Global Information Assurance Certification Paper

Catherine Peper

VP, I/T Protection and Controls

Date submitted: 11/02/03

Certification: Information Security Officer (GISO)

Second Submission – November 2, 2003

Practical Assignment Version 1.3 (February 7, 2003)

Location of class: SANS, Baltimore, April, 2003

Descriptive Title: Risk and remedies for an aging data center, a faulty data storage and recovery strategy and fragile controls around intrusion detection, prevention and response.

Abstract Summary

GIAC Enterprise has been fortunate and able to avoid catastrophic business outages in over 15 years while concurrently cycling through 4-5 generations of new technology and migrating much of its core business to the Internet. Recent assessments reveal that an aging infrastructure and outdated strategy for data storage, retention and recovery present unacceptable levels of risk to the enterprise. Immediate steps must be taken to mitigate these risks.

Like other organizations, GIAC is struggling with the mammoth task of hardening the security architecture that is under constant attack from viruses, malware and hackers. Additional defensive and risk management measures must be undertaken to fortify GIAC's intrusion prevention, detection and response capabilities if GIAC is to survive increasing attacks on its network and maintain connectivity with customers and suppliers.

The purpose of this assignment is to describe the IT infrastructure, identify and provide clarity on the most significant risks to GIAC's information and information systems and to provide appropriate policies and procedures to best mitigate these risks.

Assignment 1: Description of GIAC Enterprises

GIAC Enterprises has been in business for over 50 years and is a large health insurance company with 10,000 employees located in 12 geographically dispersed offices throughout one state. Company headquarters are located in a major city in the Southeast with the primary data center housed in one general office high-rise building. The company serves over 5 million customers and has relationships with over 50,000 physicians, hospitals and other providers of health care. Most of the sales activity is conducted with over 1,200 external agents and brokers.

IT Infrastructure

GIAC Enterprise has two IBM main-frames, 550 Windows/NT servers and 150 Unix servers. The majority of the infrastructure is located in the primary data center; however Windows servers and other supporting infrastructure are dispersed throughout the state. GIAC has virtual private network (VPN) connectivity with approximately 30 external organizations as well as extra-net connectivity with trusted trading partners such as large employer groups enrolled as GIAC customers and contracted general agents who market GIAC products. GIAC's Intranet is widely used by thousands of employees for daily transactions (e.g., access to PeopleSoft system) and access to enterprise information such as corporate policies. Availability and reliability are critical to GIAC. GIAC is governed by multiple external organizations, and security is a high priority due to the need to protect personal health information as well as comply with state and federal legislative requirements.

GIAC has a class B Internet address and a highly complex security infrastructure to support a defense in depth strategy. Internet connectively is enabled though two Tier 1 Internet Service Providers (ISP) over T3 lines connected to Internet routers using Border Gateway Protocol (BGP). In the event of a denial of service attack, the ISPs will assist in recovery of services to support GIAC's business model for high availability and redundancy.

Communication infrastructure is over a Sonet Ring, and Electronic Data Interchange (EDI) is enabled via four T1 lines. The HTTP server is Microsoft IIS/5. GIAC's message infrastructure includes a combination of MQ, Tuxedo and Open Data Base Connectivity (ODBC).

Security Architecture Basics at GIAC

The following provides an overview of GIAC's security architecture and management framework as the foundation of GIAC's defense in depth strategy.

Firewalls and the Demilitarized Zone (DMZ)

The firewall is the first line of defense from hostile activities on the public Internet. It acts as the gateway through which all traffic to and from GIAC's protected network must pass. GIAC's perimeter defense begins with Tumbleweed product suite. Internet content filtering is accomplished with World Secure server. The core firewall architecture is a "screened subnet" design. The firewall applies policy at the network and application layer and uses stateful inspection of Internet Protocol (IP) packets to maximize performance. It includes Network Address Translation (NAT) capabilities to hide internal network information such as IP addresses from un-trusted networks and Internet users. The opening of ports on the firewall is tightly governed to minimize risk to GIAC.

A Cisco Pix firewall keeps Internet packets from reaching internal (intranet) IP addresses (see Network diagram). Data that is exposed to the Internet, such as the GIAC's Web Site, domain servers, and mail servers, are placed in a carefully monitored network subnet or DMZ, which sits between the public Internet and private Intranet. While servers in the DMZ are publicly addressable, most Internet traffic is filtered prior to reaching the servers by only opening selective Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) ports on the perimeter firewall. In addition to the firewall protecting the DMZ and Intranet, the architecture allows for further sub-netting of security zones within the Intranet itself.

Border (or perimeter) routers are the last devices under GIAC's control prior to traffic traveling onto the Internet. The boarder routers separate the Internet from the DMZ. Interior choke routers protect the internal network from both the Internet and the perimeter net—they separate the DMZ from the internal "trusted" network.

The choke router does most of the packet filtering for GIAC's firewall allowing selected services outbound from the internal network to the Internet.

Authentication and Authorization

In order to protect critical information assets and personal health information, GIAC must ensure that access to secured information requires authentication against a centralized authoritive source. All entities must be positively identified before any authorization, resource allocation or other security related service is considered. The results of the authentication insure that the proper access rights and privileges can be assigned to the requesting resource. External computers and networks not controlled and owned by GIAC are considered un-trusted. GIAC uses Netegrity's suite of capabilities for authorization policy server (PMI) and delegated administrator for self-service**.** Once authenticated, user access to corporate resources is controlled through the use of rule and role based authorization to ensure that system resources are granted on a need-to-know basis depending on the users role (external customer) or job profile (internal).

Logging

GIAC needs to ensure that all significant electronic events are automatically logged utilizing standard logging services. Alerts are generated to warn of events that require investigation. These capabilities are needed to comply with federal and state regulations, including the Health Insurance Portability and Administration Act (HIPAA). GIAC also requires the ability to detect and investigate security breaches and minimize the impacts of intrusion, as well as to supply the information to support the investigation of potential fraud. Transactions must be capable of being traced from inception to completion. NetForensics is a cornerstone of GIAC's enterprise logging capabilities. GIAC is in the process of upgrading its NetForensics from version 2.3 to version 3.1. Unfortunately, GIAC needs significant improvement in this area as there are little to no logging capabilities in the internal server farm, GIAC's Extranet.

Encryption

GIAC applies integrity controls using industry proven security and cryptographic techniques to ensure confidential electronic information will be secured during transmission and storage. GIAC uses Secure Socket Layers (SSL) and Secure File Transfer Protocol (FTP). Server Digital Certificates are enabled via Verisign and Secure File Transfer via Valicert (Tumbleweed).

Intrusion Prevention

GIAC has been successful at preventing virus or other malicious code from penetrating its defense systems. The Blaster worm nearly crippled CSX Transportation and Air Canada as well as many other companies. Because of the

rapid response by GIAC's Server Management and Messaging Teams, GIAC experienced no major problems from this virus. To harden the messaging environment for high availability, the Messaging Team implemented anti-virus software on the external gateway and downloaded the new virus definitions hourly.

GIAC captures all in-bound external email to verify whether it is infected. If infected, e-mail is quarantined. This arrangement has proven effective in preventing viruses from entering GIAC's network through corporate email.

Patch Management and Alert Monitoring

It does not take many examples such as Code Red, Nimda and Blaster to demonstrate the absolute business imperative of monitoring security alerts and maintaining the ability to rapidly apply patches or hot-fixes for known vulnerabilities. GIAC's subject matter experts routinely monitor the CERT/Coordination Center (CC3) (http://cert.org) and other alert sources. In addition, GIAC established agreements with key vendors for notification of vulnerabilities (e.g., Cisco). GIAC also subscribes to IBM's Technical Support Bulletin which is distributed via e-mail to key resources. A review team is in place and meets weekly to evaluate patches, alerts and vendor notifications. An escalation process is used to decide when to apply specific patches. All patches are tested in GIAC's test center, a test plan is developed and changes and worked through a formal change management process with back-out plans should problems be encountered.

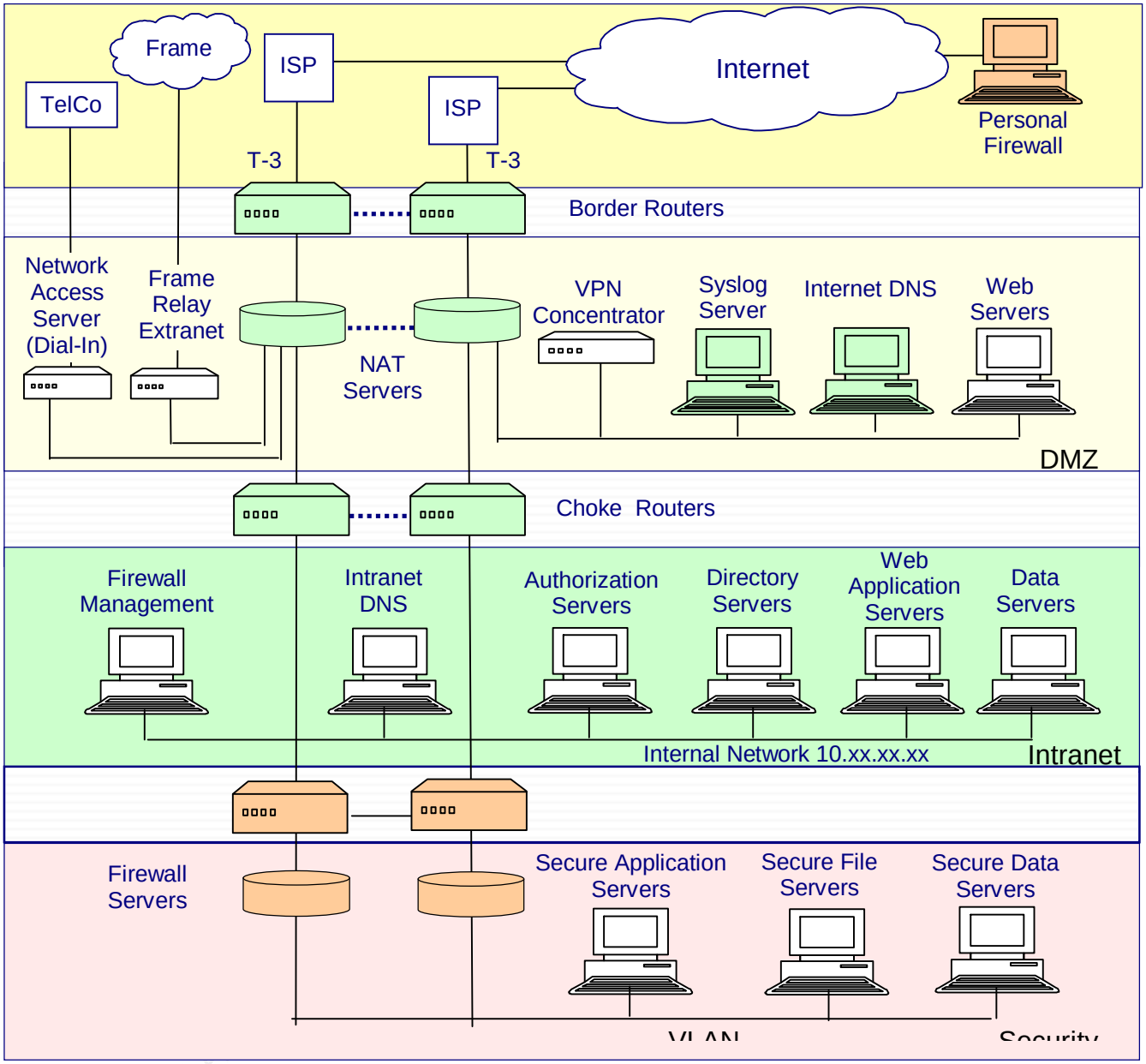
GIAC also implemented the ability to rapidly deploy patches, hot-fixes and Service packs to Windows servers using a product called Patchlink.[1] In response to a recently announced Microsoft vulnerability, GIAC was able to deploy the hot-fix to 375 servers within one week. Patches rated as critical must be applied within 7 days in the DMZ and 21 days to internal servers.

Patch management is different for the Unix platform. GIAC monitors vendor releases and other notification methods. GIAC only deploys patches in the Unix environment when they are experiencing operating system or application problems that are addressed in specific patches or when IBM issues a "hyper" alert with a known security issue. GIAC has not distributed an automated solution for the Unix platform and must deploy patches manually. Historical volumes are 2-3 emergency patches being applied per year and usually involving less than a 10% of GIAC's 150 Unix servers. Automation dos not seem cost justified at this point. GIAC will continue to monitor the volume of patches needed in this environment to determine when automation appears prudent**.**

Time Stamping:
GIAC has a tamper proof digital time stamping solution based on a hierarchy of specialized clocks to provide an evidentiary trail.

[1] Visit web site at http://patchlink.com

Network Diagram



How does GIAC Conduct Business Operations?

GIAC is in the information business and information management is a targeted area of excellence. Data is generated from GIAC's daily interactions and transactions with customers, health care providers and GIAC's sales and marketing distribution channel. GIAC has very limited face-to-face interactions with customers. The information flow begins at multiple points of capture or customer touch points (telephone, EDI, Internet). Resulting transactions are recorded in GIAC's many systems of record (SOR). Information that is needed for historical trending and analysis is integrated, synthesized and stored in GIAC's Enterprise Data Warehouse (EDS) and further specialized into data marts for dedicated business purposes. Enterprise Data is backed up and stored using Tivoli Storage Management (TSM) and Hierarchical Storage Management (HSM) facilities for business continuity purposes.

First, the business transactions. On a typical business day, GIAC processes approximately 2.7 million transactions (via telephone, e-mail, paper, electronic data interchange or EDI, Interactive Voice Response or IVR and web based). This includes:

- 450,000 claims. Seventy five percent of Claims are received electronically from over 10,000 independent health care provider locations. Avenues of submissions include batch EDI or an external provider Internet portal for online submissions. While infrequent, customers may submit their own claims on standardized printed forms that are electronically imaged.
- 50,000 inquiries. Thirty percent of inquiries are received electronically using IVR, internet and EDI. Approximately 40% of inquiries are direct calls to one of 5 major call centers with over 100 unique toll free lines. Approximately 30% of inquires are written correspondence with multiple attachments, all of which is imaged.
- 55,000 web site visits occur daily. The most popular feature s are locating a health care provider, claim status inquiries and seeking general health care information.

To execute its business model, GIAC has developed alliances with external organizations with whom it must have on-going communications. Of critical importance is the ability to verify eligibility for GIAC customers and to successfully execute medical authorizations for health care treatment. Ninety percent (90%) of claims and approximately fifty percent (50%) of inquires are completed by providers on behalf of GIAC's insured customers. Enrollment data for most of GIAC's 5M customers is submitted electronically through their employers or other organizations (e.g., Federal government). GIAC's website and EDI gateway are available 24X7 with exceptions for scheduled maintenance.

Critical business functions include:

- Claims Processing (receipt and adjudication);

- Medical Authorizations for admissions, high dollar services (e.g., MRI);
- Inquiry management (by customers and providers);
- Membership, Billing and Enrollment;
- Financial settlement (payments, adjustments, Check-writing);
- Coordination of benefits with other Payers;
- Enterprise resources functions (cash management, accounts receivable, investments, payroll, Human Resources Systems (Peoplesoft); and
- Rating and underwriting to obtain quotes for insurance coverage.

Applications and Types of Access:

GIAC has over 750 business applications running on a variety of platforms (MF, distributed) and data bases (Oracle, DB2, Unix, Access, SQL Server). While GIAC has matured capabilities to implement commercially available applications and service platforms (i.e. Siebel, Peoplesoft), there are hundreds of proprietary internally developed applications that make up the critical business functionality. The customer service representatives access legacy applications via a GUI front-end and use extensive screen scraping technology. Roles based security has been deployed throughout GIAC for information access and authentication. GIAC has approximately 500 tele-workers that connect via the Internet to dedicated Citrix servers. Agents and Brokers connect via extranet connectivity. Customers, providers and agents can also connect to GIAC via public e-mail and secure e-mail. Customers can also use the Internet web site to change demographic information, obtain expert health care advice, locate a participating provider or check on the status of a claim. Customers pre-register for self-service capabilities and are mailed a PIN and user ID.

Availability and reliability of critical applications, data and infrastructure are at the very foundation of GIAC's business model. Private and confidential customer information must be protected in order to maintain public confidence and comply with federal and state legislative requirements in addition to compliance with industry specific standards (e.g., HIPAA). Maintaining connectivity with outside organizations, trading partners and alliance members is absolutely essential.

Information integration and access to hundreds of applications is a constant challenge for GIAC. To support on-line interactions, GIAC must have highly available and integrated sources of critical information that can be presented via multiple communication channels. GIAC has developed operational data stores which are stored on the main-frame in DB2 data bases for critical subject areas (claims, customers, providers, products etc.) that are accessed simultaneously by many business applications. GIAC has implemented an enterprise data warehouse EDW to allow for access and analysis of massive amounts of data to effectively manage costs and risks.

Assignment 2: Areas of Risk

To maintain profitability, provide for continuity of care and service, GIAC must have:

- A highly available and redundant infrastructure;
- The ability to store, and reliably retrieve massive amounts of data;
- The ability to secure its network to protect the confidential, integrity and availability of information.

Because GIAC is located in a geographic area that is highly susceptible to hurricanes and tornados, its most basic need is to assure that the physical infrastructure housing critical data is adequately secured and that it can process, retain and protect health care data (GIAC's crown jewels). Based on a high level risk assessment, the three most critical areas of risk for GIAC are:

1. GIAC's primary data center;
2. storage architecture for data storage retention and recovery; and
3. intrusion prevention, detection, and response capabilities.

Risk # 1: GIAC's Primary Data Center

GIAC's primary data center has evolved over 30 years to approximately 30,000 feet of raised floor space. The mission criticality of the data center continues to increase as the business becomes more dependent on information technology to automate processes associated with sales, underwriting, claims processing and provider/customer service. Increasing pressure to lower administrative and medical cost, while simultaneously improving the customer's and provider's experience, demand that current and future information systems are continuously accessible and recoverable. New regulations, including the Center for Medicare and Medicaid Services (CMS), Sarbanes-Oxley, and HIPAA, require minimum standards for the enterprise to protect the physical and technical integrity, security and availability of health care information.

While considerable investments have been made in delivering information technology business solutions, relatively small amounts have been invested in the data center facility and its underlying electrical and mechanical infrastructure. An overall assessment revealed significant vulnerabilities including:

- **Support systems**, such as cooling tower and generators, are exposed in facilities that could not sustain winds expected in a category 2 hurricane or tornado.
- **Water intrusion** on floors above the data center and through standard plate glass windows within the data center.

- **Fire suppression systems** are dated technology (halon) with a recent history of unplanned halon discharges leaving the enterprise at risk during re-charge efforts and presenting risk to personnel on the floor.
- **Floor to ceiling heights** are insufficient to ensure adequate ventilation and cooling. Hot spots are frequently detected particularly with the newer technology and compaction of computing power.
- **Physical security** and access to premises are cause for concern. Security cameras are not routinely monitored; access for maintenance crew is not sufficiently restricted; and doors to the data center have external hinges permitting easy access.
- **Flooding** is a high probability since the facility is located in a flood zone and in close proximity to a large waterway and in a low flood plain requiring that the building be evacuated in the event of a class 2 hurricane.
- **Electrical Systems.** Of primary concern are the electrical systems. One half of the facility's custom switchgear is 30 years old and would take 15-20 weeks to replace. The main power source is 13 feet below grade making it vulnerable to outages caused by flooding.
- **Back up electrical generation systems** are at or over capacity and have no built in redundancy. Battery strings are over 5 years old (end of life) and not routinely tested. UPS batteries are cabled in one circuit configuration creating a single point of failure.
- **Cooling capacity** is chilled water and no redundancy provided.

Although facility related failures historically occur less often than application or computer hardware problems, the duration and downstream impacts of facility outages are much more severe. As the infrastructure continues to age, the likelihood of component failure in the infrastructure continues to increase. Three compelling factors drive the need to evaluate and mitigate the overall risks associated with GIAC's primary data center:

1. The increased dependence on information systems to sustain normal business operations;
2. The growing risk of facility related technology failures; and
3. Gaps between current disaster recovery capabilities and business requirements for information systems availability (facility, business planning and IT).

Why the concern? If the data center is not available, business activity in all sectors of the enterprise is profoundly impacted. The data center is the single point of failure that all remining infrastructre depends (hardware, networks, operating systems applications and data). Best estimates of impacts for each day the data center is down include:

- $1.7m in lost productivity;
- Lost good-will with the state and federal government, business partners, customers and providers;

- 2.7M business transactions do not occur;
- Business projects delayed;
- Media attention;
- Liability Risk;
- Loss of revenue; and
- Interest, fines and penalties associated with service level agreements and contracts.

Recommendations on GIAC's Primary Data Center:

GIAC's data center must support its strategic imperatives around customers needs and providing service to and strengthening relationships with health care professionals. To meet these objectives, GIAC's data center must be highly available, with redundant components (e.g., electrical, air cooling) to meet the criteria of a hardened Tier III data center. [2] The data center should:

1. Be constructed as a data center (not a multi-purpose facility);
2. Have capacity to accommodate future growth and 5 generations of new technology;
3. Be structurally sound to prevent damage from a class 4 hurricane (highest natural risk in the southeast) to include hardened structures for backup and enabling systems (cooling tower, generators, UPS);
4. Not be located in close proximity to a major transportation mode (highway, railroad, flight path);
5. Be a low profile, non branded facility to reduce the potential of targeted attacks;
6. Have high perimeter and access security to restrict access by unauthorized personnel; and
7. Have adequate protection from flooding.

To meet the necessary requirements, GIAC must build a new data center. The existing data center is out of site infrastructure capacity (mechanical and electrical), lacks fault tolerance, has little concurrent maintainability, low heat density and multiple single points of failure--it is at the end of its useful life. It is estimated that 24 months are required to design, construct, test and occupy a new data center.

GIAC risk exposure during this time is too high to postpone remediation efforts. It is recognized that data center remediation efforts have a high potential for negative impacts and must be carefully planned to avoid unintended outages. In view of this, short-term improvements to the existing facility must be limited to those areas where risk can be significantly reduced at a reasonable cost. Improvements to the electrical infrastructure must be based on the highest exposure to the organization.

[2] Based on ComputerSite Engineering Inc. detailed requirements for evaluating the mechanical and electrical environments for reliable data centers.

In summary, there are a number of short-term improvements that are needed to strengthen emergency power provisions, provide power redundancy and mitigate major risks. GIAC's Facility Services must develop immediate plans to implement the following changes:

1. Install a bilge pumping system to expel water from the switch-gear room in the event of flooding (4Q03);
2. Install a connection point to hook up truck portable emergency generators and keep one or more generators on reserve (1Q04);
3. Order and hold switch gear replacement components for items that are deemed most likely to fail (1Q04);
4. Add redundant UPS capability (1Q04);
5. Replace aging batteries and establish routine testing schedule (1Q04);
6. Reconfigure battery string into two separate circuits to protect against a single battery failure faulting the system (1Q04); and
7. Replace the two generators supporting the data center with higher capacity and redundancy 2Q04).

Risk # 2: Storage Architecture: Data Storage, Retention and Recovery

Based on a heightened sense of concern with vulnerabilities present in GIAC's data center, the next area of assessment and presumed risk was the overall disaster recovery capabilities. Recent disaster recovery (DR) testing and preparations for Hurricane Isabel re-surfaced vulnerabilities and highlighted major gaps in existing capabilities with regard to data storage and recovery.

GIAC's Information Technology's Storage Management Group manages approximately 200 TB data in its environment today. Based on the high volume of data, It is estimated that 44,000 tapes would need to be prepared and shipped to GIAC's hot site for business recovery. This would result in packaging and shipping 44 pallets of tapes, which could require a semi for transportation. Considering approximately 3% - 5% failure rate on tapes, GIAC is certain to be lacking critical data for a full restoration. When tapes are emptied out of silos (which is GIAC's disaster recovery strategy) the set of primary tapes are shipped to hot site (800 miles away) for restoration. No additional back-ups are available thereby leaving GIAC exposed. Back ups for critical applications and data bases are not consistently running to successful completion. Application owners routinely make changes after back-ups have been completed. There are no audit process in place to ensure full back ups.

Growing cost and shrinking budgets have not enabled GIAC to keep pace with growth and demand. New technology and methods have been introduced into the market that merit evaluation (e.g., mirroring, adaptive copy, tiered data structure). The user population, and some application owners in the distributed environment, manage their own data backups and are not covered as part of GIAC's existing disaster recovery plan or hot site contract. In these scenarios, reliability of data

back-ups are uncertain. There are significant gaps between customers expectations vs. validated needs (and willingness to pay) for recovery time and recovery point objectives (seconds, minutes, hours...not at all).

New, more stringent, data retention requirements are emerging as part of HIPAA requirement for 6 years retention of personal health information (PHI). Since GIAC is in the process of developing requirements to build a new Tier III data center, they need to develop a more robust storage architecture to align with the new Data Center Strategy and determine how storage and recovery strategies affect the emerging data center requirements.

In summary, GIAC must develop a new approach to data storage, retention, back-up and recovery. GIAC's tape and restore DR strategy has lived beyond its useful life and a new storage architecture must be developed. This new architecture must:

1. Align recovery strategies with agreed upon business priorities while balancing solution cost and complexity;
2. Improve efficiency by optimizing storage processes, technology and human resources;
3. Enable physical and logical segmentation of assets (hardware, operating systems, application and data) into multiple tiers for data back-up schedules, methods, media and recovery time/point objectives (RTP/RPO);
4. Develop recommendations for immediate improvements to reliability of existing recovery plans; and
5. Ensure HIPAA compliance for data retention and recoverability by April, 2005.

The risk of not completing this effort puts the business recovery capability, and therefore the survival of the enterprise, at an unacceptable risk. While an overall architecture is under development, GIAC must make immediate steps to improve reliability of existing storage, back-up and recovery capabilities to insure business recovery following an adverse event.

Recommendations for data storage, retention and recovery:

The following action plan must be implemented by end of the fourth Quarter 2003 to strengthen existing recovery capabilities:

1. Audit Tivoli Storage Management (TSM) people, process and technical environment to determine cause of specific failures in recent DR test where TSM could not be restored at all and implement immediate improvements (12/03);
2. Order surge capacity of storage media (Raven tapes and 9490's) to provide redundant copies of back tapes if DR tape shipment is activated (11/04);

3. Evaluate criticality of data stored in TSM to eliminate DR back-ups of non critical data and reduce requirements for shipping (1Q04);
4. Audit tape back-ups over 4 consecutive weeks to demonstrate ability to complete full-backups and identify gaps for immediate closure (12/04); and
5. To validate effectiveness of improvements, conduct an interim "mini" DR test in November, 2003.
6. To increase ability to complete nightly backup jobs, implement capacity upgrades by adding 3TB DASD, one Z-900 processor, new channels and director ports for processor (11/03); and
7. Add two additional storage administrators to ensure adequate resources are available to complete and properly archive data (11/03).

Risk # 3: Intrusion Detection, Prevention and Incident Response

The financial impact of security breaches has escalated dramatically in recent years and security threats are growing in numbers and sophistication.[3] Howard Schmidt, President Bush's Cyber Security Advisor, stated: "Cyber crime is costing the world economy billions of dollars and is on the increase. We have a great deal of focus nowadays on weapons of mass destruction, but we need to be aware of the proliferation in cyberspace of weapons of mass disruption".

GIAC's business is rapidly migrating to web based capabilities. A self service model for customers, health care providers and the distribution channel is a critical strategic objective. As GIAC strives to rapidly externalize information, business processes and capabilities, it must take extraordinary measures to protect private and confidential information from inappropriate disclosure or accept significant risk for litigation and penalties. Furthermore, it must prevent external parties (or misinformed or misguided internal ones) from exploiting vulnerabilities in GIAC's internal network and information infrastructure. While GIAC is less likely to be the victim of a targeted attack, it must defend itself from the major threats of pervasive and unrelenting hacker attempts on its network. These attempts arrive from the internet in the form of Denial of Service (DOS) attacks and malicious code.

An organization's defense is hardened by intrusion prevention, detection and response components which include mature processes and capabilities surrounding:
1. Penetration Testing
2. Ongoing Vulnerability and Risk Assessments
3. Network Based Intrusion Detection (NIDS)
4. Host Based Intrusion Detection (HIDS)
5. IDS Management and DSS Reporting
6. CSIRT Notification
7. Detection of Malicious code and Viruses
8. Data Integrity Assurance

[3] *CSI/FBI Computer Crime and Security Survey, April, 2002*

Like most organizations, GIAC has implemented multiple tools and processes around intrusion detection and prevention. These include technologies to monitor the infrastructure for vulnerabilities, detect violations of security policy, provide alerts to response teams, and provide necessary logging for audits or interference with system operations in an information system. Unfortunately, a slow evolution of GIAC's intrusion detection, prevention and response capabilities has resulted in incomplete and inadequate protection with siloed/fragmented roles and responsibilities. The following summarizes the high level gaps discovered as part of this assessment:

1. **Technical environment:**
   - Intrusion detection is only applied at the Internet border—it is not applied to frame relay, internal server farm or the Extranet.
   - GIAC does not have intrusion sensors on internal routers in each of its multiple facilities.
   - GIAC has insufficient licenses of NetForensics to cover the critical resources and provide access to who need it.
   - Due to limited server capacity, reporting capabilities are limited to 5 days or less and raw (log) data is only retained for 90 days. This significantly limits GIAC's ability to do trending, pattern analysis and tuning to minimize false positives and false negatives.
2. **Safeguards for "trusted" entities**:
   - Many of GIAC's employees have lap top computers or utilize remote access capabilities to work from home or while traveling. This exposes GIAC to virus or malicious code that could be "innocently" introduced from individuals home or lap top computers that may have inadequate virus protection. For example, the individual could have no personal firewall, be back-leveled or fail to apply patches.
3. **Testing**:
   - GIAC conducts 2 internal and 2 external penetration tests per year. However, staff is notified of the upcoming tests and instructed not to intervene if the penetration test is detected.
   - This prevents GIAC from testing response capabilities to ensure it can trap or deflect attempted penetrations and collect appropriate evidence from an intruder's action.
4. **Workforce**:
   - Individuals responsible for intrusion detection are also responsible for network operations, performance and availability. One individual indicated that "security here is a hobby – it is not anyone's job".
   - There is no monitoring coverage 24X7.
   - GIAC lacks focused training and continuous learning for key security individuals in the organization.
5. **Organizational alignment**:
   - Process and accountabilities are diffused with multiple I/T organizations, Internal Audit, Computer Security and the business units.

- Organizational responsibilities are not understood. Hand-offs are frequent and often clumsy resulting in delays, missteps and gaps.

6. **Processes:**
   - Issue escalation and tracking processes are primarily informal, lack documentation and are not understood by the very people intended to use them.
   - There is no agreed upon emergency escalation process that authorizes network or component shut down in rapid response to detected penetrations or other security risks.
7. **Leadership / Strategy:**
   - GIAC has no agreed upon strategy or target architecture for intrusion, prevention, detection and response. This has resulted in haphazard and disconnected management approach.

Recommendations on Intrusion prevention, detection and response:

GIAC must take both immediate and mid-term steps to mature its Intrusion prevention, detection and response capabilities. These steps should include:

1. **Fortify Technical Environment**:
   - Upgrade server and storage capacity for logging network intrusion detection activities by 4Q03.
   - Implement version 3.1 of NetForensics by 4Q03.
   - Acquire additional licenses to enable monitoring of internal network devices (beyond Internet border) by 4Q03.
   - Implement intrusion sensors on routers in every one of GIAC's multiple facilities to detect malicious code introduced by employees to internal network (e.g., from lap-tops) by 1Q04.
   - Assess the portfolio of security products and capabilities currently in house to identify gaps and overlaps by 1Q04.
2. **Leadership/Strategy**:
   - Document and gain agreement on enterprise security objectives and requirements to assure shared understanding of the targeted security posture and articulation of how secure GIAC needs to be to protect confidential information by 1Q04.
   - Benchmark industry best practices and product capabilities regarding intrusion prevention, detection and response and complete risk/gap analysis to prioritize and sequence improvements by 2Q04.
   - Develop and distribute a detailed security sub-architecture for intrusion prevention, detection and logging/monitoring which defines inter-relationships of all components by 2Q04.
3. **Processes and Policies:**
   - Develop clear escalation process for detected security breaches with defined authority levels to shut-down the network or lock down processes for infrastructure components by4Q03.

- Update or develop an end-to-end set of policies, procedures and formal processes for intrusion prevention, detection and response with clearly defined roles and responsibilities by 2Q04.
- Require that GIAC employees who use lap-tops or remote computing access have adequate firewall and current anti-virus protection capabilities and monitor compliance by 1Q04.
- Implement sanctions for employees that introduce malicious code into environment by 4Q03.

4. Workforce:

- Identify dedicated resources for intrusion detection, logging, monitoring, and incident response management whenever the network is operational (24X7) by 1Q04.
- Develop training and development plans to enable security staff to stay current with industry best practices and technology operating in GIAC's environment by 1Q04.
- Require critical staff to pursue and obtain industry recognized credentials in their field of expertise (e.g., GIAC, Microsoft, Cisco) 4Q04.

5. Testing

- Enhance vulnerability assessments and testing to include ability to measure end-to-end capabilities from prevention, detection response management and escalation processes by1Q04.

7. Organizational alignment

- Develop clearly defined role and responsibilities across GIAC's enterprise regarding intrusion prevention, detection and response by 1Q04.
- Define objectives and metrics for each organization involved in the "security chain" to assure GIAC that organizational learning and maturing is occurring at the desired pace (1Q04).

Assignment 3. Evaluate and Develop Security Policy

Evaluation of Security Policy

This evaluation is based on a GIAC internal policy on Enterprise Risk Management (see attachment A). This policy was selected as it is presumed it is the most applicable corporate policy that should have provided enterprise guidance and perhaps prevented the gradual decline resulting in the existing state of the enterprise data center (risk #1), the storage architecture (risk #2) and Intrusion detection, prevention and response (risk #3). The following is a summary of an evaluation of the policy effectiveness. Additionally, I will point out how the policy can be improved.

Structurally, the policy has all the right components including background, scope, policy statement, definitions, authority, roles and responsibilities. It provides a clear understanding of what the policy is intended to address, why the policy was established and to whom the policy applies. Unfortunately, the policy is extremely

vague and does not provide sufficient guidance regarding the when, how and who. There are no identified escalation processes when significant risks are identified. Authority level definition is weak. There are no expressed negative consequences or implications of failing to follow policy. The policy statement itself sounds like a mission statement of a department.

A sound policy should not simply state that "all management" is responsible for risk management – this makes no one accountable. In this case, the policy process was inappropriately used to just define and communicate a framework. Frameworks are educational processes. In the roles and responsibilities sections for example, the policy states that management is responsible for: "ensuring that personnel understand the ERM framework, use it in decision-making and escalate decisions when prudent. They are responsible for risk evaluation and controls to demonstrate conformity with the in intent of this policy."

Revise Security Policy:

Specific revisions to the Security policy are reflected in Attachment B.

Assignment 4. Develop Security Procedures

The following is a new Standard Operating Procedure (SOP) for Internet Security Vulnerability Assessment.

Policy Supported: Enterprise Risk Assessment (policy # 1.26)

Responsible Parties: I/T Protection and Controls Division along with designated subject mater experts and sub-teams.

Purpose and Timing:
The purpose of this SOP is to provide clear procedures, time-line and responsibilities for completion of an annual vulnerability assessment to coincide with release of the SANS and FBI Top 20 Internet Security Vulnerabilities. The SANS Institute and the FBI have jointly developed and released an updated list of the top 20 Internet Security Vulnerabilities (10 each for the Windows and Unix Environments). This list was developed in concert with thousands of security experts and represents a comprehensive overview including:

A. The vulnerabilities and description;
B. Identification of Operating Systems affected;
C. References of the published Common Vulnerability and Exposures;
D. An assessment approach to determine if we are vulnerable and where; and
E. Recommendations on how to protect against external threats.

The Internet Security Vulnerability assessment will be conducted in the fourth quarter of each year to determine how well GIAC is positioned against each of these 20 items. A consensus will be reached with Functional Management and IT Protection and controls management to determine if GIAC's exposure is high, medium or low. Assessment results will be published by year-end with improvement plans for high risk items due in the first quarter of the following year.

The intent of this Vulnerability Assessment is to provide a systematic examination to determine the adequacy of security measures, identify security deficiencies and to provide data from which to predict the effectiveness of proposed security measures and confirm the adequacy of such measures after implementation. This assessment is a complementary sub-set of GIAC's over-arching Security Management Program. This assessment will not replace other assessments such as quarterly penetration testing or Internet Audits. The intent is to take focused actions to improve our overall security posture as GIAC strives to better align efforts and adopt best practices.

Procedures:

- **Leadership and Planning:** On an annual basis, the VP of IT Protection and Controls will assign a Security Architect (SA) to complete the Internet Security Vulnerabilities Assessment.
- **Establish work-force:** Subject matter experts and team leads will be identified by the SA based on the vulnerabilities identified. IT Management will be notified of team composition and expectations.
- **Communication and Data Gathering**: The SA will distribute the SANS / FBI annual report to all team members along with a risk assessment template for collecting data. An assessment kick off meeting will be held to orient all participants and answer any questions. SMEs and other team members must complete the initial results within two weeks (target November, 15 of each year) and submit preliminary findings to the SA.
- **Assessment Framework and Content**: The SA and team members shall use GIAC's policy on risk management as the overall framework (see attachment B). In addition, the assessment template and final report will include the following:
    A. SANS / FBI specific Vulnerabilities (see above content);
    B. Assignment of probability of vulnerability being exploited at GIAC (likelihood of occurrence and frequency);
    C. Evaluate and document effectiveness of controls that are in place or measures designed to reduce or deter threats;
    D. Evaluate potential impact to the enterprise using the threat/risk assessment scoring methodology;
    E. Calculate the risk index of each threat;
    F. Identify additional controls that could be put in place;
    G. Calculate residual risk; and
    H. Develop conclusions and recommendations.

- **Consensus Building, Report Finalization and Distribution:** The SA will validate all assessment data with the SMEs and team members and assign an overall finding to each vulnerability (high, medium or low) based upon existing GIAC scoring methodology and criteria. A final draft of the summary report will be distributed to all team members for a two-week comment period. Disputes will be identified during this comment period with the VP of IT Protection and Controls having authority to make the final determination. The final report will be distributed during the first week of December to the CIO, Sr. IT Management, team participants and to the Vice Presidents of Internal Audit and Corporate Compliance.
- **Gap Closure and Prioritization of Improvements:**
  A. Identified functional managers (published in final report and based on area of vulnerability) will incorporate additional controls and recommendations for all vulnerabilities ranked as high and medium into Operational Plans during the first quarter following the assessment.
  B. If resource, budget or capacity issues do not permit improvements within 90 days, a supplemental budget or resource request must be developed and submitted by functional managers for prioritization by the IT Leadership Team and the CIO.
  C. A risk notification and acceptance form must be developed by functional managers for any outstanding risks where the risk index remains "high" or for any items that cannot be incorporated into annual plans.
  D. Divisional Vice Presidents must sign the Risk Acceptance form for high risk items and forward to I/T Protection and controls with copies to Audit, Risk Management and Compliance Divisions.
  E. Progress against all outstanding items from the assessment will be tracked and published quarterly by I/T Protection and Controls to ensure prompt closure of action items and on-going risk management.

Executive Summary

GIAC has made significant progress in recent years with development of an overall Security Framework and appropriate governance processes. Immediate emphasis must be place on the three high risk areas identified in this assessment:

A. GIAC's primary data center;
B. Data storage, retention and recovery; and
C. Intrusion prevention, detection and response.

In addition, GIAC should develop specific policies and clearly define roles and responsibilities across the enterprise to assure continued maturity of security disciplines and an integrated approach to manage on-going risks.

References

Sans Institute SANS Security Leadership Part 2: Infrastructure Security

Endorf, C.F. Information Security Management Handbook 4th Edition. New York: Auerbach Publications, 2003.

Sheldon, T. Encyclopedia of Networking & Telecommunications: New York: Osborne and McGraw-Hill, 2001.

Maggiora, P. and Doherty, J. Cisco Networking Simplified. Indianapolis, In: Cisco Press Inc., 2003.

ComputerSite Engineering, Inc - UpTime Institute
www.upsite.com/TUIpages/tuiwhite.html

www.cert.org

Disaster Recovery Institute (DRI)

Business Continuity Institute (GCI)

Effective Date: 8/30/02 **Policy # 1.26** **Page 1 of 4**
Review Date: 8/30/03 **Policy Name: Enterprise Risk Management**
Business Owner: John Doe, V.P. Risk Management
Authorization/Approval: Office of CEO

I. BACKGROUND

Successful operation of any business enterprise requires an understanding of the relationship between external and internal risks and the operation of that business enterprise. In order to be successful in the complex and turbulent health care environment, we need to accept risk intelligently. That requires an understanding of how business risks could impact our ability to achieve corporate objectives and support our pursuit of competitive advantage. Such a cultural competency provides assurance to the Board of Directors, sustains stakeholder value and improves operational efficiency through better decision-making.

Recognizing this, the company has implemented a new way to identify and examine the major risks our company is facing through a framework called Enterprise Risk Management (ERM). This framework for intelligent risk taking was initiated to provide a new perspective to decision making that includes the identification, evaluation, mitigation (or exploitation) and monitoring of our most significant enterprise risks. Responsibility for oversight of the company's risk management function rests with the Audit and Compliance Committee of GIAC Enterprise's Board of Directors and, ultimately, with the full Board. The Office of the CEO, business sector heads and key functional support areas identify a list of our most important business risks annually.

As managers and leaders of our company, we are responsible for effectively managing risks which could significantly affect our ability to achieve enterprise or business sector objectives. This is a basic and continuous responsibility that should be inherent in carrying out our ongoing managerial responsibilities.

II. SCOPE

This policy applies to all GIAC ENTERPRISE corporations and subsidiaries.

III. POLICY

The management of risk is an important management responsibility and a key factor to the future success of the business enterprise. Therefore, it is the policy of

GIAC ENTERPRISE that all management decisions will include the identification, evaluation and management of all associated ERM risks**.**

ERM is not a new procedure but an enhancement to existing decision-making methods. Therefore, the Enterprise Risk Management Framework will be embedded into other, existing processes like strategic planning, project management, business planning and operational planning.

Risk Identification and evaluation tools are provided but may not be applicable to all business decisions. The ERM framework may be executed using a number of means as long as decisions include this four-step method as part of decision making.

IV. DEFINITIONS

(See Exhibit I)

V. AUTHORITY

This policy is established by the Office of the CEO (OCEO).

Audit, Risk Management and Compliance Division provides ERM policy monitoring and oversight, ERM implementation tools and risk financing through outside insurers or retention programs.

Authority for accepting risk on behalf of the organization, subject to the requirements of existing management controls (e.g.,, check authorization) is the responsibility of its management.

VI. ROLES AND RESPONSIBILITIES

GIAC ENTERPRISE Board of Directors
Ultimate oversight of GIAC Enterprise's risk management function.

Audit and Compliance Committee, GIAC ENTERPRISE Board of Directors
Oversight of GIAC Enterprise's risk management function with particular focus on company processes for management of enterprise risks.

Office of the CEO
Establishment of this Risk Management policy.

Office of the CEO, business sector heads and key functional support areas
Determination of Enterprise Risks

Audit, Risk Management and Compliance Division

The A&C Division will act as consultants to management for their assessment and management of Enterprise Level Risk. The Audit, Risk Management and Compliance Department is responsible for:

- Managing the annual enterprise risk assessment
- Evaluation of departmental compliance with this policy through routine review of financial and operational controls.
- Development of specific requirements for existing processes that will support the Enterprise Risk Management framework.
- Training and education necessary to develop management's cultural competency for intelligent risk taking.
- Risk financing programs that support the mitigation/exploitation of Enterprise Risks.
- Establishment of ERM metrics and associated management reporting.

Management

Responsibility for compliance with this policy rests with company management. This includes ensuring that personnel understand the ERM framework, use it in decision-making and escalate decisions when prudent. They are responsible for risk evaluation and controls to demonstrate conformity with the intent of this policy.

VII. ATTACHMENTS AND ADDITIONAL INFORMATION

Risk Management Intranet Web site: ***http://riskmanagement.GIAC Enterprise.com/***

- Enterprise Risks including Descriptions and Explanations
- Enterprise Risk Management Assessment Tool
- Risk Assessment Impact Scale
- Definitions

Exhibit I:

Definitions

Enterprise Risks
A list of risks, determined annually by OCEO, business sector heads and key functional support areas, which reflect the most serious impacts to corporate objectives.

Enterprise Risk Management
A rigorous approach to assessing and addressing the risks from all sources that significantly impact the achievement of corporate objectives

Enterprise Risk Management Framework
A construct for examining risks in order to support existing decision making processes. The framework has a four-step process: Risk identification, evaluation, mitigation (or exploitation) and monitoring.

Risk Identification
The first step of the ERM Framework requires an introspective examination of the project, issue or task at hand and how it relates, or could potentially relate, to the ERM risks.

Risk Evaluation
The second step of the four step ERM framework, evaluation is a written assessment of the (1) likelihood of the risk occurring and (2) the potential impact upon the enterprise. Risk Evaluation creates a deeper understanding of the relationship the ERM risks have to the project, issue or task at hand.

Risk Mitigation/Competitive Advantage
Steps taken to control, transfer or finance the potential effects from accepting a risk. This third step of the ERM Framework presents an opportunity to consider the positive aspects of risk acceptance and how intelligent risk taking can support the organization's pursuit of competitive advantage.

Risk Monitoring
A specific process to evaluate the effectiveness of risk mitigation efforts.

Loss
A reduction in current or future value of corporate assets - tangible or intangible.

Subsidiary
Any corporation where GIAC ENTERPRISE owns more than 50 per cent of the issued and outstanding stock either directly or indirectly through one or more of its subsidiaries.

GIAC Enterprise Policy Attachment B

Effective Date: 11/01/03 **Policy # 1.26** **Page 1 of 5**
Review Date: 11/01/04 **Policy Name: Enterprise Risk Management**
Business Owner: John Doe V.P. Risk Management
Authorization/Approval: Office of CEO

I. BACKGROUND

Successful operation of any business enterprise requires an understanding of the relationship between external and internal risks and the operation of that business enterprise. In order to be successful in the complex and turbulent health care environment, we need to accept risk intelligently. That requires an understanding of how business risks could impact our ability to achieve corporate objectives and support our pursuit of competitive advantage. Such a cultural competency provides assurance to the Board of Directors, sustains stakeholder value and improves operational efficiency through better decision-making. Additionally, accountabilities must be clearly defined so that risks are identified and managed on a daily basis and that escalation process are in place to ensure that significant risks which cannot be mitigated are surfaced promptly to the appropriate decision making authority.

Recognizing this, the company has implemented a new way to identify and examine the major risks our company is facing through a framework called Enterprise Risk Management (ERM). This framework for intelligent risk taking was initiated to provide a new perspective to decision making that includes the identification, evaluation, mitigation (or exploitation) and monitoring of our most significant enterprise risks. Responsibility for oversight of the company's risk management function rests with the Audit and Compliance Committee of GIAC Enterprise 's Board of Directors and, ultimately, with the full Board. The Office of the CEO, business sector heads and key functional support areas identify a list of our most important business risks annually.

As managers and leaders of our company, we are responsible for effectively managing risks that could significantly affect our ability to achieve enterprise or business sector objectives. This is a basic and continuous responsibility that should be inherent in carrying out our ongoing managerial responsibilities. Every manager is responsible for identification and evaluation of risks within their area of accountability. These risks should be evaluated and prioritized annually for incorporation into divisional operating plans**.**

II. SCOPE

This policy applies to all GIAC ENTERPRISE corporations and subsidiaries.

III. POLICY

The management of risk is an important management responsibility and a key factor to the future success of the business enterprise. Therefore, it is the policy of GIAC Enterprise that all management decisions include the identification, evaluation and management of all associated ERM risks.

ERM is not a new procedure but an enhancement to existing decision-making methods. Therefore, the Enterprise Risk Management Framework will be embedded into other, existing processes like strategic planning, project management, business planning and operational planning.

Risk Identification and evaluation tools are provided but may not be applicable to all business decisions. The ERM framework may be executed using a number of means - as long as decisions include this four-step method as part of decision making.

Risks and mitigation plans will be incorporated into annual planning process for each division as and every project that is initiated at GIAC.

Annual risk management plans for each division will be reviewed for completeness and review of relevant action plans by the Risk Management division.

IV. DEFINITIONS

(See Exhibit I)

V. AUTHORITY

This policy is established by the Office of the CEO (OCEO).

Ownership for compliance this policy rests with VP of Audit and Compliance at an enterprise level and with the VP of IT Protection and Controls for all Information Technology.

Authority for accepting risk on behalf of the organization, subject to the requirements of existing management controls (e.g., check authorization) is the responsibility of its management. When objective criteria (e.g., financial exposure) cannot be used to evaluate significance of risk, management should use the risk assessment procedures and surface risks to the immediate Director. Using the risk assessment scoring methodology, any risk rated as “high” must be approved by the area Vice President for acceptance if adequate controls are not feasible for prompt implementation.

All Corporate controllership functions are responsible to ensure that ERM is included in each functional review step (Plans, budgets, Project Plans, System design).

Audit, Risk Management and Compliance Division provides ERM policy monitoring and oversight, ERM implementation tools and risk financing through outside insurers or retention programs.

VII. ROLES AND RESPONSIBILITIES

GIAC ENTERPRISE Board of Directors - Ultimate oversight of GIAC Enterprise's risk management function.

Audit and Compliance Committee, GIAC ENTERPRISE Board of Directors - Oversight of GIAC Enterprise 's risk management function with particular focus on company processes for management of enterprise risks.

Office of the CEO - Establishment of this Risk Management policy.

Office of the CEO, business sector heads and key functional support areas – Annual Determination of Enterprise Risks and assures development of plans to address.

Audit, Risk Management and Compliance Division - Acts as consultants to management for their assessment and management of Enterprise Level Risk. The Audit, Risk Management and Compliance Department is responsible for:

- Managing the annual enterprise risk assessment
- Evaluation of departmental compliance with this policy through routine review of financial and operational controls.
- Development of specific requirements for existing processes that will support the Enterprise Risk Management framework.
- Training and education necessary to develop management's cultural competency for intelligent risk taking.
- Risk financing programs that support the mitigation/exploitation of Enterprise Risks.
- Establishment of ERM metrics and associated management reporting.

Enterprise Security Council (ESC) – a multi-dimensional task force representing all security disciplines, (computer security, physical security, personnel security, risk management and IT Protection and Controls). The ESC will review operating plans for all dimensions of security, review the results of all internal and external audits and is responsible for development on an integrated enterprise Security plan for GIAC.

Information Systems Security Steering Committee (ISSC)- a sub-committee of the ESC, this group has oversight for all improvement efforts, plans and audits related to information systems security. All risk assessments related to information and technology systems are referred to this group for planning and action. This

committee develops and approves enterprise policy for information systems security.

Corporate Security Officer / VP IT Protection and Controls. Chair the ESC and is responsible for integrated planning and improvement prioritization based on all internal and external audits, penetration testing and vulnerability assessments (e.g., Annual Internet Security Vulnerability Assessment). Accountable for execution of annual IT risk evaluation for all I/T and has ownership for compliance with this policy for the entire IT organization.

Enterprise Risk Task Force(s) - A multi-disciplined task force(s) will be established for each of the 10 identified enterprise risks. The task forces are responsible for developing a plan of action within 90 days for submission to GIAC's OCEO.

Functional Management - Responsibility for compliance with this policy rests with company management. This includes ensuring that personnel understand the ERM framework, use it in decision-making and escalate decisions when beyond authority levels of when assessment results in high risk items. They are responsible for risk evaluation and controls to demonstrate conformity with the intent of this policy. They are also responsible to obtain approval where they have accepted a risk unilaterally and when that risk will have a direct impact on another department or division.

Process owners - Responsibility for incorporating risk management methods and frameworks into corporate process and for educating process users are the responsibility of each of the individual process owners (project management, planning, I/T).

VIII. Compliance

- Failure to comply with this policy shall result in corrective action up to and including termination.
- Failure to submit annual risk assessment will result in delays in approving annual plan and budget.
- No capability or business application can be implemented into production without submission and approval of the risk management and security plan.

VIII. ATTACHMENTS AND ADDITIONAL INFORMATION

A. Threat and Risk Assessment Criteria: The following Threat and Risk Assessment material is taken directly from an internal GIAC instruction process and is intended to provide guidance on how to evaluate the impact to GIAC.

1-2- Very low:

- Funds required to repair processes or systems, would not impair critical functions, No significant liability or threats to corporate image

3-4 - Low:

- Negative income statement impact of less than 1% of net income. Inconvenient impact upon critical functions, compliance issues could be easily resolved without significant financial consequences. Small and temporary impact to corporate image.

5-6 - Medium:

- Negative income statement impact of 3% of net income. Critical business functions impaired to where customer service significantly deteriorates. Opportunity for significant liability or impairs ability to meet regulatory expectations. Rating agency position hindered such that the rating is driven down. Business practices significantly inconsistent with industry standards

7-8 - High:

- Negative income statement impact of more than 3%. Serious threats to critical business functions for the long term. Regulatory penalties or potential restructuring required. Serious liability (lawsuits) potential. Financial ratings drastically hindered or withdrawn. Long term brand equity impairment

9-10 - Very high:

- Balance sheet or income statement impact catastrophic. Liability threats challenge the going concern status of the organization. Critical business functions impaired for a long term such that the organization may face forced sale

Likelihood of Occurrence (time Frequency or how likely)

Time/ Frequency	How Likely?
10 = daily	10 will happen
9 = weekly	7 - 8 extremely likely
8 = monthly	6 - 7 very likely
7 = quarterly	5 - 6 likely
6 = bi-annually	3 - 4 possible
5 = several times/year	1 - 2 very slight likelihood
4 = once/year	0 not
3 = once/5 years	
2 = once/10 years	
1 = seldom, none to date	

Effectiveness of Controls

To what extent do the controls in place reduce the potential impact and / or likelihood of occurrence of this risk?

91% - 100% - excellent control
71% - 90% - very good control
51% – 70% - adequate / good control
31% – 50% - some control
10% - 30% - poor control
0% no control

Risk Index

The risk index can be calculated by multiplying the (Impact) X (Likelihood) minus the % of control. Depending on the number and complexity of risk, departmental management needs to determine the cut off point. As a general rule, any score over 20 merits a high risk.

- Risk Management Intranet site: ***http://riskmanagement.GIAC Enterprise.com/***
- Enterprise Risks including Descriptions and Explanations
- Enterprise Risk Management Assessment Tool
- Risk Assessment Impact Scale
- Definitions

Exhibit I:

Definitions

Enterprise Risks
A list of risks, determined annually by OCEO, business sector heads and key functional support areas, which reflect the most serious impacts to corporate objectives.

Enterprise Risk Management
A rigorous approach to assessing and addressing the risks from all sources that significantly impact the achievement of corporate objectives

Enterprise Risk Management Framework
A construct for examining risks in order to support existing decision making processes. The framework has a four-step process: risk identification, evaluation, mitigation (or exploitation) and monitoring.

Risk Identification
The first step of the ERM Framework requires an introspective examination of the project, issue or task at hand and how it relates, or could potentially relate, to the ERM risks.

Risk Evaluation
The second step of the four step ERM framework, evaluation is a written assessment of the (1) likelihood of the risk occurring, and (2) the potential impact upon the enterprise. Risk Evaluation creates a deeper understanding of the relationship the ERM risks have to the project, issue or task at hand.

Risk Mitigation/Competitive Advantage
Steps taken to control, transfer or finance the potential effects from accepting a risk. This third step of the ERM Framework presents an opportunity to consider the positive aspects of risk acceptance and how intelligent risk taking can support the organization's pursuit of competitive advantage.

Risk Monitoring
A specific process to evaluate the effectiveness of risk mitigation efforts.

Loss
A reduction in current or future value of corporate assets - tangible or intangible.

Subsidiary
Any corporation where GIAC ENTERPRISE owns more than 50 per cent of the issued and outstanding stock either directly or indirectly through one or more of its subsidiaries