Global Information Assurance Certification Paper

GIAC Mortgage Services
A Full Service Mortgage Company

Practical Assignment
for
SANS Information Security Officer Certification
Version 1.3

-prepared by-

Albert M. Raymond
September 17, 2003

Abstract

GIAC Mortgage Services is based on a subsidiary of an actual Fortune 500 organization. For the purposes of this exercise, most of the GIAC Mortgage infrastructure, process and procedures has been fictionalized. However, the central theme of this paper is to present a complete view of an organization from both a business model perspective and an information technology perspective with the goal of uncovering real-world critical risks within the organization that could jeopardize the integrity of the organization, and then creating a policy and procedures to mitigate the issues.

GIAC Mortgage Services

Section 1 - Executive Summary

GIAC, based in Denver, Colorado, is one of the foremost providers of travel and real estate services in the world with over 8,000 employees in the United States.

GIAC is:

- the world's largest real estate brokerage franchisor;
- one of the largest retail mortgage originators in the U.S.;
- the world's leader in private labeled mortgages for high-profile clients.

GIAC Mortgage is one of the largest retail mortgage lenders nationally: GIAC is a full service lender and the leader in relationship driven mortgage banking, serving real estate brokers, affinity groups, credit unions, financial institutions, corporations and government agencies.

GIAC Mortgage utilizes a highly automated loan processing and underwriting system in conjunction with a state-of-the-art telemarketing, Internet and direct sales platform. Operating for the most part from one centralized facility in Denver, GIAC Mortgage is authorized to offer mortgage financing in all 50 states and maintains private label, full service capabilities for originating, processing, closing and servicing loans in the name of their business partners. Doing business from one central location affords GIAC the opportunity to maintain better control over the customer experience, in addition to gaining certain process efficiencies. GIAC's operation has evolved into a state-of-the art operation that can be private labeled with ease for their business partners.

Organizational Structure

The Chief Technology Officer, who reports to the CIO, sets the overall direction for the Information Technology group in terms of architecture design, new technologies to be

implemented, and overall strategic direction. The Teams listed below are responsible for implementing his philosophy.

Teams who report directly to the CTO include:
Information Security: This team is responsible for creating policy on security related matters throughout the organization and conducts continuous risk assessment and oversight of information security, access and availability controls. Information Security team has the added responsibility of auditing other departments through direct access to the security, access and system logs of the machines.

The Business Continuity/Disaster Recovery part of the Info Security team does a daily assessment of possible threats to the company that may cause interruptions in business such as natural disasters or power outages, to guarantee that the company can still service the customers and process new business in case of these unplanned events.

Network Connectivity: This team is responsible for creating and managing the connections to and from external Partner networks, as well as the design of the GIAC communications infrastructure for both internal and remote employees. This team also manages the Firewalls and the associated rule bases. All firewall changes must be scheduled and are subjected to review and approval of the Information Security Team and follow standard change control authorization procedures. The Network team also reviews the firewall logs on a regular basis, and as needed during an analysis of a security event.

Enterprise Architecture: This team is responsible for the overall design of the GIAC infrastructure, framework and topology as well as the review of all new technology components that may be introduced into the organization. The Enterprise Architects are responsible for the integration of existing and newer strategic technologies into the enterprise and for setting the direction of how the company will be embracing those technologies.

Messaging – This team handles and maintains all of the e-mail communications to and from the company, and manages all of the Exchange servers. They also manage the e-mail gateways, the servers that reside in the DMZ, and the tools that control and monitor the surfing habits of the employees. Administration of the SiteMinder tool and the LDAP database reside with this team.

Advanced Technology Services – This group is actually composed of four sub-groups: NT/Client Server, UNIX, Desktop Support and the IT Hotline. NT/Client Server is responsible for the maintenance, administration and implementation of the windows network infrastructure. The UNIX team handles all aspect of the UNIX environment within GIAC, including all of the web servers in the DMZ. Desktop Support handles all day-to-day hardware and software issues for all employees on the floor – upgrades, new installs, software conflicts, etc. The IT Solutions Hotline is responsible for creating new accounts, disabling old ones, modifying profiles and generally creating 'tickets' for the requests that come in over the phone to them.

Database Architecture – This team deals exclusively with the back-end databases that house all of the company and customer data. This team effectively own all of the data marts that hold client and customer data and used as a repository for reporting and metrics.

eBusiness – This team handles and designs the websites, both for the company, as well as all of the customized private label sites that GIAC hosts on behalf of its partners. eBusiness also designed and maintains the company intranet. The primary effort of the team is to create a pleasant user experience for the B2B and B2C websites that they create to facilitate Internet-driven business, so that maximum operating efficiencies can be realized by shifting as much of the mortgage loan process as possible to the Internet.

~

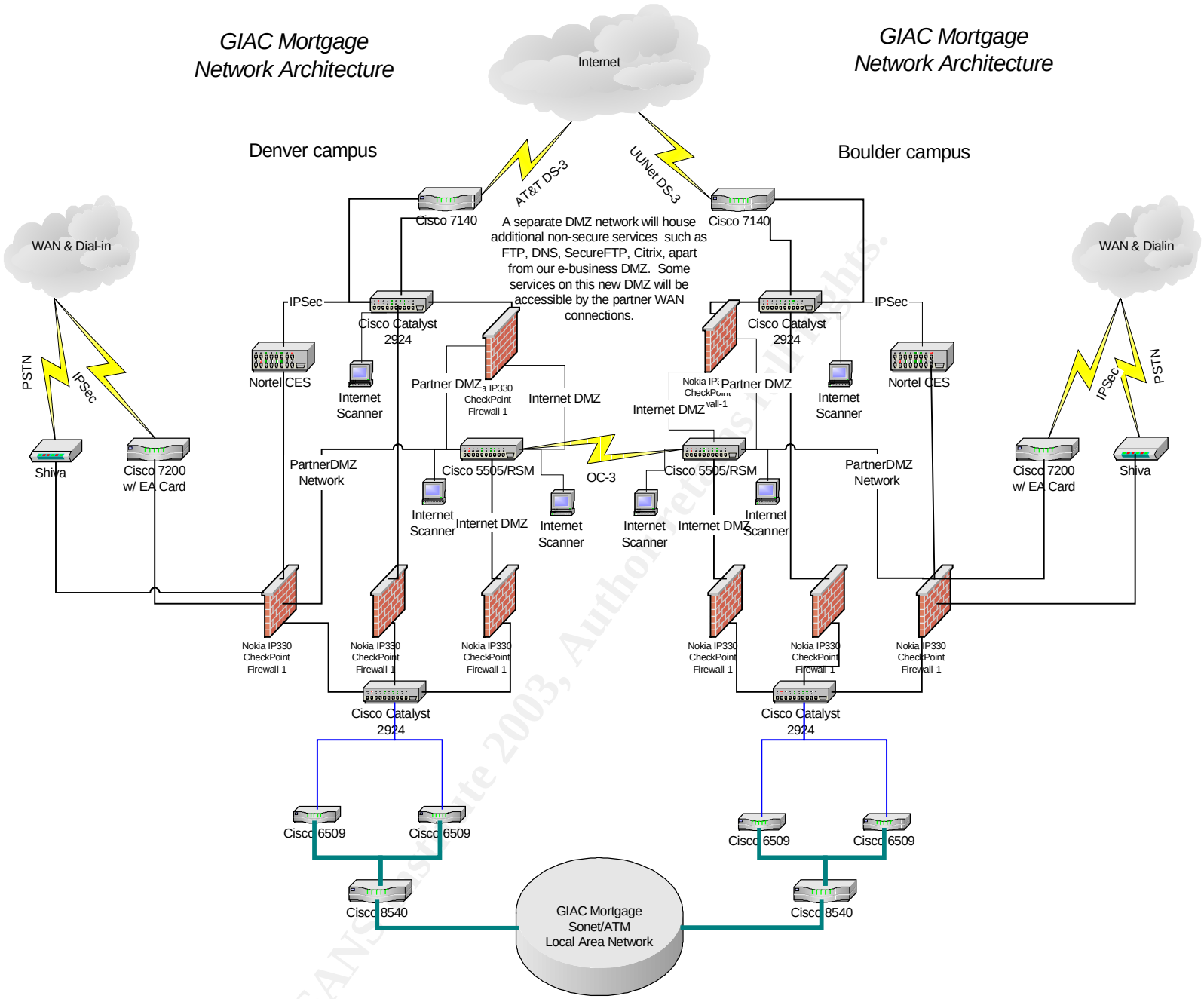
IT Infrastructure

GIAC maintains a primary data center at a Denver, Colorado campus and a secondary back-up site in their Boulder campus, where most of the IT staff is located. Boulder acts a "hot site" for Denver with real-time replication of all critical applications. An OC-3 link connects the two data centers. Business continuity and recovery is facilitated by this redundant data center strategy, along with a dynamically rerouting infrastructure running over a private SONET backbone. Soft PVC's and Private Network Node Interface (PNNI) are utilized to provide the best possible uptime.

The business continuity plans and technology architecture allows for the relocation of critical staff between the two campuses. The ability to run critical applications from either data center ensures that operations continue to function if one of the data centers is down. **(See Infrastructure diagram below.)**

The primary data center has two PDUs for providing dual power sources to critical devices. Each PDU is backed up by a separate UPS system; each UPS system is backed up by a separate generator. The backup data center has a single PDU, UPS and generator. Inter-campus data services are delivered into each site via a high-available and redundant Sonet infrastructure.

Applications in GIAC's infrastructure were developed to operate in a n-tier application development environment. The core of the GIAC Mortgage network is based on Cisco 6509 layer 3 switches. The GIAC Mortgage network infrastructure is constantly monitored by Concord Network Health, a network monitoring tool used measure capacity on all critical network links. All core servers connect to the data network through 100 Mb/s full duplex network connections. GIAC Mortgage has two DS3 connections to the Internet via two Tier 1 ISP carriers.



Internet Connectivity

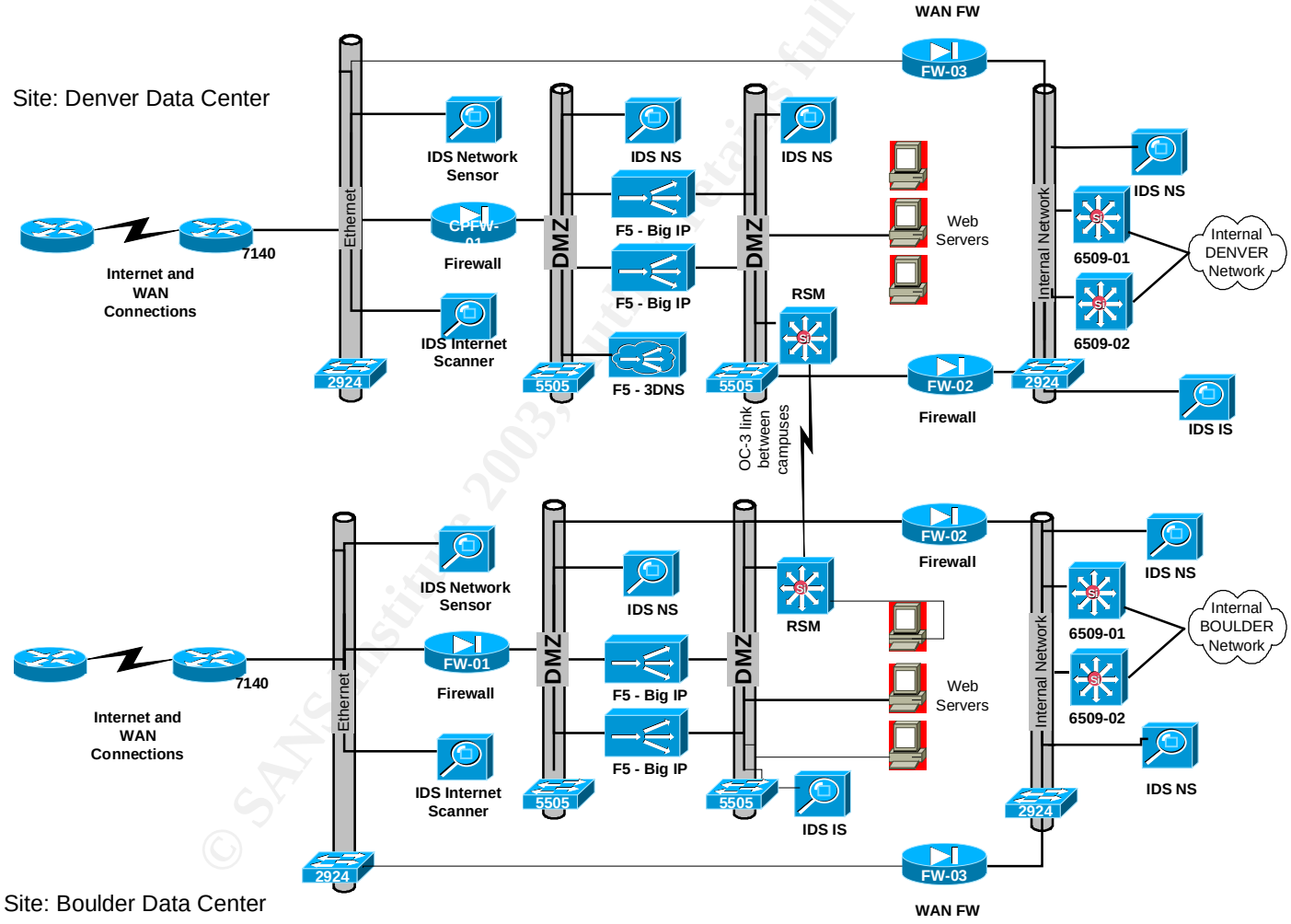
GIAC uses two Internet Service Providers, AT&T and UUNet. One vendor comes into each of the two campuses with a DS-3 line for failover and redundancy purposes.

The head-end routers that talk to the DS-3 lines at each campus are Cisco 7140's.

The connectivity then goes to Cisco Catalyst switches, and then onto the Check Point firewalls. (see Firewall description below). Hanging off of the Catalyst switches are both IDS Internet Scanner and IDS Network Sensor tools.

The GIAC Internet access topology is designed with web servers hosted on a DMZ behind the head-end router's ACL's, F5 BigIP network load balancers and bounded by external and internal Checkpoint firewall appliances creating a screened subnet architecture, which allows traffic only on ports 80 and 443 through the external connections.
GIAC's Internet connectivity is shown below.

GIAC Mortgage
Internet Connections



Information Security Overview

GIAC Mortgage is committed to the implementation of "Best-in-Class" information security measures and has aggressively pursued security measures that are fully in line with standards

of the financial services industry. The GIAC Information Security program has been implemented with the principle of "least privilege" as it relates to access control.

GIAC uses Check Point Firewalls on Nokia Appliances; Check Point NG is running on outbound web servers as their standard to enforce stateful packet inspection. There is a layered network architecture that uses both inner and external firewalls to bound the DMZs (e.g., web hosting and partner) and other special purpose firewalls protecting special services such as Internet access and VPN for remote employee access connectivity. The VPN infrastructure consists of redundant Nortel servers serving their remote user community with IPSec being utilized for VPN connections.

There are no "standard" protocols permitted through the firewalls. Permitted protocols are based on business requirements and security best practices. Changes are determined on a case-by-case basis depending upon application and business requirements and network security policies. The perimeter security is verified through vulnerability assessments performed regularly by the Information Security Team.

For their e-mail environment, GIAC is currently running Microsoft Exchange 5.5, planning to migrate to Outlook 2000 by end of year. GIAC Mortgage has standardized on the TrendMicro virus detection platform for SMTP, Exchange Mailbox and network gateway needs. The company has also standardized on the Symantec Norton Antivirus Corporate Edition system with live auto-update of signatures for all clients and servers for their desktop/server needs. Clients run on the desktop and TrendMicro runs on e-mail gateways and Exchange servers. All clients are managed by central servers with update checks every 15 minutes.

In addition, the gateways strip off an attachment if the specific extension of the attachment appears on a predefined list. Typical extensions that would not make it past the filter would be: .scr, .mp3, .vbx, .lnk, .vbs.

Connectivity for remote users and employees

No remote access is permitted to production servers across the Internet except for authorized systems administrators who utilize a hardened support platform that includes GIAC issued secure equipment (laptop or desktop), a VPN (Virtual Private Network) client with locked down configuration enforcing Kerberos key exchange IPSec tunneling, Radius and domain level authentication, an enterprise controlled anti-virus and personal firewall installation and a separate router-based firewall connection. This access is permitted only for emergency support purposes.

For remote administration, communication to all hosts that are resident on DMZs, (such as the web hosting and partner DMZs) require the use of SSH. Native Telnet, FTP and other insecure protocols are not permitted. Authentication is achieved by Kerberos key exchange and user ID and password.

GIAC has an extensive franchisee network of Account Managers and Field Service Reps that constitute their remote user force. Most of these remote users use a standard VPN tunneling client for remote access that is provided to only authorized employees. The VPN service

supports connection via a centralized modem pool as well as broadband connectivity delivered via GIAC's Internet POPs.

Business Continuity & Disaster Recovery/Backup

GIAC Mortgage has developed a complete Business Continuity/Disaster Recovery strategy that is maintained by a cross-functional, multi-disciplined team from across the business. Every department in the company is represented on this team and maintains plans specific to their business function. The business continuity plans are also supplemented by a complete and recently updated business impact assessment and disaster scenario/threat analysis. In addition, all business continuity plans are aligned with GIAC's technical systems architectures and disaster recovery plans to support high availability for critical systems, and minimally provide business-acceptable restore and recovery capabilities.

Key components of the infrastructure are located in both the Denver and Boulder campuses, including hardware for load balancing, partner gateways, and connectivity. Critical servers have a standby infrastructure in the backup data center in Boulder. Critical business data is stored on redundant or protected media, and the most critical data is replicated between the two data centers in near real time. Systems are in turn recoverable at the backup data center or as necessary from offsite media. Critical components in the infrastructure are duplicated. Many critical servers are setup in a clustered environment to enhance availability due to component failure. Fail over procedures allowing for movement from primary to standby servers, are developed to be completed either automatically

As for backups, GIAC Mortgage completes differential backups on all of its production data and systems every night. Data is initially backed up to disk storage with two copies of each back up set being made to separate tapes. For each back up, one tape set is kept onsite in the tape library and the other is rotated to offsite storage. GIAC utilizes a systems backup engine and library management tool from IBM called Tivoli Storage Manager (TSM). For tape retrieval, an automatic process is used with tape libraries.

A variety of Sun Servers exist in GIAC's environment today. These servers range from Sun Ultra 10's to the Sunfire 15K. Production servers are EMC attached via Ultra Wide SCSI connections. All UNIX servers are first hardened with a TITAN script and have all unnecessary services and scripts removed before being deployed into production. (The same is done for NT/2000 boxes with Microsoft's lockdown tool, and patched with the most recent updates, patches and hot fixes.)

Various Dell PowerEdge servers ranging from single processor to eight processors are in place and business-critical servers are utilizing EMC SAN for data storage. Less-critical servers use internal disks for data storage (with Mirrored/Raid 5 set-up).

GIAC database architecture consists of a J2EE framework for both presentation layer and common business logic. In addition, EAI (Enterprise Application Integration) technology is utilized for workflow and data integrations. Specific technologies include:

- J2EE: BEA WebLogic
- Messaging: MQ Series

- Webservers: Sun iPlanet, UNIX/LINUX Apache Web Server
- EAI: TIBCO ActiveEnterprise

The iPlanet web Servers run the WebLogic proxy agent to communicate with the WebLogic Middle-Tier server on the internal network. All content and data is severed dynamically based on URL string passed and successful authentication of the customer.

Enterprise-wide databases include vendors/products like Oracle, Sybase & Microsoft SQL Server. Various replication tools are utilized, such as Sybase Replication, Shareplex, Oracle snapshots, and Extract Translate Load (ETL) products like Data Junction are used to replicate data across different databases. Most production SQL Server databases rely on clustering to achieve the same. For Oracle, a hot standby solution is utilized to achieve high availability. Data Security is controlled by the use of roles and profiles in various databases.

GIAC's Information Security team utilizes both network and host-based intrusion detections systems in their detection of internal and external threats. On all DMZ and perimeter networks and hosts, the company deploys ISS RealSecure Network and Server Sensors. They have also deployed the ISS RealSecure System Scanner, the Fusion engine and SiteProtector for correlation analysis. Internal networks run the NetIQ Security Manager host-based intrusion detection.

At the user level, for desktop access, the solutions used in securing access to their applications and other enterprise electronic resources are based on the "shared secret" model utilizing username and password combinations. Employee access to internal applications is controlled by an in-house developed tool, created in Powerbuilder, that provides role and rule-based authentication and authorization. This program creates profiles and is used primarily by the IT Solutions Hotline who are tasked with account creation (and deletion.) All web-based applications, designed for both internal and external users and partners, have Netegrity's SiteMinder application as the 'gatekeeper' with an iPlanet LDAP holding the user accounts.

GIAC runs both NT and Windows XP Professional on the desktop, with a migration plan towards a full XP desktop image by mid-2004. For NT Systems, all hardware is Dell based. New NT server systems are deployed with running NT2000. All older systems are running NT 4.0 SP6. All UNIX based systems are running on Sun hardware using Solaris 8. All older systems are running Solaris 6.

Finally, wireless access points have begun to show up within GIAC's network environment. Easy to deploy inexpensive and compact wireless devices and hardware are becoming more prevalent in businesses and especially at home offices and remote franchisee offices. Though not officially sanctioned or supported, GIAC has yet to formally deny the use or issue a policy on how wireless devices and access are to be allowed.

~

GIAC Business Operations

GIAC Mortgage is the number one private label mortgage outsourcer in the United States, and private labeling represents the bread-and-butter of GIAC's business operations. To the customer, the GIAC name is invisible; GIAC does not advertise in its own name - even their franchisees do business under other names - so it is important to cultivate private clients and deliver that transparent experience to the private label's customers as if the private label was selling the service. The ability to deliver and to continue to deliver that experience to the customer is considered to be GIAC's "crown jewels."

GIAC Mortgage's Origination System (GMOS) is an in-house developed, n-tier application that includes desktop clients, middle-tier application servers, messaging servers and database servers.

Customers can interface with GIAC Mortgage through the telephone, Web or through GIAC Franchisee offices (who do business under other commercial names). Franchisees (and private clients) market the mortgage program to its customers, promoting 800 numbers, Web address or other channels. (**See Mortgage Process diagram below**)

Private label customers have access to a team of mortgage consultants at GIAC who are dedicated to a particular private client business channel. Consultants, using their GMOS technology, will help the customer choose the best mortgage for their needs. GIAC provides loan approvals in 15 minutes of completed application and offer a streamlined process to all of its partners.

To protect the "crown jewels" of the private label experience, all customer interaction, phone, documents, and e-mails will be done in the private client's name. In the origination department, private clients have multiple dedicated toll free numbers based on channel and customer segment.

Once the application is created, the loan is sent to a team of counselors again dedicated to the private client relationship who process the loan with a goal of meeting the customer's planned closing date. GIAC handles all aspects of the closing. Even at closing, all documents are printed with the private label's logo and business information. The private client's brand name is constantly reinforced throughout the entire process.

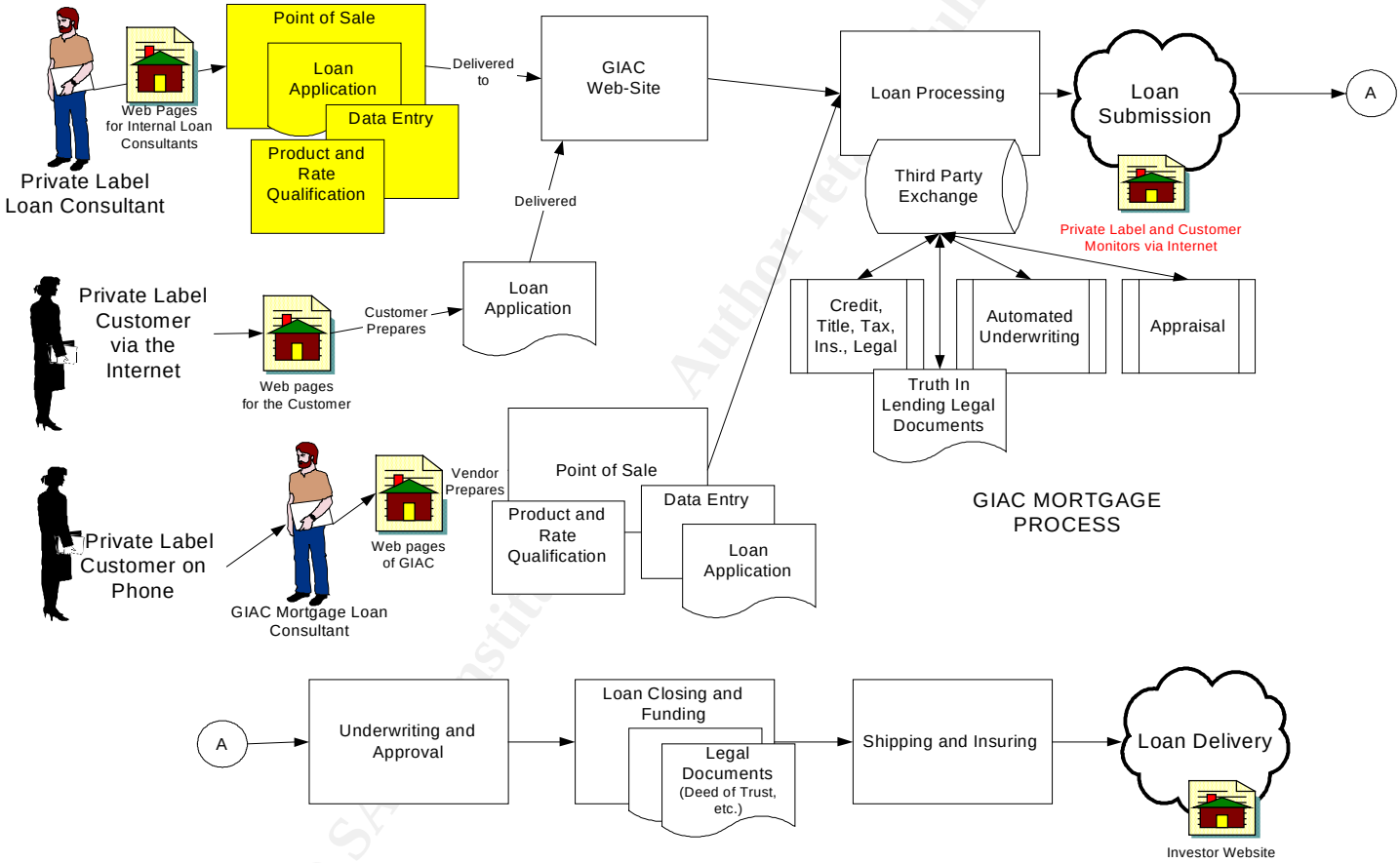
From the Internet, GIAC can originate products for private client's customers through GIAC's "Fifteen Minute Home Loan" platform which private client's can build around or link to any of its web sites. GIAC has spent considerable time developing web content allowing the customer to conduct the entire application and approval process on the Internet. GIAC has an exclusive relationship with Freddie Mac for its proprietary on-line approval process. This is the most streamlined approval process in the industry. The current functionality includes: live daily rates; mortgage reference information; calculators including monthly payment; maximum loan amount; rent vs. buy; pre-qualification; application, full online approval, rate lock capability and compete access to loan status once the customer is

in process. It is all implemented with full private labeling capabilities at no additional expense to the private client.

To improve efficiencies in loan processing, the private client's customer has the option to communicate via the Internet by connecting, via www.*privateclientwebsite*.com to www.whatsthestatusofmymortgageloan.com.

THE GIAC MORTGAGE PROCESS

At this site, all the customer's pertinent loan information is available. All conditions opened



and closed, current rate quotes and closing information, closing costs and loan counselor contact information is available from this single site.

~

Section 2 - Risk Identification within GIAC Mortgage

Based on an ongoing annual Business Impact Analysis (BIA) across the organization, the three top critical risks to GIAC Mortgage were identified and listed below. They are:

1. Widespread use and sharing, and lack of accountability of generic ID's
2. Unauthorized access to the GIAC network from wireless devices
3. Unauthorized access or compromise of GIAC's customer's "restricted confidential information"

Risk #1 – Widespread use and sharing of generic ID's
What is the risk?
When not used properly, generic or shared IDs can result in unauthorized access or changes. The bigger problem is the lack of adequate accountability surrounding these types of accounts, and the possible impairment to data integrity that may result.

Why is this a risk to GIAC?
With over 8,000 employees, it is difficult to keep track of everyone's rights and privileges in all applications. With their LDAP database and authentication/authorization services like SiteMinder, GIAC must pay a fee for each license. A generic ID is sometimes created to ease that financial burden and to make it easier to do routine and repeatable events like training and quality assurance testing. Often, many employees share the same ID over and over while accessing applications or services. That ID often remains the same, with the same unchanged password for many years. With a number of QA, testing and service environments that use generic ID's, the lack of accountability across these environments is problematic.

What are the potential consequences of the risk?
Since many generic, testing and service ID's often remain the same, with the same password for many years, the risk is high of unauthorized access to data by an employee that has since left the department or company but remembers the ID and password.

Since generic ID's are typically not assignable to specific people, the situation exists for limited accountability for authorized access to information.

What can be done to mitigate the risk?
GIAC needs to create, publish and enforce a policy on the use of generic and testing ID's.

The policy should state that IDs are to be assigned to specific users only. Those ID's should be explicitly denied for use by more than one employee at a time. Whoever is assigned an ID is accountable for its use regardless of the application or environment it is used.

A central authority (the Information Security team, or the IT Hotline) should be responsible for both creation of all ID's as well as deletion, and be accountable for who is assigned the ID so that tracking use of the ID can be verified and validated.

Generic, testing and service ID's should be deleted as soon as testing is complete or the ID's are no longer necessary. At the very least, the ID should be disabled and the password changed. When a new user is assigned the ID, they must change the password on the initial logon to one of their own.

Risk # 2 – Unauthorized access to the GIAC network from wireless devices

What is the risk?

Though currently proliferating in the workplace, the use of wireless is still a kind of "wild-west" technology with a number of inherent insecurities. Simply installing a wireless network or access point internally can cause a company to unwittingly extend the perimeter of its network beyond its physical space. If not properly secured, the access point can allow unauthorized visitors within close proximity of the access point admittance to the entire network. Without a formal policy delineating correct wireless policy, users do not know how to set-up and configure wireless access, nor do they know when they are engaging in bad practices.

Why is this a risk to GIAC?

Like most companies who deal in mortgages and confidential financial customer data, GIAC has much to protect and a lot to lose if its network is compromised by unauthorized intruders. GIAC is regulated by legislation like Gramm-Leach Bliley to ensure the integrity of and safeguard customer data. Without the proper encryption and authorization mechanisms in place, GIAC would not only open up a clear path into the company network, but be in clear breach of its fiduciary responsibilities to its partners and their customers

What are the potential consequences of the risk?

GIAC may be extending its network beyond its capability to secure it. The matter of convenience that the wireless access affords the users may be negated by the additional liability and insecurity that the wireless infrastructure brings with it. Being able to access the GIAC network via an access point that does not properly authenticate the users, or even via a rogue access point that the company did not authorize, puts a user right into the GIAC network with potential access to all customer restricted confidential data. GIAC would suffer the loss not only of the confidentiality of data, potentially the integrity of it, possibly the availability of the network (through a denial of service attack against the access point), but most importantly the accountability of tracking known users who access network resources.

What can be done to mitigate the risk?

First, GIAC must create, publish and enforce a wireless usage policy.

Policy statements should include assertions that in order to use or access all wireless LAN implementations, or applications utilizing wireless LAN technologies,

All **users** must:

- Access the GIAC network through an approved VPN connection after authenticating to the GIAC access point.

All **Administrators** must:

- Place the wireless access point(s) in a separate DMZ, separated by a firewall from the rest of the network
- Enforce authentication and access control over all wireless LAN link(s).
- Encrypt all data traffic over the wireless LAN using Wi-Fi protected access (WPA) 128 bit key or better.
- Ensure that all wireless access points are secured with a strong administrative password. Administrators must ensure all vendor default usernames and passwords (and SSIDs) are removed from the device. Administration of the device should be prohibited from the wireless network.
- Enforce user-level authentication (i.e., user ID and password) before granting access to the network or any networked resources via the wireless LAN.
- Enforce application-level authentication (i.e., application-level user ID and password) before granting access to any application over the wireless LAN.

Risk # 3 – Unauthorized access or compromise of GIAC's customer's "restricted confidential" information

What is the risk?

Currently, much of the confidential and more sensitve "restricted confidential" customer data is stored in databases, file systems and e-mail without encryption controls in place. Data that is transmitted over internal and external networks is in some cases is secured via IPSec and SSL transport layer encryption, but generally, data in storage is in clear text.

Why is this a risk to GIAC?

This situation is a risk is usually understood to be present by most companies that have an Internet present, so it is not necessarily unique risk to GIAC, but since almost half of GIAC's revenue is derived by the financial arrangements it has with its private label customers, the company needs to maintain the ability to continue this business practice. As the world's leader in private labeled mortgages for high-profile financial services clients, GIAC has a lot to lose if this channel of business – the "crown jewels"- is ever imperiled since GIAC does not do business under its own name. The company has to maintain the integrity of that experience so it is always transparent to the customer in every channel. Naturally, the databases that house the customer data of the private clients are coveted assets by hackers and insiders looking for opportunities to do bad things; if those information assets of the client's customers were to be compromised, the resulting negative publicity would be devastating to GIAC's ability to keep and attract additional clients in the future.

What are the potential consequences of the risk?

A employee who has not been constrained by appropriate access controls, or a non-employee who is inside the network can then attempt to access the databases that store both confidential personal data as well financial data like credit card numbers, bank account numbers, asset account numbers, etc. The likely legal liability and federal legislation to

protect the data notwithstanding, the adverse publicity to both the company and the private clients whose customers data was compromised would be devastating to the long-term feasibility of GIAC doing business on behalf of private clients.

What can be done to mitigate the risk?
There are a number of solid security efforts that GIAC can employ to make the environment that houses customer data as secure as reasonably possible. First, GIAC should assume a "default deny" stance on all devices. This would mean that unless specifically allowed, a service, access or connection is denied. This posture should be applied to GIAC's entire Internet perimeter and on the internal business applications. To be assured that the company maintains this posture, and to give the company another perspective to its security stance, they should employ a third-party firm to do vulnerability and threat assessments.

Internally, GIAC should minimize the effects of vulnerable hardware and software that could be used to launch or introduce exploits into the company. In addition to employing a patch management program to keep servers and workstation up-to-date, GIAC should try to minimize the exposure to known exploits run against the many Microsoft operating systems it has in-house. An effective initial step would be to not allow any Microsoft based servers in the DMZs; that is, deploy UNIX or Linux-based machines only. Any Microsoft service should be deployed behind secure reverse proxy only. Doing this won't completely avoid vulnerability and liability, but it will certainly lower the number of total exploits that the company might be vulnerable to.

Finally, GIAC should begin to encrypt data in storage. Though the process of encryption/decryption may have a noticeable effect on latency, it is fast becoming a requirement in the financial services industry which is heavily mandated by legislation like Gramm-Leach-Bliley and California SB 1386. Preferably, the company should use a commercial encryption algorithm that is 128-bit strength or better. Today, this could be Triple-DES, AES, MD5, etc.

Section 3 - Evaluation and Development of a GIAC Security Policy

The following policy is based upon a policy in use at the corporate parent of the author's company. The SANS format was used as a format for the policy.

GenericID Policy

Purpose
The purpose of this policy is to provide guidance for the use and restrictions associated with GenericID's.

Scope
A GenericID is an ID that enables a group of users to access a file, computer, or program. The GenericID allows an individual that is not a permanent employee to have access to a

part of the system to perform a designated function. This policy defines the use and misuse of GenericIDs to access any company system.

Policy

The GIAC Corporation restricts the use of any GenericID. To use a GenericID for access to any company system there will be individual accountability assigned to each GenericID. A record will be kept to identify the person who is assigned to each GenericID. This record will be accessible to the manager of the department, Human Resources, and Corporate Information Security.
NOTE: A GenericID, which can shared, is not the same as a User ID which shall not be shared. It is a violation of the Core Policies to share a User ID and Password.

Roles & Responsibilities

It is the responsibility of employees (contractor, consultant, temp):

- To use a GenericID only when approved to do so.
- To report the unauthorized use of any GenericID.
- To receive the approval for the use of a GenericID.

It is the responsibility of Technical services, Network Services, System Administrators, Network Administrators, and Account Administrators:

- To ensure that the approval has been granted for the individual to receive the GenericID access.
- To ensure that all GenericIDs are restricted to only those individuals that are approved for this access.
- To ensure that when a GenericID is no longer needed to disable it within the system to ensure that it is not accessed.

Guidelines

With certain exceptions, GenericID's are restricted and will not be used. With approval certain guidelines will be followed to ensure the proper usage of GenericID. The following guidelines will be followed when creating and using GenericID's.

1. Individual accountability is assigned to each GenericID for track proposes. Use the following examples to apply a common sense approach to any situation you may encounter.

   Example 1: If three unnamed consultants need ID's when they arrive, they should be given their own ID's (e.g. Consult1, Consult2, and Consult3). An existing GenericID can be re-issued to a new user but not if another user is still using it.

   Example 2: System administrator accounts with generic names (e.g., Root, Administrator, Supervisor, etc.) that are utilized by multiple support personnel should be required to show in audit trail records the individual that is using them at any point in time.

2. The account administrator identifying the person who is using each GenericID must keep a record. This record should show how long the access is needed, who has

authorized its use, and who will be using it. The authorizer should be the manager from the business unit that initially requested the GenericID's creation. This manager retains the responsibility for maintaining the legitimacy for the user assigned to the generic account.

3. When the person assigned the GenericID stops using it, the ID will be disabled and the password changed. Management authorization and an accountability record must accompany reuse of the ID by another person.

4. When the GenericID has been issued to a user, the password will follow the corporate policy on Passwords:
   - The password created must adhere to the company policy on construction, aging and uniqueness
   - If the GenericID account is needed, but will be used by another user, the password must be changed before the account is reused and must follow the password policy.

Generic ID Policy Evaluation

Summary Review – This policy does an admirable job at addressing a very common problem universal to many large companies. The policy was obviously established to combat the use and sharing of generic ID's by employees, but more importantly to begin to establish accountability in the use of those ID's. More than likely, GIAC initiated the implementation of this policy with strong encouragement from the Audit department, who probably pointed out that the lack of accountability, and a "paper trail" for user actions, was a reckless course of action in the long-term. Part of the strength of this document is that the language of the actions detailed for both users and administrators is understandable and unambiguous, yet firm.

Sections

Purpose:
The description of the policy's purpose is straightforward enough, and explains why the policy was created, but it is not sufficiently detailed to explain what specific issue the policy will attempt to resolve.

Background:
This section is not included as part of the policy. Though not always needed in every policy document, it helps give the affected user(s) more information about the policy or its intentions, and puts the issuance of the policy into a context that should help the user(s) with proper implementation.

Scope:
The description in this field does not really address the intended reach of the policy, i.e. who is covered by the policy, or what system it applies to. It is more of a description of what a

generic ID is. The information included here should probably be part of the Background section. Interestingly, the section here does note a possible risk of a generic ID, but does not go far enough to address why the policy needs to be implemented.

Policy Statement(s):
The policy statement lacks what I consider to be critical to a cogent policy statement: guiding principles. This section mentions all of the restrictions associated with and the administration around generic ID's but does not elaborate on how they can be used and in what types of environments (development, QA, production.) Additionally, there is no mention of whether or not exceptions to this policy will be approved in any scenario, and by whom if they are approved.

Responsibility:
The language in this section is clear and concise, explaining what the roles and responsibilities are for all parties. The R&R of the technical resources could have been delineated a little better with the inclusion of details of specific tasks that each department would be responsible for (e.g. who creates ID's, who ensures that the user is approved to use the ID, and how?)

Action:
This section is misnamed "Guidelines", and should be named Actions or Standards, since it has definitive steps to follow and ascribe to, rather than just recommendations. The language is strong and specific as to the use of ID's, both by the user and the administrator. The shortcoming of this section is that it does not assign responsibility to the actions it prescribes.

GIAC Generic ID policy Revised

The current generic ID policy is only partially complete. The policy needs to encompass other ID's that may be used by multiple employees, like testing or training ID's, and should address machine-run ID's like service accounts which are automated, and run without human intervention. Expanding the scope of the policy does increase the length of the document, but in doing so, it adds clarity to the intentions of the policy, and removes any ambiguity as to how ID's can be used and in what context and applications that they can be used.

GIAC Generic ID Authorized Use Policy

(Testing IDs and Service Accounts)

Purpose

The purpose of this policy is to provide guidance for the use of Generic IDs and identify restrictions on their use. When used in an inappropriate manner, Generic IDs can result in unauthorized access or changes, lack of adequate accountability and impairment to data

integrity. This policy is intended to define the permitted uses for these IDs and to clarify when their use constitutes an abuse of access to any GIAC Mortgage system.

Scope

A Generic ID is a user ID or user account that is not assigned to one specific individual and as a result provides little to no accounting of responsibility. The scope of this policy covers both general usage and restriction requirements as well as specific permitted uses. These permitted uses include special IDs established for testing needs and for unattended processing. The IDs in these two categories are identified as Testing IDs or Service Accounts, respectively and are further described below:

- A Testing ID is a user account reserved for testing and analytical purposes to either ensure a program, system or application is working properly, or to permit temporary access to a program or system to complete QA Testing.

- A Service Account is an ID or account that is setup specifically for unattended use in a scripted process, a scheduled job or process, or for batch functions that would not require an individual to log in.

Policy Overview

GIAC restricts the use of all Generic IDs. In order to obtain or use such an account, the following provisions must be met:

- There must be a valid business need;
- Accountability must be assured;
- Audit trails and records must be maintained;
- All records must be accessible to Human Resources, IT Management and/or Information Security Team, as required;
- The Generic IDs or accounts must adhere to established naming standards;
- All IDs must be deleted as soon as they are no longer needed; and,
- Information Security team has final approval over the creation of all Generic IDs.

Permitted Uses for Testing IDs

Policy Statements

The following policies must be followed when creating and using Testing ID's:

1. The use of any Testing ID is restricted for any environment other than which it was created and intended.

2. Testing IDs must not be used in production without the prior approval of Information Security. By default, Testing IDs are to be confined to Development and QA environments. Special generic Training IDs may also be set-up in training environments.

3. For tracking proposes, Coordinators must be assigned to ensure accountability for each Testing ID.

4. Where other testing needs exist that are not satisfied by Generic Testing IDs, employees must obtain their own individually assigned Testing IDs (e.g. Mary Jones will use his "jonesm_tst" Testing ID to do her program and system testing.)

Roles & Responsibilities

Employees (IT staff and business testers):

- Must only use a Testing ID when approved to do so.
- Must communicate such use to Coordinators.
- Must report the unauthorized use of any Testing ID.
- Must not request Testing ID roles/profiles to be modified.
- Must only use Testing IDs in the specific environments for which they were created

Coordinators (designated responsible individuals):

- Responsible for the distribution of Testing ID's to users. Coordinators should always know who has been assigned the specific Testing IDs by maintaining the appropriate records.
- Know the password associated with each Testing ID.
- Change the passwords every 45 days to maintain the highest level of security as per the company password policy.

Administrators (System Administrators, Information Security, IT Solutions Hotline):

- Should not modify a Testing ID from its original role/profile. For example, ID "appX_mgr" is a Manager Testing ID for Application "X" database and should only be used to test scenarios within Application "X".
- Ensure that approval has been granted for an individual to receive Testing ID access.
- Ensure that all Testing IDs are being controlled by Coordinators and restricted to only those individuals who require this access.
- Ensure that Testing IDs are disabled and deleted when they are no longer needed.

Permitted Uses for Service Accounts

Policy Statements

The following policies must be followed when creating and using Service Accounts:

1. The use of any Service Account is restricted for any use other than for scripted, scheduled or batch processing functions. These functions are to be unattended and would not require an individual to manually log in to the system.

2. Service Accounts are not to be used by employs to log in to any application for administration, support or other related purposes. Where employees have the need to access systems for administration, support or other related purposes, they must first be authorized to do so and then must utilize their own assigned IDs in order to enforce accountability.

3. Passwords for Service Accounts must be maintained securely and must not be shared or displayed.

4. A manager-approved request to the IT Solutions Hotline is required before creating a Service Account.

5. Service Accounts must adhere to the following naming convention:
    a. Account name must reflect the environment for which it was created and intended. Information Security must approve policy exceptions.

Roles & Responsibilities

Employees (IT staff):

- Use a Service Account only where required for unattended processes or functions.
- Report the unauthorized use of any Service Account.
- Ensure locations of scripts containing Service Accounts and passwords are secured and appropriately masked from display.
- Obtain approval for the creation and use of a Service Account and ensure naming standards are followed.
- Never use Service Accounts in the place of individually assigned User IDs for administration, system support or other related purposes.

Administrators (System Administrators, Information Security, IT Solutions Hotline):

- Ensure that approval has been granted for creation of a Service Account and that created accounts follow the established naming standards.
- Ensure that Service Accounts are deleted as soon as they are no longer needed.
- Ensure that Service Accounts are restricted and not available for direct login.
- Ensure that all Service Accounts are placed in the Windows domain group called "Process Accounts"

~

Section 4 – Developing Security Procedures for GIAC's policy

GIAC Generic ID, Testing ID and Service Accounts Creation Procedures

Overview

Inappropriate use of Generic IDs, Testing IDs and Service Accounts can result in unauthorized file access or changes, lack of sufficient accountability, and can permit multiple users to access a file, computer, or program for either approved or unapproved purposes. These procedures are intended to outlines the steps that each appropriate individual shall follow to use these IDs. Use of generic and Testing ID's and Service Accounts within GIAC must be in accordance with the GIAC Generic ID Authorized Use Policy.

Responsibilities

GIAC employees:
- Are required to get Manager/Supervisor/Team Leader approval before requesting/using a generic ID
- Are required to place a service request to the IT Solutions Hotline for ID creation once approval is received
- Must provide the Hotline a copy of the approved service request when requesting a new ID from the Hotline, along with their individual NT logon, which type of ID is required, and the application where the ID will be used
- Are required to follow the GIAC Generic ID Authorized use policy
- Are required to follow the Password Policy for using generic ID's as well

GIAC Managers/Supervisors/Team Leaders
- Are required to first give approval to any request for use of a generic ID before a service request is submitted to the Hotline
- Are expected to approve a generic ID for appropriate business need, and ensure that the employee uses the ID within the intended application
- Are expected to receive the created ID from the Hotline and distribute it to the requesting employee
- Are expected to notify the Hotline when the ID is no longer needed

GIAC IT Solutions Hotline
- Is expected to create the requested ID only when an approved service request is received.
- Is expected to follow the naming convention listed in the Procedures section of this document
- Is expected to e-mail the completed ID to the employee's Manager/Supervisor/Team Leader
- Is expected to delete or disable ID's when not in use or are no longer needed
- Is expected to provide Information Security a monthly list of all approved and created ID's

GIAC Information Security
- Is expected to have final approval over the creation of all generic IDs
- Will exercise auditing and oversight responsibilities over all employees use of generic ID's.

Procedures

GIAC Employees
- When requesting a generic, testing or Service account to be created, employees must forward a service request to their Manager/Supervisor/Team Leader for approval

- Once approval for the ID is received, the service request can be e-mailed to GIACITHOTLINE

- When requesting a new ID, the following descriptive fields must be supplied to the Hotline:

i. First field = "service or application needed"
ii. Last field = "Service"
iii. Description = "usage of account"
iv. Department = "name of department requesting account"
v. Manager = "name of employee's Manager"

- Once received, employees shall only use Testing IDs in the specific environments for which they were created

GIAC IT Solutions Hotline
- When an approved service request is approved, the Hotline shall follow the naming convention below for ID creation:

Example: An employee from Financial Reporting requests a Service Account for use in Tivoli. His manager's name is Jane Doe. The request to the Hotline should contain the following information:

i. First field = **Tivoli Monitoring**
ii. Last field = **Service**
iii. Description = **this is a service account for scheduling Tivoli monitoring**
iv. Department = **Financial Reporting**
v. Manager = **Jane Doe**

The newly created Service Account will then have the username of "**svcs_tiv**".

- Once created, the ID shall then be e-mailed to the employee's Manager/Supervisor/Team Leader.

- When notified that an ID is no longer needed or used, the Hotline will delete or disable the ID in NetIQ Directory and Resource Administrator.

GIAC Information Security
- On a monthly basis, Information Security will collect a sample of access logs from critical applications to ensure that employees are not accessing application for which they are not authorized. The team will use the list of created ID's from the report provided by the Hotline to determine the appropriate access privileges. If an ID is being used inappropriately (e.g. used in an application other than it was intended, being shared or logged in multiple places at once, in existence after the employee who requested the ID has been terminated), the Information Security team will disable the ID using NetIQ Directory and Resource Administrator, inform the Hotline of the action, and then inform the Manager/Supervisor/Team Leader of the employee involved.

~

Section 5 – References

Northcutt, Stephen, "Inside Network Perimeter Security" 2003, New Riders Publishing

Danchev, Dancho "Building and Implementing a Successful Information Security Policy," June 25, 2003 URL: http://www.windowsecurity.com/pages/security-policy.pdf

In Brief: The Financial Privacy Requirements of the Gramm-Leach-Bliley Act; Federal Trade Commission URL: http://www.ftc.gov/bcp/conline/pubs/buspubs/glbshort.htm

AirDefense White Paper, "**Understanding the Layers of Wireless LAN Security & Management**" April 2003 URL: http://www.airdefense.net/whitepapers/index.html

Paul, Brooke "Building an In-Depth Defense" July 9, 2001 Network Computing URL: http://www.networkcomputing.com/1214/1214ws1.html

Last Updated: September 19th, 2017

Upcoming Training

SANS Oslo Autumn 2017	Oslo, Norway	Oct 02, 2017 - Oct 07, 2017	Live Event
SANS Tysons Corner Fall 2017	McLean, VA	Oct 14, 2017 - Oct 21, 2017	Live Event
SANS San Diego 2017	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	Live Event
Community SANS Memphis MGT512	Memphis, TN	Nov 06, 2017 - Nov 10, 2017	Community SANS
SANS San Francisco Winter 2017	San Francisco, CA	Nov 27, 2017 - Dec 02, 2017	Live Event
SANS Cyber Defense Initiative 2017	Washington, DC	Dec 12, 2017 - Dec 19, 2017	Live Event
SANS Security East 2018	New Orleans, LA	Jan 08, 2018 - Jan 13, 2018	Live Event
Northern VA Winter - Reston 2018	Reston, VA	Jan 15, 2018 - Jan 20, 2018	Live Event
Community SANS Columbus MGT512	Columbus, OH	Jan 15, 2018 - Jan 19, 2018	Community SANS
Community SANS New York MGT512*	New York, NY	Jan 22, 2018 - Jan 26, 2018	Community SANS
SANS Miami 2018	Miami, FL	Jan 29, 2018 - Feb 03, 2018	Live Event
SANS London February 2018	London, United Kingdom	Feb 05, 2018 - Feb 10, 2018	Live Event
SANS Southern California- Anaheim 2018	Anaheim, CA	Feb 12, 2018 - Feb 17, 2018	Live Event
SANS Boston Spring 2018	Boston, MA	Mar 25, 2018 - Mar 30, 2018	Live Event
SANS 2018	Orlando, FL	Apr 03, 2018 - Apr 10, 2018	Live Event
SANS Baltimore Spring 2018	Baltimore, MD	Apr 21, 2018 - Apr 28, 2018	Live Event
SANS OnDemand	Online	Anytime	Self Paced
SANS SelfStudy	Books & MP3s Only	Anytime	Self Paced