Enterprises organization was established on 1991 in South Florida. There are 75 total staff members housed in the Miami Office, roughly 15 of them travel heavily throughout the nation. We specialize in the recruitment of IT Professionals for organizations whose core employee base consists in System Architects, System Engineers, Application Developers, Data Base Administrators, Security Specialists, Business Analysts, Testing Specialists etc. In order to be able to fill these positions, we recruit nationally for IT professionals via internet portals, educational institutions, vocational schools, job fairs, advertisement's in technical publications and partner referrals. Partner referrals come from a national recruiting network composed of companies providing similar services. Members of this network have agreed on pre-arranged placement fees for referrals. Our # 1 product offering is "GIAC Total Solution" that provides a comprehensive end-to-end solution in professional IT staffing for large to midsize Human Resources organizations. The basic services provided under this product offering to our corporate clients are as follows:

- Job Posting
  - Regional
  - National
  - Newspapers
  - Magazines
  - Internet Portals
  - Professional Organizations

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

- Candidate's Technical Screening
    - Testing for Competencies
    - Interviewing
    - Verification Technical Certifications
- Candidate's Background Checks
    - Criminal
    - Credit Profiles
    - Military
    - Academic Credentials
    - Work History
- Verification of Personal References

GIAC's Organizational Structure is as follows:

- Executive Management
    a. President / COO
    b. CIO
    c. CFO
    d. Corporate Lawyer
    e. 3 Directors
    f. 5 Division Managers
- Operations and Risk Management
    a. Account Executives (5)
    b. Senior Recruiters (10)
    c. Associate Recruiters (3)
    d. Risk Analysts (2)
- Marketing and Sales
    a. Senior Sales Representatives (7)
    b. Sales Support (6)
    c. Market Analysts (2)
- Information Systems and Project Management Office (PMO)
    a. Project Managers (2)
    b. Architects (1)
    c. Web Masters (2)
    d. Network Engineers (3)
    e. Data Base Administrators (2)
    f. Business Analysts (2)
    g. Application Developers (2)
    h. Desktop Support (2)
- Human Resources
    a. HR Generalists (3)
    b. HR Clerks (3)
- Finance and Payroll
    a. Financial Analyst (3)
    b. AP/AR Clerk (2)
    c. Payroll Clerks (2)

NOTE: No Information Security Office or Audit Function currently in place.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

IT Infra-structure:

Connectivity / Authentication:
Our network tries to leverage as much of the public Internet infrastructure as possible to be able to maintain low overhead costs. ISP connectivity for our corporate users is provided by Bell South Communications via a dedicated T1 connection. Job Candidates, Business Partners and Corporate Clients connect to our web sites using their own ISP accounts. All users authenticate via the use of a private user id and a password. Job Candidates establish their own accounts online, while Business Partners and Corporate Clients must have accounts setup via a request to GIAC Account Executive that acts as liaison with the GIAC Information Systems Group.

Network Zones:
The *internal trusted zone* of the network is reserved for critical corporate entities that must be adequately protected against external intrusions to preserve their confidentiality, integrity and availability. We protect the *Internal Trusted Zone* from external threats thru the use of two CISCO PIX 525 firewalls. One works in primary mode and the second one in fail-over mode. The **"**crown jewels" to our kingdom are the *JTS and JPS Production Data Bases*. They contain business critical and sensitive information about Job Candidates, Corporate Clients and Business Partners. They are housed within an Oracle DB Environment that resides as part of the *JTS and JPS Application Servers* also located in the *Internal Trusted Zone.* The rules defined in the firewalls reflect the security policy of the organization for incoming and outgoing traffic into and from our private network. The main objective of the firewalls are to protect internal assets from "external intrusions and attacks" and block any "malicious traffic" from coming into our private *Internal Trusted Zone*. Access to the *Internal Trusted Zone* is strictly limited to corporate staff or contracted 3rd party vendors in a "need to know" basis.

Firewall Traffic Rules:
Network traffic from a lower security zone to a higher security zone is denied by default and can only be allowed through firewall access rules. *In addition, the firewall is configured to block the following incoming traffic:*

- ACTIVEX Controls
- Java Applets
- Network File Services (NFS)
- X. Windows
- Berkley R Commands
- TELNET
- SAM
- NETBIOS
- FTP

CISCO PIX 525 configuration features are set to prevent or substantially minimize the following type of attacks:

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

- Ping of Death Attack
- Land Attack
- SYN Flood Attack
- Broadcast Attack
- Bandwidth Attack
- Covert Channel Attack

The following firewall rules are in place to allow the following traffic into the Internal Trusted Zone:

- E-MAIL communications (SMTP) through PORT 25
- Network Management using (SSH) through PORT 22
- Network Management using (SNMP) through PORT 161
- Domain Name Services (DNS) through PORT 53
- Log Records of External Network components through PORT 514
- Web Server non-encrypted traffic HTTP requests through PORT 80
- Web Server encrypted traffic HTTPS requests through Port 443

Corporate LAN Architecture:

The LAN Architecture deployed is Windows 2000 Active Directory with 75 on site workstations and 25 laptops using a standard desktop image with Windows 2000, Office 2000 Suite, VISIO and Internet Explorer 5.5. There is an MS 2000 Exchange Server that services all internal corporate mail. To provide remote access there is a dedicated RAS server that supports a modem pool ranging in speeds of 33K to 56k. There is an Internal DNS Server that replicates with an External DNS in the DMZ for fail-over purposes. The Print File Servers serve as a backup to the Main Domain Controller. Firewalls, Routers and Switches are managed by CISCO WORKS. There is Cisco 6500 Switch to handle all connectivity in the corporate LAN environment.

Demilitarized Zone(DMZ):

We have two web servers that house the Job Placement System (JPS) and Job Tracking System (JTS) applications sitting outside the PIX firewall. They are installed on Microsoft IIS Servers using Internet Explorer 5.5. They are protected by two "Border Routers" with dual ISP T1 connections to provide fail-over and to filter traffic coming from the Internet. These two CISCO 3745 routers sit at the edge of the DMZ. They protect the identity of internal addresses via Network Address Translation (NAT). These routers are also used as a "line of defense" through the use of "Reflexive Access Lists". These Reflexive ACLs shut down a session in the event of inactivity over 30 seconds to prevent a possible "session spoof". A CISCO 2950 Switch is connected to both routers and provides connectivity for servers sitting in the DMZ.

The JTS and JPS web servers are the "front doors into the business". Due to their criticality, two other web servers are in place in a fail-over mode. These components are used to conduct critical business transactions that will be described in more detail in the Business Operations section of the document. These web sites are protected via SSL X.509 Certificates issued by Verisign to provide robust 128 bit encrypted communications with our clients. The web

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

servers communicate to the application servers sitting in the *Internal Trusted Zone* through port 80 and 443. Corporate Clients and Business Partners use the Job Placement System (JPS), while Job Candidates make use of the Job Tracking System (JTS) to conduct business transactions. There is an MS 2000 Exchange that handles all Internet E-mail traffic and a DNS Domain Server that works in replication mode with internal DNS server.

Anti-Virus:

All laptops, workstations and servers located in the *Internal Trusted Zone* are deployed with Symantec Norton Anti-Virus installed and enabled. Anti-Virus updates are pushed automatically using "E-Policy Orchestrator" to all of these components. In the case of workstations and laptops, these updates take place during the LOGON process into the network.

Miscellaneous:

Home Office is equipped with scanners, color printers, copy machines and paper shredders. Internet Access is given to "all employees".

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

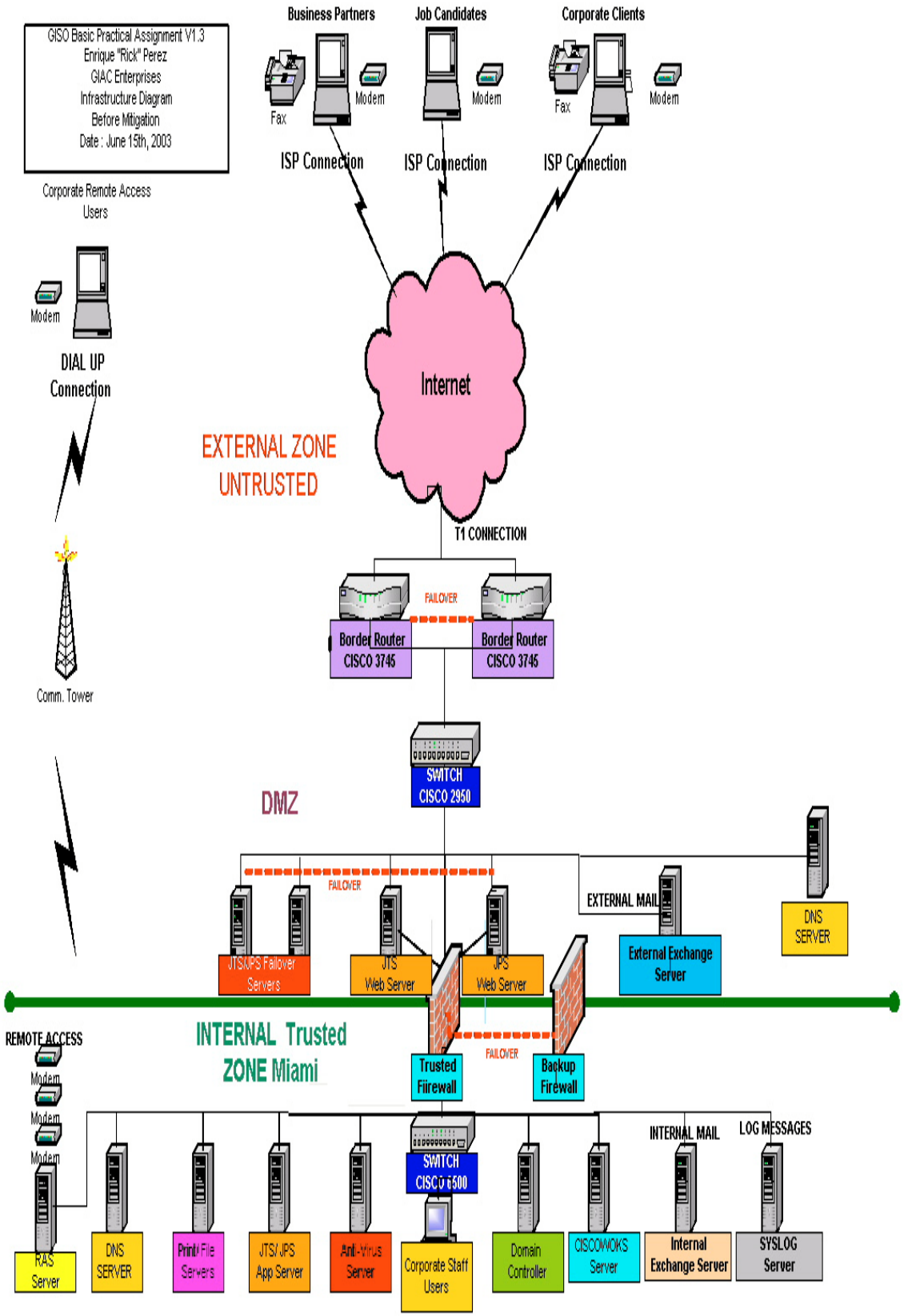


Figure 1. Network Diagram before Remediation

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Business Operations

GIAC Enterprises is an IT professional recruiting services organization. We pride ourselves on the ability of our senior staff to find quality prospects in the IT industry for permanent placement at medium to large scale U.S. based organizations. The GIAC Recruiting Team is composed of a well balanced professional staff with experience in diversified areas of IT and corporate staffing. Our offices are located down town in the 17th floor of an Office Complex known as the "e-mall". Access to the building has 24X7 surveillance, including non-working days. Access to offices in our floor requires the use of a security badge that when used logs the time of entrance and departure. The corporate servers are housed in a secured room with the same control mechanism; however, only System Administrators and Computer Operations personnel are allowed access. Vendors must be given a temporary badge to access facilities and must be accompanied by an employee at all times. Due to the "high risk" of a Hurricane in the South Florida area, we have established a Disaster Recovery Strategy with one of our Business Partners to be able to resume operations in less than 48 hours.

Our main source of revenue derives from "GIAC Total Solution" engagements with large organizations. This product provides companies with a solution that is competitively priced based on the company's total number of IT employees and turnover ratio. Our bread and butter vehicles to conduct our business are two web-based applications. The Job Tracking System (JTS) and the Job Placement System (JPS) run in their individual Windows 2000 Box with a two way trust relationship between them. The web servers communicate through an encrypted tunnel to the JTS/JPS application servers which house the "crown jewels" of the kingdom, These applications provide all of the necessary functions to our users and staff to conduct core business transactions. Some of these functions, but not limited, to are:

- Establishment of Profiles for:
  - Job Candidates
  - Business Partners
  - Corporate Clients
- Entry of Job Requisitions by Corporate Clients and Business Partners for:
  - Project Managers
  - System Analysts
  - Application Developers, etc.
- Entry of Job Candidates Resumes
  - Personal Information
  - Skills
  - Work Record
  - Academic Record
  - Certifications
  - References
  - Hobbies

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

- Online “real time” searches for:
    - Potential Matching Positions
    - Potential Matching Candidates

We have four different types of users accessing the different components of our network:

Job Candidates, who connect into the Job Tracking System (JTS) through their personal ISP connection. They authenticate through a user id and password that is established during their initial visit to our web site. Job Candidates are permitted to look for openings that have been entered by Business Partners and Corporate Clients into the Job Placement Data Base. The search can be conducted by a job candidate by supplying the following information in the “Search Page”:

- Industry
- Region
- Position Description
- Salary Range
- Skills, etc.

Potential matches are displayed to job candidates with summarized job posting information obtained from the Job Placement Data Base. At this point, job candidates will determine if they want to apply or not. In the event they apply, an E-MAILI is sent by the application to the Corporate Client or Business Partner with the complete Job Candidate’s information except “contact data”. If the Corporate Client or Business Partner is interested in this candidate, then they can contact our Senior Account Executive handling this account to negotiate terms of the placement.

Corporate Clients and Business Partners**,** who log into our websites through their ISP connection and authenticate using their user and password established by GIAC Administrators. They use the Job Placement System (JPS) application to enter job postings and look for potential job candidates from our Job Tracking System (JTS) Data Base. Clients that have pre-approved relationships with GIAC Executive Management on placement fees can contact job candidates directly, while others must contact the Senior Account Executive handling the account. These companies are also allowed to send in requirements via a FAX or E-MAIL in the event web application is not available. E-MAIL/Faxed documents are data entered by our corporate staff into the Job Placement System (JPS) application.

GIAC Corporate Staff, who access the web applications, LAN applications and E-MAIL through the corporate LAN. They authenticate via an established user id and password assigned to them by Information Systems. Once authenticated to the LAN, they must go through a second level of authentication when accessing the Job Placement System (JPS) and Job Tracking System (JTS) web

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

applications. They are required to go into these applications to perform data entry, data base queries in a "super user mode". GIAC corporate positions under this classification are:

- Recruiting Staff
- Information Systems
- Sales and Marketing Staff
- Human Resources Staff
- Executive Management

All GIAC Corporate staff has remote access dial up capability through RAS in order to be able to access LAN applications and corporate E-MAIL. Remote access through dial-up to Job Tracking System (JTS) and Job Placement System is not permitted. Access from remote to these web applications must be done using their ISP connection and then authenticating as "super users" at the web site.

ASSIGNMENT # 2

This section of the document will identify the three most critical areas of risk for GIAC that could be compromised by an "intrusion" or "attack" taking into consideration the impact to the organization from a quantitative and qualitative perspective. The section will outline the following:

- The Risk
- The Contributing Factors to the Risk
- Why Protection is Needed
- Potential Business Impact
- Mitigating Steps
- Best Practices that should be implemented **(Extra Credit)**

It should be noted that the mitigating steps implemented to address one risk area, could also serve the purpose of mitigating other risk areas. In addition, It is strongly recommended that in order to effectively implement these security measures, policies and best practices, that ***the implementation of an Information Security Office be adopted***. The responsibilities of this group will be to conduct the following at the minimum:

- Information Security Assessments
- Intrusion, Detection and Response
- Incident Investigations
- Policies and Procedures Definition
- Vulnerability Analysis
- Virus Detection, Containment and Eradication
- Security Patch Detection and Distribution to Information Systems

The Information Security Office (ISO) should adopt an industry proven security standard, such as, ISO 17799 along with security policies that are consistent with those standards.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Risk #1 :

"Confidential" information incorrectly classified as "public" regarding Job Candidates, Corporate Clients and Business Partners may be compromised due to inadequate protection and weak access controls. This data is stored in our Job Tracking System and Job Placement System Data Bases or better refer to as the "crown jewels".

Risk #1/ Contributing Factors:

1. ***Incorrect classification of "Confidential" data as "public" due to lack of training of Information Stewards*** in classifying, handling, protecting and disposing of corporate information
2. ***Inadequate level of protection*** of Job Placement and Job Tracking Data Base to protect information from external and internal access. "Confidential" information must be protected by at least two firewalls from the External Un-trusted Zone and requires strong factor authentication to allow access as per Risk Management Guidelines.
3. ***Lack of an Audit Function or Internal Compliance Group*** to conduct risk assessments on a periodic basis of critical business operations that would reveal areas of exposure, such as this one.
4. ***Lack of a Data Base Scanning Tool*** to detect vulnerabilities within the data base environment does not allow us to implement security measures to address these weaknesses and make our environments more robust.
5. ***Lack of segregation of environments*** in the current configuration does not allow us to isolate the database for proper protection. In the current configuration the Oracle Data Base instance shares a server with the Application and makes the data base more vulnerable to attacks at an application layer.

Risk #1 / Why?

There is a high risk of "intruders" getting unauthorized access to confidential information stored in our databases in order to jeopardize the credibility of our firm. We must protect from members of the "Black Hat Community" that make a living out selling information to competitors and can even hold us "ransom" in order to preserve the confidentiality of our own data. We can not afford to have work records, academic credentials, salary requirements, job skills, geographic preferences altered in a Job Candidate profile or a Job Posting. This may result in an electronic notification being sent to a Corporate Client with a Job Candidate that does not remotely match the original job opening or vice-versa. In another scenario, an "intruder" that has penetrated our data base environment might switch the E-MAIL addresses of *Corporate Profiles*, so resumes intended to be distributed to match the postings of one company are sent to another. This would create a great deal of confusion within the operation and our Corporate Clients.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Risk # 1/ Potential Business Impact:

The information stored in our Job Tracking System and Job Placement System Data Bases are by far the most critical asset within our operation. Confidentiality and trust are the foundation to the success of our business. The disclosure of client's sensitive information to the public or competitors or lack of integrity of this data may cause one or all of the following:

- Loss of trust from Job Candidates, Corporate Clients and Business Partners
- Loss of current and future job placements
- Loss of current and future outsource engagements
- Loss of additional capital required to perform damage control
- Loss of credibility within the IT Recruiting Industry
- Loss of morale within the organization
- Loss of good corporate team members
- Even, the possible dissolution of GIAC Enterprises

Risk #1 / Mitigating Steps

Risk # 1 / Mitigating Step #1

Properly classified information stored in Job Placement System and Job Tracking Data Bases as "Confidential", so it can be adequately protected as per Risk Management Policy.

Risk #1 / Mitigating Step #2

Conduct training classes for GIAC Information Stewards to be given by Subject Matter Experts in the area of Information Classification and Protection. This training should also address in detail the roles and responsibilities of an Information Steward and what techniques should be used to determine the proper classification of information, how to handle it, how to store it, how to transmitted and finally how to properly discard of it. When training is completed, all Information Stewards will be required to re-evaluate classification of assets under their responsibility.

Risk # 1 / Mitigating Step #3

Implementation of *Data Base Scanner 4.1 Engine* from Internet Security Systems.The implementation of this scanning tool will allow us to perform a scan to detect data base vulnerabilities, such as, stale logins, check the strength on passwords, detect potential attacks on logins and it will allow us to enforce Data Base security policy established by GIAC. In addition, it will allow us to perform a comprehensive analysis of our data base defenses from an "external attack" by performing a *Penetration Test*. Data base Scanner will be installed on a Microsoft SQL Server 8.0 running Windows 2000. The server will be hardened by removing excess services and all unused ports will be closed or disabled. In addition, all outstanding security patches and latest service packs will be installed.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Risk# 1 / Mitigating Step #4

Implementation of a Data Base Zone Environment within the Internal Trusted Zone protected by a Checkpoint 1 Firewall. This will add one more layer of protection to the "crown jewels" in support of our "defense in depth" approach. This firewall will only allow bi-directional SQL traffic through port 1521 for the application interface with Application Server. Users requiring access to these databases must strongly authenticate as indicated in Mitigating Step # 5 which follows. Checkpoint 1 Firewall will be hardened by removing excess services and all unused ports will be closed or disabled. In addition, all outstanding security patches and latest service packs will be installed.

Risk# 1 / Mitigating Step #5

Implementation of Axent's Defender Security Server (DSS) working in conjunction with a Radius Authentication Server to provide Strong 2 Factor Authentication at new Checkpoint 1 Firewall. Authentication will take place through the use of a Defender Token requiring a PIN # for activation. All users requiring access to "new' Data Base Server must use this hardware token to generate a one-time password for access. The Radius and DSS Servers are installed in a common Windows NT 4.0 server with Microsoft SQL Server 7 installed for Defender. The server will be hardened by removing excess services and all unused ports will be closed or disabled. In addition, all outstanding security patches and latest service packs will be installed.

Risk # 1 / Mitigating Step #6

Implementation of a dedicated server to house Job Tracking System and Job Placement System databases to separate the data base environment from the Application objects. The isolation of our "crown jewels" into this dedicated data base server will allow us to implement other security measures to effectively protect the "crown jewels". The server will be hardened by removing excess services and all unused ports will be closed or disabled. In addition, all outstanding security patches and latest service packs will be installed.

Risk # 1 / Mitigating Step #7

Implementation of an Audit Function within the organization that will perform at the least yearly reviews of critical operational areas. This group will identify deviations from operational policies and identify areas where there might vulnerabilities or exposures that need to be addressed by Information or System Steward.

Risk #1/ Best Practices

Refer to "Recommended Best Practices". Appendix G.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Risk #2:

The business need to heavily use Internet Mail to communicate with clients and allow our web sites to be readily available to the general public represents a major risk to the stability of these applications. The risk exacerbates due to the fact the only filtering taking place at this time is being done by Border Routers, thus making all DMZ servers susceptible to external attacks in the form of Viruses, Worms, Trojans. DDoS, etc.

Risk #2 / Contributing Factors:

1. The large number of vulnerabilities associated to Microsoft IIS Servers and Exchange Servers, make them very attractive to the "evil doers" of the Internet. Most exploited vulnerabilities of IIS servers are failure to handle unanticipated requests, buffer overflows and the widespread exploitation of Sample Applications. In the case of Exchange Servers the exploitation is well diversified resulting in SPAM, DDoS and introduction of malicious code and viruses via disguised attachments. It should be noted that the vulnerabilities associated to our web servers are inherited by the application servers via application interface connection through port 443 and 80 in "Trusted Firewall".
2. The lack of a firewall appliance with stateful inspection to protect servers in the DMZ will not allow us to block most common attacks at the network layer coming externally through the Internet.
3. The lack of a "complimentary" appliance to inspect traffic coming through port 80 and 443 does not fully provide a safe heaven to our web site applications as most recent attacks are coming through the application layer.
4. The development of the Job Tracking System and Job Placement System web applications was done "in house" under a very tight deadline and without the benefit of *Web Application Standards* in place to assist developers in generating security proven code. In addition, these applications have not undergone a Security Assessment to identify potential vulnerabilities and application deficiencies.
5. There are no tools in place to conduct "content filtering" at the Mail Gateway to prevent SPAM and potentially harmful E-MAIL communications
6. There is no virus detection agent deployed at the Mail Gateway to prevent the introduction of viruses into our Exchange Servers.

Risk #2 / Why?

The reliability of our web portals complimented by the use of E-MAIL is indispensable to our success. A business disruption in this part of the operation would result in substantial revenue loss; as our Corporate Clients, Business Partners and Job Candidates could not interface timely and efficiently with our operational folks. Communications would be limited to faxes and phone calls and in the professional recruiting business, this would not suffice.

Risk #2/ Potential Business Impact:

The inability of our clients to be able to communicate interactively with our folks through our web portals and E-MAIL will result in one or all of the following:

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

- Loss of Job Candidates
- Loss of Business Partners
- Loss of Corporate Clients
- Loss of credibility with the IT Recruiting Industry
- Loss of current and future revenue opportunities
- Loss of capital required to resume normal operation
- Loss of productivity by having to work through FAX and Phone
- Low employee moral
- Possible employee turnover

Risk #2 / Mitigating Steps

Risk # 2 / Mitigating Step #1

Hardened "ALL" Servers and Verify Maintenance has been performed:

1. Verify the latest service packs are installed.
2. Verify all outstanding security patches have been installed.
3. Verify all unnecessary services have been removed or disabled.
4. Verify all unused ports are closed or disabled.
5. Verify all "Sample Applications" and "Web Administration Tools" have been removed.
6. Un-map unnecessary ISAPI Extensions with the use of the IIS Lockdown wizard.
7. Ensure WEB Root is kept clean by removing hidden directories and that the server only stores content needed.
8. Analyze "link structure" to remove unnecessary links from public access
9. Verify default passwords on servers is not used
10. Verify all administrator or root accounts have been given strong passwords according to GIAC policy.

Risk# 2 / Mitigating Step #2

Implementation of a Perimeter Firewall from Borderware to protect DMZ servers from external attacks, un-authorized access and potential malicious traffic such as worms, Trojans and Viruses. The firewall will work in conjunction with existing Border Routers to provide a strong hold at the perimeter. Prior to bringing the appliance online the following security procedures will be applied:

- The OS of the firewall will be harden by removing all unnecessary services that might be abused by an intruder
- Outstanding operating system security patches will be applied to firewall
- A baseline of the firewall configuration will take place to monitor any changes in a periodic basis

Risk # 2 / Mitigating Step #3

Implementation of Symantec Norton ANTI-VIRUS 2003 software in DMZ Servers and Mail Gateway to prevent the contamination and propagation of new viruses introduced in the Internet constantly. This compliments the existing deployment

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

of NORTON throughout all laptops, workstations and servers located inside the *Internal Trusted Zone.*

Risk # 2 / Mitigating Step #4

Implementation of N Circle IP 360 Network Vulnerability Analysis and Intrusion Detection Engine. The strategic deployment of Device Profilers and Traffic Monitors in the DMZ, Internal Switch and at the Mail Gateway will detect potential intrusions. In addition, this tool will identify vulnerabilities for devices located within those subnets. This *intrusion detection tool* in conjunction with our Perimeter Firewall functions as our earliest detection point of un-authorized access in our "Defense In-Depth Strategy".

Risk # 2 / Mitigating Step #5

Implementation of ISS REAL SECURE 5.0 Host Intrusion Detection Engine in ALL SERVERS. This Signature Base Engine will detect possible intrusions that have penetrated our Firewalls and Network Intrusion Detection Engines. This is our last line of defense along with the anti-virus deployment in all servers, workstations and desktops.

Risk # 2 / Mitigating Step #6

Implementation of TEROS-100 APS Appliance in the Web Servers to provide real-time proactive detection and prevention of the following malicious attacks:

- HTML Denial Of Service Attacks
- SQL Injection Attacks
- Command Injection
- Cookie Tampering
- Buffer Overflows Exploits
- Session Hijacking
- Impersonations
- Credential Tampering, etc.

TEROS-100 APS will analyze the contents of HTTP/HTTPs bi-directional packets going through the web servers and drop the malicious ones before they can reach our application servers. The TEROS-100 APS solution becomes more efficient as time goes on as it learns in HTML Interaction Mode what type of traffic should flow between Web Browser, Web Server and Web Application.

Risk # 2 / Mitigating Step #7

Conduct an Information Security Assessment of existing Job Placement System and Job Tracking System web applications **.** This assessment should use as foundation the Development Standards recommended by Information Security Office. The assessment should key on the application vulnerabilities (CVE's) identified by N Circle IP 360 and others documented by industry wide security associations like SANS and SEI Institutes. In addition, this information security assessment process should be incorporated in the organization as standard

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

process to be repeated any time there is significant change to applications or infrastructure.

Risk # 2 / Mitigating Step #8

Implementation of CipherTrust IRON MAIL for safeguarding our Exchange Servers. This appliance sits between the Perimeter Firewall and the Exchange Server to ensure all outgoing and incoming mail connections travels through it. It identifies and stops, SPAM, Viruses and E-MAIL attacks before they reach our Exchange Servers. This preserves the integrity of our E-MAIL application and prevents possible "traffic jams" at the gateway.

Risk #2/ Best Practices

Refer to "Recommended Best Practices". Appendix H.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Risk #3:

Abuse by employees of company-wide access to the Internet through GIAC's ISP connection for the purposes of conducting illegal or un-ethical activities. Some of these activities, but not limited to are, gambling, prostitution, espionage, acquisition or distribution of copyrighted material, sharing political, religious and racial opinions in public forums, disclosure of corporate sensitive information and possibly launching Distributed Denial of Service Attacks (DDoS) on other Corporate Networks from our own internal network.

Risk #3/ Contributing Factors:

1. Access given to all employees with disregard to business function being performed.
2. Lack of user authentication and session logging at the firewall for sessions going out to the Internet.
3. Lack of Web Content Filtering Tool at the Firewall to prevent access to sites that violate GIAC Policy.
4. Lack of a Web Usage Monitoring Tool to track daily usage by employee.
5. Lack of Internet Usage Policy that clearly states the permitted activities and what disciplinary actions may be taken for non-compliance.

Risk #3 / Why?

Even though, GIAC Enterprises makes the Internet the "Life Line" to our existence. As such, we must ensure that the use of this vehicle within our organization is done with the utmost level of professionalism and ethics. We have a well diverse group of employees of different race, religion and political affiliations that must understand that expressing personal views through our corporate ISP connection is not permitted. In addition, they must be fully aware that violation of security policy with regards to unethical or illegal use of the Internet will be of "0 TOLERANCE".

Risk #3/ Potential Business Impact:

Our most important asset is the integrity of our people and the trust our Job Candidates, Business Partners and Corporate Clients place on them. Breaking that trust as stated previously in this document would have a serious impact in our ability to continue to function at peak level. Illegal or Un-ethical activities associated with an Internet user carrying the @GIAC.COM would put our firm in that undesirable position. As important to the potential loss of trust is the strong possibility of legal actions against our organization for not properly preventing this behavior. For potential business impacts in more detail, please refer to the same section under Risk #2 and #3.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Risk #3 / Mitigating Steps

Risk # 3 / Mitigating Step #1

Implementation of security policy with regards to the illegal or un-ethical use of the Internet through the use of company-owned resources. In order to ensure compliance, a mandatory *Awareness Training Session* for all employees should be conducted by the Information Security Office. All employees must sign an acknowledgement that they have received the training on the policy and fully understand its content.

Risk # 3 / Mitigating Step #2

Implementation of Surf Control Web Filter from Surf Control Corp at the Perimeter Firewall to monitor Internet navigation and usage. This tool will help us employ intelligent, policy-driven technology to help manage the content coming in and out of our network. Security Alerts will be automatically sent to Information Security Office for possible investigations. Management Reports will be generated periodically to identify usage by GIAC categories defined, for specific individuals, time of day, etc. These reports will be distributed to employee's direct manager.

Risk # 3 / Mitigating Step #3

Implementation of Approval Process to grant Internet access to employees based on their job functions. Approval is to be obtained at Director Level. This process must be put in effect immediately to determine the validity of access already granted.

Risk # 3 / Mitigating Step #4

Establish user authentication through a user id and password at the Perimeter Firewall in conjunction to enabling *logging* to have the capability of reviewing session activity of users that are suspected of conducting unauthorized or illicit activities over the Internet.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Assignment #3
Evaluate Security Policy

Associated Risk :
Confidential information incorrectly classified as "public" regarding Job Candidates, Corporate Clients and Business Partners may be compromised due to inadequate protection and weak access controls. This data is stored in our Job Tracking System and Job Placement System Data Bases or better refer to as the "crown jewels".

Policy obtained from :
Own Organization's 10 Key Control Policies

Policy Location:
Appendix F

Purpose:
The policy states very clearly in the first statement the intent of the policy, which is to properly classify information according to sensitivity in order to protect it accordingly. It also identifies what characteristics of this data are to be protected, such as, integrity, confidentiality and reliability.

Scope:
In this area, the policy provides good examples of what type of corporate documents or data stores would fall under the policy. It defines the four different types of information classification and the associated control components. However, it does not define clearly if this policy only applies to GIAC employees or if it also applies to Business Partners, Corporate Clients and 3rd party contractors.

Background:
This policy does not provide any background information regarding Information Classification. The importance and need of this policy does not really warrant the need to do so.

Policy Statement:
The policy is adequately structured in communicating the classification of information as it addresses what type of corporate information needs classification, what classifications they would fall under taking into consideration the value to us and others, who are the parties that could be impacted and where the responsibilities lie to properly label it, handle it and protect it.

Action:
There are three distinct actions that are invoked by the policy. "Classification and Labeling" by the Information Steward at document creation, "Access, Handling

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

and Disclosure" and "Protection" that should be exercised by all Employees, Business Partners, Corporate Clients and contracted 3rd parties.

Summary:

There are four areas that I feel the policy could be enhanced. The first area is associated with the definition *of GIAC Secret vs. GIAC Confidential*. I do not see a clear demarcation between the two. In this event, I would add additional characteristics that would allow the reader to clearly differentiate between the two, maybe even include a couple of examples for the sake of clarity.

The second area that I feel falls short is under the *Control Components*, as surprisingly the *disposal* of the information is not addressed. This control is paramount to preserve the spirit and effectiveness of this policy. The well known practice of "dumpster diving" by the *Black Hats* can turn our *trash into their cash* as corporate sensitive information is usually sold to the highest bidder. The policy should address this control and identify what methods should be used depending on the classification given.

The third area, addresses the need to have *consistency in the terminology* used. The policy states that "Classification and Labeling" is up to the Information Steward. However, under "protection" the responsibility is given to the "Business Unit Standard". Who sets the standard for a Business Unit? The Information Steward. So; in this scenario, I would refer to the Information Steward.

Last, and most dangerous is the default classification as "public" of a document or entity that has not been labeled. I would strongly recommend that these kind of documents default to "Internal Use Only". This would be a more conservative approach in order to prevent public disclosure of what could be sensitive information.

As a general comment, the policy adheres to the principles of security as far as information stewardship. However, it is not very practical to have all information classified by Information Steward as he/she is not readily available to classify every document originated daily within GIAC Enterprises. I recommend the development of a well-defined matrix maintained by Information Custodians that can be used by Employees, Business Partners, Corporate Clients and 3rd Party Vendors as a reference. This would allow originators to classify the limited documents such as memos, e-mails, reports, etc., but would also allow Information Stewards to classify sensitive documents that would carry significant risk, such as, contracts, external financial reports, commercial web content, data base repositories, etc.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Revised Policy:

Title: Information Classification Policy

Version: 1.0

Last Revision on: June 30th, 2003

Purpose and Background:
The purpose of this policy is to establish the need to classify GIAC corporate information in order to provide proper protection while it is stored or "at rest" and while it is being transmitted or "in motion". Recent industry regulations call for penalties in the event job candidates private information is divulged using our repository as seed. It is important all staff members properly understand the importance of properly classifying or labeling information so it can be handled, protected and dispose of, accordingly.

Scope:
This policy applies to al GIAC Employees, Business Partners. Corporate Clients and any other GIAC contracted party creating, handling, protecting or disposing of corporate information. Corporate information is considered as "data" stored or transmitted in one of the following medias; Paper, disk, CD, diskette, e-mail, instant message, voice recording, video tape, video conference, fax, telephone and even conversations.

Responsibility:
1. The Information Security Office is responsible for the implementation of this policy and must ensure the following:
    a. The information classification policy is updated on a regular basis, published as appropriate and accessible by everyone
    b. Appropriate training is provided to Information Stewards and Information Custodians so they can train the rest of the staff
    c. Security Procedures are in place and updated in support of this policy
2. The Information Steward is responsible for classification of all corporate data under their business unit
3. The Information Steward is responsible for authorizing Secret, Confidential and Internal Use only information for disclosure and disposal.
4. Corporate Communications must clear all information that is classify as public by Information Steward

Policy Statement:
All information should be reviewed by Information Stewards on a periodic basis and classified according to its use, sensitivity, and importance. We have the following four categories:

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

GIAC Secret:
This classification applies to the most sensitive business information to be shared and discussed among GIAC's Executive Level Management. Executive Level Management is considered to be Director level and above. *Its unauthorized disclosure will cause seriously and adversely impact to GIAC's credibility and ability to operate*. An example, of this type of information would be the development of a new product offering or the preliminary distribution of a Financial Statement, etc.

GIAC Confidential:
This classification applies to less sensitive business information which is intended to be shared among all GIAC Employees on a "need to know basis". *Its unauthorized disclosure may adversely impact GIAC, its employees, clients and business partners.* An example of this type of information might be, the information collected by Application Server Logs, Job Request submitted by a Corporate Client, Business Partner Agreement of placement fees, etc.

GIAC Internal Use Only:
This classification applies to all other non-public information which does not clearly fit into the above two classifications. While its unauthorized disclosure is against policy, it is not expected to seriously and adversely impact GIAC, its Employees, Clients and Business Partners. Information under this category could be the internal phone book, Global e-mail address book, internal job postings, etc. *Information that is not labeled will default to this category.*

GIAC Public:
This classification applies to information which has been categorized by Information Steward as such and approved by GIAC's Corporate Communications for release to the public. By definition, there is no such thing as unauthorized disclosure of this information and it may be freely disseminated without potential harm.

This section of the policy defines the *controls* that must be applied to a classified artifact.

Classification and Labeling:
Classification and labeling is performed by document originator upon the creation of any corporate information in accordance with "Information Classification Matrix". This matrix is stored in the Corporate Intranet and maintained by Information Stewards. If the document does not fall within the categories defined in the matrix, originator must seek classification from Information Custodian. The classification is determined based upon the classification categories referenced above. When assigning the appropriate classification, due care must be taken. If a higher than necessary classification is placed on information, it may restrict its use causing staff frustration and undue expense. If information is classified too low, the disclosure could damage GIAC, its employees, clients and business partners.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Access, Handling and Disclosure:
There is no special handling required for Public Information*. Secret, Confidential and Internal use Only information must:*
1. Not be read, discussed or otherwise exposed on public places
2. Not be discussed over open telephone lines
3. Not be left in voice mail recordings
4. Not be shipped via Regular Mail
5. Not be transmitted in clear text

Protection:
There is no special protection required for Public Information*. Secret, Confidential and Internal use Only information must:*
1. be encrypted during transmissions and while it is stored.
2. be shipped by mail service approved by Information Security Office
3. be at least password protected to obtain read access. For the purpose of update, *strong factor authentication* should be in place
4. be approved by Information Steward before it is placed in public web site
5. be transported physically in a locked container and never left unattended

Disposal:
The disposal of information once its use and retention period has been completed is the final control component in the data life-cycle:

1. Secret , Confidential and Internal Use Only information that is stored in paper requires disposal through a "paper shredder" or specially labeled locked trash cans labeled "Information Security Office" throughout the building. If stored on magnetic media, it must be deleted with a software tool approved by Information Security Office that performs "electronic shredding".

2. Permission to dispose of Secret, Confidential and Internal Use Only information requires approval of the Information Steward.

3. There is no special disposal requirements imposed on Public Information.

Action:
1. Data Classification Matrix must be developed by Information Stewards
2. Information Security Office must identify software used to perform "electronic shredding"
3. Information Security Office must identify "Mail Service" to be used for protecting data
4. Information Security Office must deployed Locked Trash Cans throughout the building to dispose properly of Secret, Confidential and Internal Use Only information
5. This policy goes into effect immediately.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Assignment 4

Develop Security Procedures

The following procedure outlines the steps required to conduct an Information Security Assessment by the Information Security Office (ISO) on a new project or on an existing Application or Business Function. The procedure details the forms that are part of the Information Security Assessment Life Cycle from original "Request" to "Final Assessment" phase.

Information Security Assessment Procedure

Purpose:

The purpose of this procedure is to make sure all GIAC personnel is aware of the Information Security Assessment Life Cycle. When to request one, how to request one, understand the different phases of the process, what forms should be used, the approvals needed and what are the responsibilities and deliverables expected from each party involved. It should be noted that the procedure makes reference to a customized *Discovery Questionnaire* and *Technical Security Requirements*. These documents are very extensive to include as part of the Appendix. However, they address the following information:

Discovery Questionnaire:

- Asset Classification
- Business Continuity
- Compliance
- Computer and Network Management
- Information Security
- Organization and Management
- Personnel Security
- Physical Security
- System Access
- System Development and Maintenance

Technical Security Requirements:

- Data Delivery Security Requirements
- Firewall Security Requirements
- Database Security Requirements
- Network Security Zone Authentication Requirements
- NT Server Security Requirements
- Open Systems Application Design Security Requirements
- Remote Access VPN Security Requirements
- Router Security Requirements
- UNIX Security Requirements
- Web Application Security Requirements

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Importance to the Organization:
This process serves as the *checkpoint* to existing Business Functions or new projects on how well they conform to the established organization security policies and technical security requirements. The final deliverable from the Information Security Office will be a list of *findings* identifying areas of non-compliance that might put the organization at risk. Each finding must be addressed by the Project Manager or Information Steward by identifying *Mitigation Steps* or by requesting for an "exception" due to special business or technical circumstances.

Responsibility:
It is the responsibility of the Information Security Office to provide training and awareness to the entire organization of the importance of following established security policies. In addition, the office must clearly define when a Security Assessment is needed and what process to follow to request one. It is the responsibility of the Project Managers and System Stewards to request the assessment on a timely fashion, provide the necessary documentation to the Information Security Office to conduct the assessment and to respond to the findings identified by the Information Security Office accordingly.

When is an Information Security Assessment Required?:
A Security Assessment and signoff must be performed by the Information Security Office in order to:

1. Ensure security of the GIAC system infrastructure
2. Maintain compliance with GIAC Policies and Procedures.
3. Evaluate any new connections that are plan to be made to the GIAC network, regardless of whether the project is a development activity; pilot project; or production implementation and will always be required in the event of:

    a. A major technical infrastructure change, including new technology or major upgrades for major existing technology components;
    b. The addition or change of a service, product or application to the GIAC processing environment; and
    c. Development work or processing is outsourced which requires connectivity to the GIAC network; or which requires transfer of GIAC Secret or GIAC Confidential information.

The Procedure:

Request Phase:

1. Project Manager/System Steward submits an E-MAIL communication to Information Security Office at (ISO@GIAC.COM). The e-mail must attach an Information Security Assessment Request Form (Appendix A).

2. Information Security Office receives request and assigns Information Security Analyst and a CNTL# for internal management.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Statement of Work Phase:

1. Information Security Analyst contacts Project Manager/ System Steward via e-mail or phone to schedule a meeting.

2. Security Assessment Meeting takes place between ISO Security Analyst and Project Manager/System Steward to discuss in more detail some of the following topics that are applicable to the project:
   - Review of Assessment Process
   - Project Team Composition
   - Project Overview
   - Review Data Classification
   - Review Data Storage Protection Requirements
   - Review Data Transmission Protection Requirements
   - Review Data Flow To/From and within our Private Network
   - Review Network Connectivity Proposed
   - Review Data Base Environments (Access Control/ Data Sensitivity)
   - Review involvement from 3rd Parties
   - Review Any Emerging Technologies to be used

   As result of the meeting, the following should be agreed upon as part of the meeting minutes:
   - Projected Timelines and Associated Deliverables
   - Estimated Effort from Information Security
   - Change Control Process
3. Information Security Office puts together a Statement of Work (Appendix B) And submits it via E-MAIL to Project Manager/System Steward for approval.

Discovery Phase:

1. Once Statement of Work (SOW) has been approved by Project Manager/System Steward, The *Discovery Phase* begins. In this phase, the Information Security Analyst will develop a customized Discovery Questionnaire based on the nature of the project and how it complies to the organization's security policies. In addition, the Information Security Analyst will identify the appropriate Technical Security Requirements that apply depending on the project technical specifications.

2. The Discovery Questionnaire and Technical Security Requirements are sent by Information Security Analyst via e-mail to Project Manager/System Steward no longer than two weeks after approval of SOW.

3. Project Manager/System Steward shares information with his/her team to gather responses to the Discovery Questionnaire and to determine if they adhere to the Technical Security Requirements.

4. Project Manager/System Steward completes Questionnaire within three weeks of receipt. Completed Discovery Questionnaire is sent to Information Security Office via E-MAIL. In addition, Project Manager/System Steward

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

documents any Technical Security Requirement that might not be met. This is the birth of The "Information Security Assessment Issues List" (Appendix C).

Assessment Phase

1. Having received the completed Discovery Questionnaire, the *Assessment Phase* begins. In this phase, the Information Security Analyst reviews the responses given by the project team and looks for areas of non-compliance against policy or Technical Security Requirements. Analyst compiles all non-compliance items onto the "Information Security Assessment Issues List" (Appendix C) and recommends means to mitigate issue.

2. At this point, a meeting is called between ISO Security Analyst and Project Manager/System Steward to review each issue identified as to not being compliant to security policy or technical security requirements.

3. Project Team is given two weeks to determine if they will seek mitigation to be compliant or will submit a "Compliance Exception Request Form" (Appendix E) stating special circumstances. This determination is sent via e-mail to Information Security Office

4. Information Security Office generates Final Assessment Report (Appendix D) identifying all findings and what determination was taken, to mitigate or file for exception. Final Assessment Report is sent to CSO.

Compliance Phase:

In order to ensure that all *new projects* undergo an Information Security Assessment, the Information Security Office gets a notification from the Project Management Office (PMO) of approved projects. This initiates the dialog between the Project Team and the Information Security Office. In addition, the *project initiation kernel* used by all new projects contains a step to contact the Information Security Office and a "Control Gate" that requires approval from one of its members.

In the event, an Information Security Assessment is performed upon a Business Unit or Function. These type of requests are initiated by the Business Unit's Director to the Corporate Security Officer, this way the Information Security Office is aware from the start.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

APPENDIX

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Appendix A

Security Assessment Request Form

Use this form to request an Information Security Assessment for your project.

Requester Information

Requestor:		**Phone:**	
Request Date::		**Dept:**	

Project or Application Description:

1) Please provide the following:

Project Name:		**CNTL #:**	
Install Date*:		**Business Unit:**	
Sponsoring Dept:		**Director:**	

* If not known, please provide the estimated month or quarter that the implementation might occur.

2) Provide a short description of the project or reference a source for its description:

Form Distribution:

3) Send completed form to ISO@GIAC.COM.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Appendix B

ISO Statement of Work

Date:
Cntl#:
ISO Analyst
Extension:

I. Project Summary

II. Implementation & Development Approach

III. Roles & Responsibilities

IV. Assumptions

V. Estimates

Activity	Description	Person Hours	Total at $	Person Months	Total at $	Total
Request						
Discovery						
Issues Definition						
Assessment						
Total Labor:						
Non-Labor Expenses						
Contingency						
TOTAL COST:						

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Appendix C

ISO Security Assessment Issues List

Project:		**Business Unit:**		**Cntl#:**	
Project Manager:		**Phone:**			
ISO Analyst:		**Phone:**			
Proj. Install		**Assessment Due**			

Introduction:

The goal of a Security Assessment is to resolve design issues and comply with GIAC's Policies, and Procedures. Adherence to these policies and requirements is mandatory without an approved exception.

Issues List:

Each security policy issue and any compensating security measure are listed below:

#	Security Issue Description and Control Policy	Suggested Mitigating Requirement	Owner	Due Date

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Appendix D

ISO Final Information Security Assessment

Project:		**RTN:**		**Cntl #**	
Contact:		**Phone:**			
Analyst:		**Phone:**		**Mail Stop**	
Project Install Date		**Assessment Due Date**			

Compliance Statement:

The current project design does not fully comply with GIAC's Policies and Procedures

Unresolved Policy Exceptions:

Each of the following unresolved policy issues must be resolved or approved as an exception by the Process Management Committee:

No.	Policy Control Reference	Compliance Finding
1		
2		

Best Practice Recommendations:

Best Practice Recommendations appear below:

Final Assessment Approval

Signature (CSO) Print Name Date

Acknowledgement

Signature (Primary Stakeholder) Print Name Date

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Appendix E.

Compliance Exception Request Form

Please complete the *Compliance Exception Request* for each request, ensuring that you have thoroughly described the need for an exception. Submit to Process Management Committee

GENERAL INFORMATION

Completion Date:
Requester's Name:
Requester's Title:
Reporting Manager Group Division: ❒ Account Management ❒ Service Management ❒ Finance ❒ Strategy/New Business Development ❒ Information Controls & Compliance ❒ Systems ❒ Processing
Type of Policy Exception Request: ❒ Compliance Extension Request ❒ Permanent/Ongoing Request
Exception Period Requested (*mm/dd/yyyy format - not to exceed one year*): From:_____ To:_____
Policy for which Exception is requested:
Procedures for which Exception is requested (Multiple listings are allowed):
Provide a high level overview of the Exception Request, and describe the business need for the exception versus the acceptance of the associated risks:

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

JUSTIFICATION

Identify the business reason(s) for the exception (Multiple choices are allowed):

- ❒ Lack of staffing resources
- ❒ Lack of funding
- ❒ Cost exceeds benefits
- ❒ Minimal risk
- ❒ Other compensating controls exist
- ❒ Other. Please describe: _____

Specify the other/compensating controls in place to mitigate/eliminate the risks documented above:

REQUESTER MANAGEMENT APPROVALS

Title	Printed Name	Signature	Date

At a minimum, one Stake Holder must approve this request.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Appendix F

Information Classification Policy

GIAC Corporate information requires classification in order to adequately protect its integrity, confidentiality, and reliability. GIAC-created materials includes files, data base, reports, presentations, emails, memoranda, or other materials created by an individual and used to perform business activities or to support management decision-making.

The Information Classification Policy has two components:

I) Classification categories
II) Control components

The more sensitive the corporate information is classified, the more extensive the control components must be to provide adequate protection.

I) Classification Categories

1. GIAC Secret: This classification applies to the most sensitive business information which is intended for use within GIAC. Its unauthorized disclosure could seriously and adversely impact GIAC, its employees, clients and business partners

2. GIAC Confidential: This classification applies to less sensitive business information which is generally for use within GIAC. Its unauthorized disclosure could adversely impact GIAC, its employees, clients and business partners.

3. GIAC Internal Use Only: This classification applies to all other non-public information which does not clearly fit into the above two classifications. While its unauthorized disclosure is against policy, it is not expected to seriously and adversely impact GIAC, its employees, clients and business partners. The vast majority of GIAC information falls into this category.

4. GIAC Public: This classification applies to information which has been approved by GIAC management for release to the public. By definition, there is no such thing as unauthorized disclosure of this information and it may be freely disseminated without potential harm. Information without a label is by default classified as public.

II) Control Components

a. Classification and Labeling: Classification and labeling is performed by the Information Steward upon the creation of any corporate information. The classification is determined based upon the classification categories referenced above. When assigning the appropriate classification, due care must be taken. If a higher than necessary classification is placed on information, it may restrict its use causing staff frustration and undue

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

expense. If information is classified too low, the disclosure could damage GIAC, its employees, clients and business partners.

b. Access, Handling and Disclosure: This control component is the most critical element of the information classification categories. Major control principles include: the manner in which access is provided to the information, and the distribution process and controls on disclosing the information.

c. Protection: All corporate information in an individual's possession must be protected based upon the individual's business unit standard. The standard must include a certain minimum level of protection that ensures the integrity of information.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Appendix G.

Risk# 1 Best Practices To Be Implemented

1. The Data Base Administrator must ensure that whenever a new user requires access to the Data Base Environment, they are assigned their own account for which they are responsible. A critical step of obtaining a new account must include the signing of an acceptable use policy and confidentiality agreement. This policy and agreement must include, but are not limited to, the following:
    a. the user is responsible for, and will be held accountable for, all actions
    b. performed by the account – therefore, do not give you password to
    c. anyone for any reason
    d. the users actions may be audited and monitored at any time, and
    e. the users access to the system is subject to revocation if misuse has
    f. been determined
2. The Database Administrator must adhere to the policy of not embedding passwords in scripts, stored procedures, or other locations where they may be discovered in clear text. Procedures should be developed to determine if passwords have been embedded in scripts, stored procedures or other locations
3. The Data Base Administrator must adhere to the policy of not creating "Guest" accounts. A periodic review must be performed to ensure that no "Guest" accounts have been set up without the Information Security Office's knowledge
4. The Data Base Administrator must work with Information Security Office to develop a password escrow system for securing highly privileged accounts
5. The Data Base Administrator working closely with the Information Security Office must ensure that any accounts created by a vendor are immediately disabled or removed following completion of their work
6. The Data Base Administrator working closely with the Information Security Office must develop roles for administering the database. Specific roles must be developed for each type of administrator.
7. The Data Base Administrator must ensure that whenever object privileges are assigned, they are not assigned with the "WITH GRANT OPTION". In addition, he/she must perform a periodic review of object privilege assignments.
8. Data Base vulnerabilities identified by a "Scan" and classified as "critical" by the Information Security Office will require a response from the Data Base Administration Group within 48 hours. If a security patch is available for installation, the patch must be installed within 24 hours of distribution. Deviation from these guidelines will require an "exception request" to the Information Security Office. Exceptions not received within these time frames will require escalation to Executive Management.
9. A "Penetration Test" must not be conducted without the approval of Corporate Security Officer. The results of the test must be labeled "secret" with one copy

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

going to the Information Security Office and the other copy furnish to Chief Information Officer.

10. Data Base Environments that are non-compliant with Security Policy will result in a notification from Information Security Office to Information Steward stating area of non-compliance and what is the expected time frame to comply. Information Steward will either concur with the finding or seek an exception from the Information Security Office stating its justification.
11. All configuration changes to all network components must go through a Change Control Process that will ensure segregation of duties and that proper approval is obtained from the Information Security Office.
12. All firewalls will be configured using the principle "TO DENY FIRST, THEN ALLOW " to only allow explicitly identified traffic via rules applied by Firewall Administrator.
13. All firewall logs will be sent to a centralized server to be consolidated with other network component logs. The logs must be reviewed periodically with Information Security Office.
14. All administration requests coming into firewalls must use SSH.
15. All firewalls should have appropriate session timeout values assigned.
16. All firewalls should log any dropped packets.
17. All firewalls without a fail-over mechanism that go offline must deny all traffic to protected zone until appliance is back online
18. Users are responsible for safe handling and storage of all GIAC authentication devices. Defender tokens should not be stored with a computer that will be used to access GIAC's network or system resources. If an authentication device is lost or stolen, the loss must be immediately reported to the Information Security Office
19. The Radius Server must log all successful and failed authentication requests.
20. All requests to add new users or establish new user groups in Radius Server requires the approval of the Information Security Office
21. Radius Servers and DSS Servers must be configured in a fail-over mode.
22. Defender Tokens must be requested from Information System Group with approval of direct supervisor.
23. Information Security Group must maintain an inventory of all tokens distributed and monitor that PIN numbers are changed every six months.
24. Training of Information Stewards and Custodians on Information Classification and Protection must be conducted at least on yearly basis.
25. The Information Steward Role should be complimented by an Information Custodian to expedite the process of classification of data on day to day operations.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Appendix H

Risk # 2 / Best Practices To Be Implemented

1. A *Security Patch Process* must be in place that will identify outstanding security patches not applied to our web servers.
2. A *certified image* approved by Information Security Office must be developed to ensure that all web servers prior to implementation are configured accordingly. In addition, all security patches and service packs would have been applied prior to network deployment.
3. All web servers must be deployed with a *fail-over* configuration in place in order to prevent disruption of service. The Information Systems Group must be notified immediately of a web server failure to determine if a server can be rebooted and assumed the backup roll. Information Security Office must be notified to perform a review of the logs associated with the web server that went offline.
4. *Web Server Logs* must be reviewed periodically with participation from the Information Security Office
5. *Integrity Checking Tools* like TRIPWIRE must be implemented to determine if any configuration changes has been made outside of the change control process. Any discrepancies should be investigated to determine the source of the change and the reason for the change.
6. A common strong *password enforcer engine* must be used by all web servers to protect the confidentiality job candidates establishing accounts online..
7. *GIAC Web Administrators* must maintain an active, enabled and current version of the approved virus screening software installed and diligently updated with the latest "inoculation signatures". This must be accomplished through an automated process to deliver computer virus definition upgrades to all Web Servers on a daily basis.
8. Virus screening must take place on 3rd party vendor software that needs to be integrated into web server applications. As part of the application documentation, a list of 3rd party software should be included along with an indication that each software component was scanned for viruses, how the software was scanned, which virus scanning software was invoked, and an indication that no viruses were found.
9. GIAC web Administrators may not install 3rd party executables in a web server unless it is digitally signed and approved by Information Security Office.
10. If a Web Server is identified as containing VIRUS, it must be taken offline immediately to conduct "forensics" and reconfiguration. This should be accompanied by a system wide scan for detected virus to ensure there has been no propagation. The Information Security Office must lead this effort and provide an "Security Event Report" to the Corporate Security Officer.
11. Potential Network Intrusions identified by N Circle IP 360 must result in an automated notification to Information Security Office for investigation via electronic mail. ISO organization will manage the event to address containment and to perform root cause analysis of this event.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

12. The application of Ontology Rules to N Circle IP 360 must go through a formal change control process in which the Information Security Office is a key member of.
13. Access to N Circle IP 360 Console must only be given to Network Administrators approved by Information Security Office and members of the Information Security Office involved in Incident Response function..
14. Devices over the *maximum vulnerability score* established by the Information Security Office will require a response from device administrator within 48 hours indicating course of action.
15. *Critical Alerts* of vulnerabilities issued by Information Security Office will require a response by device administrators within 48 hours indicating course of action.
16. *Security Patches* associated with a *Critical Alert* must be installed within 24 hours by device administrator.
17. Vulnerabilities not removed via a security patch installation or inability to perform upgrade on Operating System due to technical limitations must be properly documented via the exception process with the Information Security Office.
18. The process to update "attack signatures" must be coordinated between the Vendor, Information Services and Information Security Office.
19. Signature Data Base must have limited access to Administrators and Information Security Office members involved in Incident Response function.
20. Users attempting to log on to a server will be given three attempts to authenticate. Failure to successfully authenticate will be result in user account being disabled.
21. Access to the network servers located in the DMZ or Internal Trusted Zone will be achieved by individual and unique logins, and will require authentication. Authentication includes the use of passwords, smart cards, biometrics, or other recognized forms of authentication.
22. All GIAC Servers residing in DMZ and Internal Trusted Zone must have logging turned on to be able to conduct Log Analysis.
23. Establishment of thresholds to determine the possibility of an attack, such as, volume, type of traffic, sign on attempts, session time, etc. must involved the involvement of Information Security Office and Information Steward.
24. *Development Standards* for web applications must be followed to ensure that good security coding techniques are in place to prevent the most common forms of attack. Some of these techniques are:
    a. Hyperlink Inspection
    b. Prevention of Cookie Tampering
    c. Enforcement of Form Consistency
    d. Prevention of Buffer Overflows
    e. Prevention of Cross Site Scripting
    f. Java Applet Reverse engineering, etc
25. Implementation of Web Applications into production requires that a *security code review* be conducted with involvement of the Information Security Office. Deviations from *Development Standards* require that an Exception Form be

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

filed with the Information Security Office and approved by senior executive management.

26. Critical Web Application Vulnerabilities identified in 3rd party application code must be reported to Information Security Office. This office will send a "Security Vulnerability Notification" to offending 3rd Party requesting a security patch be deployed within the next 90 days.
27. A yearly penetration test with a focus on web exploitation at the application layer must be conducted yearly by an approved 3rd party security service provider approved by the Information Security Office. Information System Group will need to address "vulnerability" according to the level of exposure to the organization.
28. An Information Security Assessment and signoff must be performed by the Information Security Office in order to: 1) ensure security of the GIAC Network Infrastructure; and 2) maintain compliance with the GIAC Security Policies and Procedures. Security Assessments must occur before any new connections are made to the GIAC network, regardless of whether the project is a development activity; pilot project; or production implementation and will always be required in the event of:
    a. A major technical infrastructure change, including new technology or major upgrades for major existing technology components;
    b. The addition or change of a service, product or application to the GIAC processing environment
    c. Development work or processing is outsourced which requires connectivity
29. The Security Assessment findings will disclose any areas of non-compliance and will provide recommended solutions for compliance. These solutions are intended to meet business and operating practices that fulfill corporate responsibility to GIAC. An assessment with findings must be read, signed and returned to the Information Security Office within 10 business days. The corresponding action plan must be submitted to the Information Security Office within 15 business days.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Appendix I

Risk # 3 / Best Practices To Be Implemented

1. Internet connectivity must be approved by requestor's Director and Information Security Office and must be utilized for business purposes. GIAC employees are responsible to exercise due care while accessing the Internet as they are representing GIAC.

2. Employees must not establish connections with Internet Service Providers (ISPs) or other external networks for the transmission of GIAC data unless this arrangement has first been approved by the Information Security Office.

3. Employees may not visit nor download information or programs from inappropriate web sites unless this has first been approved by the Information Security Office. Inappropriate web sites include those that contain unlawful or unlicensed software, may be described as sexually explicit, provide on-line gambling, or provide information that can contribute to unlawful discrimination or harassment on the basis of race, color, sex, sexual orientation, creed, religion, age, marital status, national origin, ancestry, disability, medical condition, or veteran status. Employees who fail to follow this policy are subject to discipline, up to and including discharge.

4. Users are prohibited from establishing any electronic commerce company or organization arrangements over the Internet unless the Information Security Office have first evaluated and approved of such an arrangement. GIAC *Secret, Confidential and Internal Use Only* information must not be sent across the Internet unless it is in encrypted form.

5. Employees who connect to the Internet from home via GIAC-owned laptop computer must do so only through first connecting to the GIAC network via remote access and then connecting to the Internet through a GIAC Internet firewall. Employees must not connect to the Internet from home by any other means.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

References

Teros.
"Protecting Prot 80: Techniques for Eliminating Web Application Vulnerabilities"
URL: http://www.teros.com/registration/register.shtml

Ciphertrust,
"10 Keys to Safeguarding Your E-MAIL Systems"
URL: http://www.ciphertrust.com

CISCO. "SAFE: A Security Blueprint for Enterprise Networks".
URL:
http://www.cisco.com/en/US/netsol/ns110/ns170/ns171/ns128/networking_solutions_package.html

Computer Security Institute.
"2002 CSI/FBI Computer Crime and Security Survey".
URL: http://www.gocsi.com/press/20020407.html

Internet Security Systems. "Data Base Scanner Evaluation Guide", Version 4.1
URL:
http://www.iss.net/products_services/enterprise_protection/vulnerability_assessment/scanner_database.php

SANS. SANS / FBI "Top 20 List".
URL: http://www.sans.org/top20/

Software Engineering Institute. "Deploying Firewalls".
URL: http://www.cert.org/security-improvement/modules/m08.html

Software Engineering Institute," Securing Public Web Servers ".
URL: http://www.cert.org/security-improvement/modules/m11.html

Software Engineering Institute," Securing Desktop Workstations ".
URL: http://www.cert.org/security-improvement/modules/m04.html

Spitzner, Lance. "Auditing your Firewall Setup".
URL:
http://searchnetworking.techtarget.com/originalContent/0,289142,sid7_gci801354,00.html
Search Networking.
March 15th 2001

Author's Organization. "10 Key Control Policies and Procedures Reference Guide", Version 2.7
URL: ***Unable to provide as per Security Policy***
January 31st, 2002

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.