Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

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

GIAC Certified Security Consultant

Practical Assignment

Version 1.0.

Presented by: Kevin B. Fiscus
August 20, 2004

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

© SANS Institute 2004, Author retains full rights

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Abstract/Summary

This assignment involves KBF Consulting, a fictional IT consulting firm with 25 employees. In this scenario, KBF Consulting has been contacted by GIAC Enterprises, a large publishing firm who is seeking to have a security assessment performed. This assignment involves the development of work product following the sales process including:

- The documentation of the KBF Consulting methodology and approach
- The development of a sales proposal and a sales pitch
- Project performance documentation including a project plan, meeting/interview facilitation ideas, a discussion of potential project pitfalls or problems and areas where, during the course of the project, the client's expectations can be exceeded
- An example of the final project deliverable

The following document contains the results of this assignment as directed by the GIAC Certified Security Consultant (GCSC) Practical Assignment, Version 1.0 (April 19, 2004).

Part 1 - Methodology and Approach

1. KBF Consulting Overview

1.1. The Company

KBF Consulting is an IT engineering and consulting form specializing in IT infrastructure builds, assessments and upgrades. KBF Consulting has four practice areas:

- **Networking** - The networking practice focuses on LAN/WAN network infrastructure, IP Telephony, network convergence and remote access solutions.
- **Systems** - The systems group focuses on highly available web co-location builds, network operating system infrastructure design, directory services and enterprise applications such as email and document management systems.
- **Application Development** - The application development group focuses on building web-based applications based in Java and Microsoft .net technologies.
- **Information Security** – The information security group focuses on security assessment, the design, enterprise-level security program design, security product implementation and security operations support.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

1.2. Staffing

KBF Consulting utilizes resources from all practices as needed to complete its engagements leveraging its certified expertise in networking, systems, development and information security. KBF Consulting consultants are certified by both technology vendors and by independent certification authorities. Certifications held by KBF Consulting personnel include:

- Certified Information Systems Security Professional (CISSP) – International Information Systems Security Certification Consortium (ISC)2[i]
- Cisco Certified Internetworking Expert (CCIE) – Cisco Systems[ii]
- Cisco Certified Network Professional (CCNP) – Cisco Systems[iii]
- Cisco Certified Design Professional (CCDP) – Cisco Systems[iv]
- Microsoft Certified Systems Engineer (MCSE) – Microsoft Corporation[v]
- Microsoft Certified Solutions Developer (MCSD) – Microsoft Corporation[vi]
- Microsoft Certified Application Developer (MCAD) – Microsoft Corporation[vii]
- Microsoft Certified Database Administrator (MCDBA) – Microsoft Corporation[viii]
- Sun Certified Systems Administrator (SCSA) – Sun Microsystems[ix]
- Sun Certified Network Administrator (SCNA) – Sun Microsystems[x]
- RSA Certified Security Engineer – SecurID (RCSE) – RSA Security[xi]
- RSA Certified Security Engineer – ClearTrust (RCSE) – RSA Security[xii]
- GIAC Certified Forensics Analyst (GCFA) – Global Information Assurance Corporation[xiii]
- Project Management Professional (PMP) – Project Management Institute[xiv]

1.3. Products and Services

In addition to its experienced consultants, KBF Consulting has developed a robust suite of security services. These services revolve around the concept that information security is an ongoing process designed to achieve an acceptable level of risk. Information security involves all of the actions taken to protect an organizations data and related assets. This includes the protection of corporate intellectual property and other sensitive material. Also included are the computers, network devices, cables and other hardware necessary to store, process and transmit data. The reach of information security extends to the realm of physical security where physical security affects the protection of information assets.

KBF Consulting has developed a detailed approach to information security revolving around the concept that information security is an ongoing process as illustrated in the following diagram.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

The four-phase security process begins with the assessment phase. This phase involves reviewing the state of security to determine if existing risks are acceptable. In the event the assessment reveals that the existing security program is completely adequate, the process returns directly to the operations phase. Given the dynamic state of both business and information security, it is more likely that the assessment phase will reveal that modifications to the overall security program are necessary.

The planning for such modifications occurs in the design phase. This phase focuses on functionality and process requirements rather than on specific products. The results of the design phase are a set of requirements to be used in the implementation phase.

During the implementation phase the requirements established in the design phase are used to identify where modifications are required. These modifications may include the implementation of products, process or policy. The products and processes are fully planned, implemented and integrated into the operational environment in this phase.

After implementation, the security process enters the operations phase. This phase involves the operations of security technology, the performance of security processes and the day-to-day involvement of organizational personnel in the protection of information assets.

As illustrated in the “Information Security Process” diagram, the security program does not stop at operations, rather it continually returns to the assessment phase. This occurs in two circumstances. The assessment phase is initiated at regularly scheduled timeframes to ensure that security remains in line with current business and security objectives. The assessment phase is also initiated because of an event such as a security breach, the publication of a new vulnerability or the implementation of a new technology. As the assessment phase is initiated, the security process in its entirety begins again.

KBF Consulting has developed a comprehensive suite of security services that correspond with the security process and allow KBF to assist its clients in the

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

development and fulfillment of a comprehensive, strategic information security program. This allows KBF to utilize a standard approach to develop a highly customized and flexible security program that reduces risks to a level commensurate with individual client needs. In turn, our clients will be able to implement a security program that meets their current requirements and can adapt to future changes in business and security requirements.

The following are the standard security services offered by KBF Consulting.

Assessment Services:
- Network Security Assessment
- Systems Security Assessment
- Security Operations Assessment
- Vulnerability Assessment
- Risk Assessment

Design Services:
- Security Program Design
- Security Roadmap Development
- Secure Network Architecture Design

Integration Services:
- Policy / Standards Development
- Systems / Device Hardening
- Intrusion Detection
- Integrity Verification
- Event Correlation
- Firewall
- IPSec VPN
- Clientless SSL VPN
- Strong Authentication
- Web Access Management (SSO)
- Anti-Virus Software
- Anti-Virus Gateway
- Anti-Spam Software
- Anti-Spam Gateway
- Content Inspecting and Filtering
- Intrusion Prevention
- PKI
- Secure Messaging
- Database Encryption
- File System Encryption

Security Operations Support:
- Incident Response
- Investigations/Forensics
- Security Awareness
- Monitor / IDS Tuning
- Rogue Wireless Detection
- Information Security Audit
- Managed Security Services

2. GIAC Enterprises Overview

GIAC Enterprises is a publishing company that produces a wide range of electronic news and information as well as print publications. The organization has approximately 7,000 employees and a global reach with reporters and field offices located in the United States and throughout numerous countries. Their corporate headquarters and data processing/IT operations are located in the mid-western United States with another major operations facility in New York City.

As a publishing company, GIAC Enterprises has all the security concerns of traditional corporations including the protection of financial, human resources and

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

other mission critical applications. In addition, GIAC Enterprises has reporters submitting time sensitive stories for publication. The confidentiality, availability and integrity of the submitted stories must be maintained. At the same time, the reporters are averse to many traditional security technologies such as strong authentication and encryption. GIAC Enterprises is also concerned about their compliance with the recently enacted Sarbanes-Oxley[xv] regulation.

GIAC Enterprises has realized that their traditional method of addressing security on a tactical, project-by-project basis has been somewhat effective but does not scale and will not be effective into the future. They are attempting to address these concerns by designing a strategic information security program.

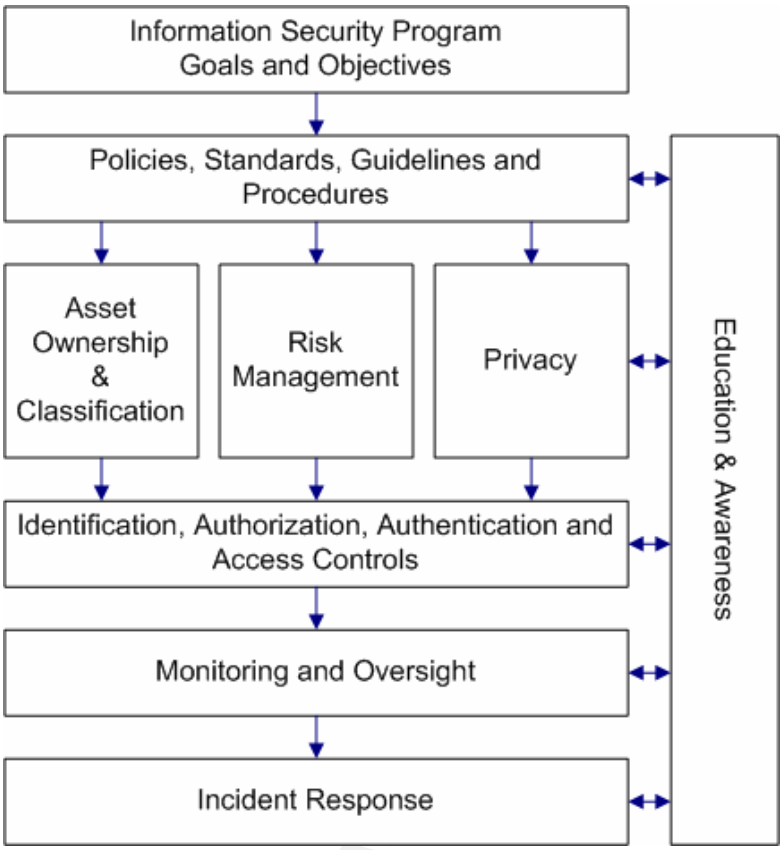
3. Methodology & Approach

3.1. Base Security Framework

KBF Consulting takes a process and goal oriented approach to information security. Rather than acquiring and implementing technology to fulfill a perceived need, KBF Consulting focuses on the goal of risk management. Risk management seeks to apply controls appropriate to the level of risk. The following diagram illustrates the major components of the KBF Consulting standard information security program.

This framework was developed by the KBF Consulting Information Security Group based in industry standards including ISO17799[xvi] and material from SANS[xvii], the National Security Agency (NSA)[xviii], the National Institute of Standards and Technology (NIST)[xix], the Center for Internet Security (CIS)[xx], the Department of Energy[xxi] and the United States General Accounting Office (GAO)[xxii]. While the KBF Consulting approach is derived from industry standards and commonly accepted “best practices” it has been tempered and modified by KBF Consulting’s extensive real-world experience. This framework is used because it provides sufficient strength to be useful and adequate flexibility to allow it to be molded into a wide variety of situations and organizations. While most of these components will be included in all security programs, the level to which each is applied will vary based on the specific business requirements of GIAC Enterprises.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.



The following sections provide a description of each of the framework components.

3.1.1. Information Security Program Goals and Objectives

The base of an information security program is a firm understanding of the goals and objectives of the organization with respect to information security. This involves determining the level of emphasis that will be applied to information security objectives and the level or risk an organization is willing to tolerate. While some organizations have high risk tolerances and thus put minimal effort toward information security initiatives, others view information security as a fundamental component of their business operations. Before developing a security program, it is necessary to determine the executive level corporate viewpoint. A statement of information security intent similar to a mission statement should be developed that defines the highest level corporate security viewpoint. This document provides the direction for the rest of the program.

3.1.2. Policies, Standards, Guidelines and Procedures

Policies, standards, guidelines and procedures are the written representation of the information security program. They define the requirement and establish the correct manner by which those requirements are to be fulfilled. The differences in these documents are a matter of scope, intended audience and the expected length of time before modification to the document is required.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Policies represent the highest level documents and are intended to provide broad guidance or set high level requirements. Policies are created to last between three and five years and are designed to provide the foundation for the remaining program documents. They are almost always enterprise in scope not referring to specific business units or technologies. Policies represent the top of the hierarchy. As such, all standards, guidelines and procedures must be in compliance with policies.

In addition to policies, which are high-level and business unit or technology independent, organizations must rely on technical or operational standards and guidelines. These documents are more detailed than policies and refer to specific technologies, applications and/or business units. Standards set requirements where guidelines provide strong recommendations. Both types of documents contain minimum secure configuration requirements and operational details for the subject addressed. Standards and guidelines will range in scope from those governing a specific business unit or technology to those involving the entire enterprise. Enterprise standards and guidelines will be less detailed than those with a more narrow focus. These documents should be created with an expected lifetime of between 1 and 2 years.

Procedures establish how the policies, standards and guidelines are to be complied with. They can be operational or technical in nature. In either case, the procedures define the actions to be taken to adequately meet the established requirements. Procedures are subject to frequent change based on business, operational or technical considerations.

3.1.3. Asset Ownership and Classification

Ownership is the concept that assigns responsibility to specific individuals or groups. Ownership must be determined for applications, information, systems, devices and security requirements. Establishing ownership serves two critical functions. First, clearly defined ownership allows individuals to be held accountable for performing their assigned security related functions. Lack of clearly defined ownership allows an individual to deny responsibility for non-compliance with established requirements. Second, ownership reduces the risk that individuals or groups will have conflicts over who has control over a specific asset or function. Lack of clearly defined ownership can lead to multiple groups attempting to comply with requirements in different ways, each assuming they have the authority to do so.

For most organizations the CEO is the ultimate owner of all assets and processes. The CEO, however, can delegate “operational ownership” to appropriate personnel who can, in turn, delegate operational ownership downward. The furthest extent to which operational ownership can be delegated is determined by the culture of the organization however end users are generally not designated as owners.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Data classification is the process by which data and related assets are grouped and labeled according to their sensitivity. Each classification group is related to a set of requirements and responsibilities that define how data is to be protected, handled, transported, stored and disposed of. Without a data classification program, it becomes the responsibility of each employee to independently determine the sensitivity of a particular piece of data and to understand how it should be handled. Formalized data classification removes much of this ambiguity and promotes proper security for data of that sensitivity.

Generally, data classification is the responsibility of the data owner or designee. Owners must define the classification that will be assigned to the various types of data within their operational unit. Owners can delegate classification labeling requirements, in accordance with established policy, to individuals including end users; however, the owner is ultimately responsible for compliance.

3.1.4. Risk Management

The primary goal of an information security program must be to reduce risk to information and related assets to an acceptable level. To be effective, the security program must act to support business operations rather than hinder to them. To these ends, an information security program will be based on the concepts of risk assessment and risk management rather than on risk elimination. A risk elimination strategy attempts to remove all risk. While, in rare cases, this may be possible, the associated costs generally far outweigh the benefits. An extreme example of this concepts involves and example of a small asteroid or meteor impact. There is a chance, however small, that a business facility will be struck and destroyed by the impact of a celestial body such as an asteroid or meteor. This type of event would be catastrophic. To eliminate this risk, a facility would need to be hardened and located under ground. This would be extremely expensive. When viewed from the perspective of the extremely small probability of such an impact, most organizations do not take such precautions. They, in effect, make the determination that the risk is acceptable. This is known as risk management. Risk management is accomplished using a process of risk assessment whereby the likelihood that a threat will exploit a vulnerability causing harm to an asset is determined. Risk assessments generally attempt to determine how much harm, expressed as a monetary figure, a security incident would cause and the number of times per year the incident could be expected to occur. This allows for the calculation of an expected annualized cost for security incidents. This cost can then be used, in conjunction with the value of the asset(s) in question to determine the resources that can be justifiably used to mitigate the perceived risk.

Risk assessments are performed to determine the level of resources appropriate for risk mitigation. These assessments must be factored into each and every aspect of business operations where information or technology is involved. While it is possible to conduct a risk assessment each time a change is made to

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

the computing environment, this is often not feasible nor is it necessary. Many situations can be considered in advance of their occurrence and thus proactive risk assessment and mitigation strategies can be developed. These proactive risk mitigation decisions can then be documented in the form of security policies, standards, guidelines and procedures. Once created, policies and standards provide the instructions for reducing risk to an acceptable level. With effective policies and standards in place, a risk assessment only needs to be conducted when a situation has not been adequately addressed by the policies or when deviation from those policies is required.

3.1.5. Privacy

In today's "information age" personal information is collected, processed, stored and exchanged with increasing frequency. Of growing concern is the use to which that information is put. Most specifically, the use and control of personal information must be addressed. This applies not only to information collected about clients or customers but also to the personal information about employees. Government regulations (HIPAA[xxiii], California S.B. 1386[xxiv] et. al.) have begun to establish requirements for handling personal information. These regulations, in many cases, have also established liabilities for the mishandling of personal data. An information security program must include provisions for the identification and protection of personal information.

3.1.6. Identification, Authentication, Authorization and Access Control

At its core, information security is concerned with providing access to information to some while denying access to others. Those with a legitimate business need for access to information or services must be provided with that access. All others should be denied. These objectives are accomplished by the proper implementation of access controls. Controls include many traditional security technologies such as firewalls and passwords. They also include operational processes by which an individual is determined to have a legitimate business need for access and the processes by which such access is granted. Three concepts are critical in accomplishing adequate access control:

- **Identification** – the process by which an individual presents his identity
- **Authentication** – the process by which an individual's identity is verified
- **Authorization** – the process by which it is determined which resources an identified and authenticated individual will have access to.

3.1.7. Monitoring and Oversight

An effective information security program can not rely on good intentions to achieve adequate security. Oversight must be included in the security program to verify compliance with security requirements is being achieved. Oversight is accomplished using a combination of technical and administrative controls.

Administrative oversight is generally accomplished as part of the process of audit and review involving periodic compliance checks. These checks not only verify compliance with existing policies and standards, but also verify that existing

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

policies and procedures successfully mitigate risk to an acceptable level. The oversight function must be complemented by administrative controls whereby individuals are held accountable for compliance with security requirements. Education and awareness ensures that each individual knows the part he or she plays in security. The oversight process ensures that requirements are being complied with. For this to be effective, individuals must be held accountable for compliance. This accountability must include recognition for high levels of compliance and appropriate disciplinary action for non-compliance.

Technical oversight is accomplished by the implementation of a wide variety of tools. These tools include but are not limited to:

- System and device event logs
- Network traffic monitoring
- Application (i.e. email, ftp, etc.) monitoring
- Intrusion detection systems
- Integrity verification systems
- Event correlation

3.1.8. Incident Response

Due to the dynamic nature of information security, the complexity of the systems involved and the frequency of new vulnerability discovery, it is infeasible to attempt to eliminate the risk of a security breach. Protective measures must be supplemented with the ability to detect security incidents, log and track activities and respond to suspected security incidents in an effective and timely manner. Incident response involves those activities necessary for response preparation, response performance and follow-up. These activities will include:

- Developing network and systems documentation specifically for incident response
- Verifying monitoring and logging has been effectively implemented
- Monitoring notification and consent
- Proactively and reactively reviewing security related log and monitor data
- Performing actual incident response
- Initiating investigations
- Suggesting mitigation strategies to reduce the risk of future occurrences
- Reviewing the response process

The goals of incident response are to:

- Determine if an incident has actually occurred
- Determine if an incident presents a business continuity problem
- Promote the accumulation of accurate information relating to the security incident
- Protect privacy rights established by law or policy
- Minimize disruption to business operations
- Minimize public relations problems by ensuring accurate understanding and reporting of security incident information

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

- Allow for legal or civil recriminations against perpetrators
- Provide accurate reports and useful recommendations

"Investigations" is a sub-component of incident response and involves a detailed review of an incident in order to determine what was done, how and by whom. Investigations will involve the collection of evidence that may be used in future administrative, civil or criminal proceedings. The investigations process must be conducted with great care to preserve evidence as, once evidence has been compromised, it frequently cannot be recovered. Investigations as a component of a security program will involve a variety of technical and non-technical aspects including:

- Evidence handling
- Chain of custody maintenance
- Forensic data duplication
- Network traffic analysis
- Forensic system examination
- Legal review
- Personnel interviews

3.1.9. Education and Awareness

Many organizations have gone through the process of documenting security requirements in the form of policies and standards. All too often these documents are placed on a shelf and serving no useful purpose. For a security program to be effective, it is important that education and awareness be provided to those responsible for organizational security. This begins with the distribution of policies and standards to those governed by them. The distribution must be targeted; providing information to those requiring that information. This includes distribution to executives, managers, technical staff, security practitioners and average users as appropriate. The process cannot end with distribution. It must include education efforts that ensure recipients have received the information and understand it and its effects. People can be one of the greatest security strengths of an organization. They can also be one of the greatest weaknesses. The difference is often the level of training and awareness provided. To ensure people benefit, rather than hinder the overall security program it must include security awareness and education. The process will begin with policy and standards training and will continue as an ongoing part of daily operations. This ensures that everyone is aware of the part he or she plays in information security and has the information necessary to maintain and enhance the information security program.

3.2. KBF Consulting Methodology

KBF Consulting has developed a detailed methodology for performing its assessment and design services. This approach is designed to step through the process methodically to ensure that each component of the project is accurate and provides the foundation for subsequent steps. The approach consists of nine steps as follows:

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

3.2.1. Data Collection

To start the process KBF Consulting begins with the collection of relevant information. During this stage, KBF Consulting collects two distinctly different types of information, client data and external data. Client data consists of the information necessary to determine the client current state. The collection of client data is accomplished by reviewing documentation (i.e. diagrams, procedures, previous reports, policies, standards, etc.) and by interviewing appropriate client personnel. External data consists of relevant laws, regulations, industry standards, guidelines and benchmarks. KBF Consulting uses this information, in conjunction with KBF Consulting's real world experience, to define and document the "best practices". This information is also used to develop a set of questions and discussion points to be used when collecting client data.

3.2.2. Current State

Once sufficient data has been collected, KBF Consulting condenses and consolidates it into a clearly defined current state document. This document describes KBF Consulting's understanding of the client environment as identified by information collected in the previous stage.

3.2.3. Client Review

To ensure the accuracy and validity of the current state information, KBF Consulting submits it to appropriate client personnel for review. This ensures that there have been no misunderstandings or miscommunications resulting in inaccurate conclusions. This step is critical since the current state provides the foundation for the remainder of the KBF Consulting methodology. During the client review stage, KBF Consulting will resolve any discrepancies in order to achieve an accurate picture of the current environment. Client signoff at this stage is required before progressing.

3.2.4. "Best Practices" Documentation

Once the current state document has been approved, KBF Consulting modifies it to include "best practices" taken from the information compiled in the data collection stage of the process. Best practices are documented within the relevant section of the current state document to allow for quick and easy reference. It is important to note that these "best practices" do not represent the final outcome of the assessment. They are the result of the assimilation of the set of industry standards, guidelines, benchmarks and regulations from the data collection stage. As such they truly represent a commonly accepted best approach to be used as a benchmark against which the final recommendations will be made.

3.2.5. Gap analysis

After documenting the best practices, the gaps between best practices and the current state are identified. This gap analysis represents an unbiased statement of the identified gaps. It is important to note that the gaps do not represent the final recommendations.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

3.2.6. Recommendations

After identifying the current state, relevant best practices and gaps, KBF Consulting documents its recommendations. In some cases the recommendations may bring the client into "compliance" with identified best practices. In other cases, the recommendations will fall short of or exceed best practices as deemed necessary to fit the cultural, technical and resource availability requirements of the client. KBF Consulting's recommendations are designed to adequately and reasonably address problems identified during the assessment. In a security assessment, the recommendations are designed to reduce risk to client assets to an acceptable level. While doing so, KBF Consulting ensures that the recommendations are commensurate with the potential impact of the identified risk.

3.2.7. End State Documentation

Following the development of the findings document (including the current state information, best practices, gaps and recommendations) KBF Consulting will prepare a document describing the final goals of this initiative. This document will combine the recommendations made in the findings document in order to paint a picture of what the cumulative effect of the implementation of the full set of recommendations will look like.

3.2.8. Findings Presentation

The results of the entire assessment will be condensed into a presentation. This presentation is designed to provide a high-level overview of the findings. KBF Consulting can prepare presentations for a wide variety of audiences including executives, management and technical personnel.

3.2.9. High-Level Roadmap Development

KBF Consulting breaks the objectives of the end state document into manageable projects. These projects are then prioritized based on need, resource availability and prerequisites. The roadmap document will contain a description of each initiative and estimates for budgetary and resource requirements. The main document will be presented with a project plan identifying each initiative, priorities and dependencies. This allows for the achievement of end state goals as part of a manageable and controllable process. It also provides a vehicle for determining annual budget allotments and personnel requirements.

Part 2 - Proposal and Pitch

1. Proposal

KBF Consulting – Statement of Work

Information Security Assessment & Security Program Design

Client Name: GIAC Enterprises

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Client Contact: Mr. John Doe - CIO
Contact Phone: 111-555-5105
KBF Account Manager: Kevin Fiscus
Preparation Date: August 20, 2004

1.1. Scope of Work

GIAC Enterprises has requested a Statement of Work (SOW) from KBF Consulting to complete an Information Security Risk Assessment and security program design. Based on discussions with GIAC Enterprises executives the purpose of this project is to establish a Phase 0 that will define a scope and plan for "Project Secure" which will improve GIAC Enterprises' ability to conduct business across all of its Global Operations.

The proposed Information Security Risk Assessment will focus on three defined areas:

- Policy and Operations Review
- Network Security Assessment
- Systems Security Assessment

To be useful, the information collected in the three security reviews must be related to GIAC Enterprises business requirements. More specifically, the information from the security assessment must be expressed in terms of risk to the client organization. Risk can be defined as the likelihood that a threat will exploit a vulnerability causing harm to an asset. The factors of that definition identified by a risk assessment are "likelihood" and "harm". KBF Consulting will work with GIAC Enterprises to determine the criticality of their systems and processes in relation to any discovered vulnerabilities or weaknesses. We will then factor in potential threats to determine the risks faced by the client. Finally, we will work with GIAC Enterprises to determine which risks require mitigation and which are acceptable.

Anticipated discussion points will minimally include:

- Architecture and design of the information security program
- Integration of existing tools and technologies
- IT Operational compliance with Standard Operating Procedures
- Development of management metrics geared towards preparing GIAC Enterprises for meeting External audit requirements
- Remediation procedures
- Governance for interdepartmental escalations
- Information Technology operations, change management and security policies

The following sections describe the three security reviews:

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

1.1.1. Policy and Operations Review

Security Program Review

KBF Consulting will look at the security "big picture" to determine what makes up the GIAC Enterprises security program. We will determine the presence and effectiveness of high-level components such as change management, software development, development lifecycle, authentication, monitoring, incident response, policies, disaster recovery, business continuity or contingency planning, education, training and physical security.

KBF Consulting will assess the existing level of security governance and accountability in place to ensure security measures are properly implemented. KBF Consulting will identify and document who is responsible for GIAC Enterprises information security, the processes by which they are held accountable for the performance of their assigned duties and the roadblocks they encounter when doing so.

KBF Consulting will evaluate the current processes for ensuring compliance with external audits and security reviews and the process by which GIAC Enterprises internally audits information security. KBF Consulting will identify and document how GIAC Enterprises prepares for, conducts, takes part in and reacts to security audits and will provide suggestions and recommendations to facilitate the successful performance of and involvement in future audits.

KBF Consulting will review the processes by which security tasks and objectives are accomplished. While reviewing security processes such as user provisioning and change management, KBF Consulting will identify and document the types and sources of input data, how that data is processed, any automation, and the types and destinations of process output data. KBF Consulting will make recommendations for streamlining, additional automation, more efficient collection of input data and more efficient use of output data to ensure that the security processes best support GIAC Enterprises security objectives.

KBF Consulting will review the systems and software development life cycle to ensure security is included at the initiation of a development process and maintains a focus throughout the lifetime of the system. KBF Consulting will review system security requirements and guidelines, security exception handling, system testing and system change control to ensure that security is adequately addressed as part of the process.

KBF Consulting will review the incident handling and response process. As part of this review, KBF Consulting will identify and document the methods by which security events are detected and reported, the information available to incident responders, the response, containment, investigation, and recovery processes and the extent to which the results of security incident response are used to increase the level of GIAC Enterprises security.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

While strategic in nature, this component will examine not only the high-level presence of security concepts but will assess the effectiveness and efficiency of the processes, technologies and tools that are part of the GIAC Enterprises information security program.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Security Documentation Review
KBF Consulting will review the existing security policies, standards, guidelines, management and procedures. We will review these documents for both content and structure, based on industry standards (ISO17799[xvi], TCSEC[xxv], Common Criteria[xxvi]), applicable government regulations such as Sarbanes-Oxley[xv], commonly recognized best practices and KBF Consulting's extensive real-world experiences. KBF Consulting will also review the policy lifecycle and policy management processes to assess the effectiveness of policy development, ratification, dissemination, review, modification and retirement. Our findings will include areas where the modification of existing documents or the development of new documents would be recommended as well as areas where the policy development process may be improved.

Personnel Review
KBF Consulting will look specifically at the people in the organization to assess their security capabilities. For security practitioners, the review will focus on their skill sets and experience to determine what, if any, additional training or education would be beneficial. For those not directly involved with security the review will address the level of security awareness. This component may also include "social engineering" attempts. KBF Consulting will also look at the organizational structure of those involved in GIAC Enterprises security to determine if that structure facilitates efficient and effective information security.

1.1.2. Network Security Assessment

Technical Network Device Review
KBF Consulting will conduct a technological review of corporate network devices. We will review the configuration of a representative sample of network infrastructure devices including switches, bridges, routers, hubs, firewalls, telephony systems, wireless access points and VPNs. KBF Consulting will review the devices for their use of authentication and authorization controls. KBF Consulting will assess the use of network device logging and monitoring functions. We will review the operational configurations to determine if security vulnerabilities exist based on improper or inefficient device configuration.

Network Architecture Review
KBF Consulting will also assess the security considerations of the network architecture and design including secure network segmentation, VLANs, network addressing, load balancing, fault tolerance, traffic management, firewall placement and DMZ design. We will focus on determining which areas of the network are trusted and which are not. The "trust levels" will be reviewed as they relate to data sensitivity (i.e. highly sensitive information on a highly untrusted network would be noted). This review determines the level to which the design of the network facilitates the confidentiality, integrity and availability of data assets.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

1.1.3. Systems Security Assessment

Technical Systems Review

KBF Consulting will review a representative sample of the mission critical systems and applications to determine their security state. We will review these systems to determine their configuration, patch levels, authentication, access controls, security configurations and other pertinent security related information. KBF Consulting will also review the use of system and application security logging and monitoring features. The goal of the technical system review is to discover any known weaknesses or vulnerabilities that exist on company computers as a result of their configuration. These would include systems running unnecessary services, systems with default passwords or no passwords to standard system accounts (i.e. root, Administrator, guest), systems that are subject to compromise because of the lack of a security patch or systems that have excessive or unnecessary user accounts.

Systems Architecture Review

KBF Consulting will review the security considerations of the systems and application architecture including directory services, name services, domain structures and logical system addressing methods will be included in the review. We will determine if the enabling system technologies are causing vulnerabilities that can be exploited or if the overall design of systems or applications can be exploited.

The objective of this assessment is to review GIAC Enterprises security program, supporting systems, applications, and network infrastructure for major security flaws that could impact the stability and operations of the environment. In completing this analysis, KBF Consulting will compare the GIAC Enterprises security architecture to industry "best practices" and KBF Consulting's internal reference material gained from previous client engagements.

As an IT consulting engineering firm, KBF Consulting is well positioned to assist GIAC Enterprises with this critical business initiative. Our engineering staff consists of individuals with experience in security, networking, systems and technical writing. This breadth of knowledge, in conjunction with our proven "best practice" methodologies, enables KBF Consulting engineers to successfully complete complex assignments of this nature.

1.2. Implementation Strategy

1.2.1. Project Staffing

Based on previous experience and the anticipated scope of work to be completed for this project, a project team will be assembled. This team will consist of the following positions:

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Project Manager
KBF Consulting will assign a project manager to GIAC Enterprises for this project. The project manager will address all technical questions regarding deliverables for this project and coordinate all activities outlined in this scope of work. The other assigned engineers will work under direction of the project manager.

Business Analyst
This individual will be responsible for understanding GIAC Enterprises business processes and relating those processes to information technology and information security objectives.

Senior Security Engineer/Consultant
This individual will be responsible for providing security subject matter expertise and will address all security related issues.

System Security Engineer
This individual will be responsible for reviewing GIAC Enterprises operating system configurations and systems architecture design.

Network Security Engineer
This individual will be responsible for addressing all LAN / WAN / Internet connectivity issues.

Technical Analyst/Writer
This individual will be responsible to documenting and pulling together all the information uncovered during the project.

KBF Consulting plans to utilize these resources as necessary to accomplish the defined deliverables. KBF Consulting does not see the need for complex structure and large number of people to complete this project. Rather, KBF Consulting believes a project manager with the support of the other engineers is well positioned to address the scope of work defined in this document. The benefit of this approach to GIAC Enterprises is the ability to develop a good relationship with the project team members and efficiently work through the tasks necessary to complete the SOW deliverables. Further, a small project team helps reduced the overall costs of completing the project. KBF Consulting has used the approach on similar projects and has found it successful.

KBF Consulting will also require the involvement of GIAC Enterprises personnel on a part time basis. These personnel will assist KBF Consulting in information collection and data gathering. These individuals will also be involved in bi-directional knowledge transfer as the KBF Consulting and GIAC Enterprises teams work together to assess the current state of GIAC Enterprises security and to provide appropriate comments and recommendations.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

1.2.2. Project Approach

At the start of this project, a kick off meeting will be conducted between GIAC Enterprises and the KBF Consulting project team. This meeting will allow both parties to have input into the design of a customized project plan that includes the following: coordination of internal schedules, scheduling defined meetings and the introduction of key members of each team that will be the key internal/external "contacts" assigned to this project. Both companies will be asked to sign off on the final project management plan, timelines, key milestones and deliverables required to successfully complete this project.

KBF Consulting will conduct this project in two phases.

Phase 1 – Assessment and Initial Roadmap Development
Phase 1 will involve developing an understanding of where GIAC Enterprises is and where it needs to be as related to information security. Gaps will be identified and a high-level roadmap for achieving the identified security objectives will be created. This phase will consist of five steps as detailed in the following sections.

1. Data Collection
The first step of phase 1 will involve the documentation of the GIAC Enterprises information security current state. To accomplish this, KBF Consulting will begin by collecting relevant data. The data collection will involve all documents and reports stated in the GIAC Enterprises Information Security Strategy Project Request for Proposal. Any additional relevant and appropriate information such as existing policies or standards will be reviewed should it be made available.

KBF Consulting will also conduct interviews with appropriate individuals as identified by GIAC Enterprises. The interviews will be a combination of formatted questions and free-form discussion. When possible, KBF Consulting will provide the interviewee with prior notification as to specific discussion points to allow the interviewee time to collect pertinent information. As the goal of the interview process is to develop an understanding of the perspective of the interviewee, the meetings will also include open discussion to allow the interviewee to provide focus and depth to areas of importance to them. These interviews are designed to accomplish two goals. First, they will allow the KBF Consulting team to more fully and accurately identify the current environment. Second, they will provide KBF Consulting with an understanding of the current view of risk by the individual being interviewed. This will include the presence of perceived risk, the tolerance for risk in various areas within GIAC Enterprises and specific areas where GIAC Enterprises personnel perceive unacceptable levels of risk.

2. Current State
KBF Consulting will prepare a current state document that presents a consolidated view of the information collected during the first step of phase 1. This will include details about the current security program and the information

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

pertaining to GIAC Enterprises' perception of risk. This document will be presented to appropriate GIAC Enterprises personnel for review. This is important as the current state will be a major factor for the remainder of the project. Any inaccuracies or misunderstandings in the current state must be corrected to ensure the project is not based on faulty information.

3. Future State (Recommendations)

Once the current state has been accepted by GIAC Enterprises, KBF Consulting will expand the document to include the future state vision as it relates to the current state. This will illustrate the results of a risk assessment detailing areas that require modification to achieve an acceptable level of risk. The recommendations for the future state will be documented in conjunction with the relevant current state findings to allow for easy understanding and quick reference. The future state will also be documented in an "Information Security Framework" document that provides a concise description of the final security program including its components, roles and responsibilities.

4. Gap Analysis

In the next step, KBF Consulting will document the specific gaps between the current and future states. These gaps will focus on areas where the current state does not meet the requirements of the future state and thus does not reduce risk to an acceptable level. These represent potential weaknesses. In addition, KBF Consulting will document areas where the current state exceeds the proposed future state. These represent areas where a cost savings or performance benefits can be achieved by reducing excess or waste.

5. "Roadmap" Development

For the final step in the first phase, KBF Consulting will identify the initiatives or projects that will allow GIAC Enterprises to achieve the proposed future state. As requested, the initiatives will be designed to occur over a three year timeframe and will include an initial identification of the groups responsible for each project and high-level budgetary information. The roadmap will be prioritized based on the impact of each initiative and initiative dependencies.

Once work begins, KBF Consulting expects to complete phase 1 of the project (*Assessment and Initial Roadmap Development*) with in 12 - 14 weeks. Consulting fees to complete this work are described in the *Cost Summary* section.

Phase 2 – "Roadmap" Elaboration

During the second phase, KBF Consulting will add detail to the roadmap developed in the first phase. This will include the development of detailed project plans for each identified initiative. Each project will be defined in detail including where the responsibility for the completion the project within GIAC Enterprises lies. Project costing will be determined including material, personnel and other resource requirements. Based on the budgetary estimates, the prioritization will

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

be re-evaluated to ensure, as possible, that the financial impact of the identified initiatives is moderated across the full three year timeframe. KBF Consulting will then develop a master project plan defining the timeframes and scheduling for all identified initiatives.

As the specific work and deliverable for phase 2 will be generated in phase 1 of this project it is not possible to set a fixed price however, based on KBF Consulting's past history with similar projects, KBF Consulting expects phase 2 of the project to be completed in the six weeks identified in the RFP. Projected pricing and timeframes for phase 2 of this project can be found in the *Cost Summary* section of this document.

1.3. Deliverables

For this particular statement of work, KBF Consulting will prepare a number of key deliverables:

1.3.1. Phase 1 – Deliverables

- **Project Plan** – KBF Consulting will prepare a formal project plan outlining the project goals, objectives and milestones, dependencies and timeline.

For each of the three focus areas (policy and operations, systems security and network security), KBF Consulting will prepare the following documents:

- **Current State Table of Contents Documents** – These documents will outline the sections and subsections that will be addressed in detail in the Current "State of Security" documents. Once approved by GIAC Enterprises, these documents will serve as the operational template for the remainder of the project.
- **Current "State of Security" Documents** – These documents will detail, for each focus area, the current GIAC Enterprises information security environment. Their purpose is to provide an organized summary of the network environment, systems and security operations that can be referenced when discussing information security risk matters.
- **Assessment Summary Documents** – These documents will expand upon the current "State of Security" documents by detailing commonly recognized "best practices", a gap assessment comparing the current "State of Security" to the defined best practices and KBF Consulting's recommendations. The Assessment Summary Documents will contain the information found in the "State of Security" Documents. For each topic covered, KBF Consulting will elaborate on the relevant "best practices" and industry standards. KBF Consulting will then compare and contract the current state and best practices sections highlighting areas where GIAC Enterprises security meets or exceeds "best practices". KBF Consulting will also point out areas where GIAC Enterprises security does not meet industry standards and why. Finally, for each topic, KBF Consulting will provide detailed

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

suggestions and recommendations for modifying technology and/or processes to bring GIAC Enterprises more in line with best practices and industry standards to increase the security of GIAC Enterprises data and related assets.

Based on a joint KBF Consulting / GIAC Enterprises review of the assessment summary, KBF Consulting will prepare the following documents:

- **Security Program Design Document** – KBF Consulting will prepare a document describing and defining the planned GIAC Enterprises information security program. This document will describe the optimal GIAC Enterprises information security program including its organizational structure, technology requirements, departmental functions, security processes, training considerations, oversight and governance. This document will serve as the strategic goal toward which operational, technological and procedural changes will move GIAC Enterprises.
- **Implementation Roadmap Document** – KBF Consulting will work with GIAC Enterprises to develop a project plan that will allow GIAC Enterprises to successfully implement the security goals and objectives defined in the Security Program Design document. KBF Consulting will break down the roadmap into definable initiatives. We will then help GIAC Enterprises prioritize and estimate budgetary considerations for each key initiative. This roadmap will include initiative dependencies, technology, personnel and operational requirements and training considerations as appropriate.

Once the GIAC Enterprises security program design document has been developed and the roadmap document has been created, KBF Consulting will prepare the following:

- **Phase 1 Executive Summary Document** – KBF Consulting will create an executive level briefing document describing the findings and recommendations for the first phase of the project. This document will not delve into significant technical detail. Rather, it will focus on risks identified to GIAC Enterprises business objectives and the benefits of acting on the recommendations made to mitigate those risks.
- **Phase 1 Executive Summary Presentation** – To supplement the Phase 1 Executive Summary Document, KBF Consulting will conduct a presentation to GIAC Enterprises executives. This presentation will review the content of the executive summary document and will include a question and answer session to ensure that all key GIAC Enterprises stakeholders have a full and complete understanding of the results of phase 1 of this project.

As part of the deliverable for this project, KBF Consulting will conduct meetings and presentations, as necessary, to review the deliverables, answer questions, and provide direction for next step action items.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

1.3.2. Phase 2 – Deliverables

KBF Consulting will provide to GIAC Enterprises as part of the second phase of this project a master project plan detailing timeframes and dependencies for all identified initiatives. In addition KBF Consulting will provide a project plan for each initiative. Along with these planning documents, KBF Consulting will create:

- A phase 2 executive summary document
- A phase 2 executive summary presentation

1.4. Project Assumptions

- KBF Consulting will provide a full time, dedicated, hands-on project manager.
- All personnel assigned to this project will report to the KBF Consulting project manager and will be responsible to that project manager for the timely completion of project assignments and deliverables
- KBF Consulting will be given access to speak with and receive support from all identified GIAC Enterprises personnel who have knowledge deemed useful to complete this project
- The unavailability of KBF Consulting personnel resulting in a delay in the project may result in a change order increasing KBF Consulting's project fees.
- The costs stated in this statement of work do not include capitol expenses associated with hardware or software purchases
- Technical Documentation – KBF Consulting will be able to review available policies and related documentation.
- Facilities Access – KBF Consulting will be provided with access to all necessary facilities related to this project.
- All work will be performed during normal business hours (Monday thru Friday between 8:00am and 6:00pm).
- Technical Documentation – KBF Consulting will be able to review available documentation describing the current network/system infrastructure, application design, and security related matters.
- System Access – KBF Consulting will be provided with access to all necessary systems and devices. KBF Consulting will require direct, administrative access to the systems and devices or will require GIAC Enterprises personnel with such access to provide information requested by KBF Consulting.
- This statement of work will be considered valid for a period not to exceed 30 days from the date of this document.

1.5. Cost Summary

1.5.1. Phase 1 – Consulting Services Fees

The following table illustrates the projected personnel and the estimated expensed for Phase 1 of this project.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Name of Consultant	Hourly Rate	Total Hours	Estimated Expenses
Senior Project Manager	$175.00	480 Hours	$84,000.00
Senior Security Eng.	$165.00	480 Hours	$79,200.00
Network Security Eng.	$165.00	480 Hours	$79,200.00
Systems Security Eng.	$165.00	480 Hours	$79,200.00
Business Analyst	$150.00	300 Hours	$45,000.00
Total Projected Hours and Costs		**2,220 Hours**	**$366,600.00**

KBF Consulting will also employ a technical writer and any additional "subject matter expert" deemed necessary to complete the deliverables for Phase 1 of the project. KBF Consulting is prepared to complete this assignment on a flat fee model based on the deliverables defined in the project approach section, and the assumptions listed in the project assumptions section.

Total Phase 1 Fee: $366,600

Based on initial meetings with GIAC Enterprises, KBF Consulting has determined that this project will require meetings with between 33 and 38 GIAC Enterprises personnel in sites located in two different states. These meeting represent a significant portion of the time allocated for phase 1 of this project. If deemed acceptable by GIAC Enterprises, KBF Consulting may be able to decrease the cost of the project by optimizing the schedule of meetings. This can be accomplished by reducing the number of meetings involved and by ensuring that the meetings are scheduled to reduce "down time" between meetings.

A reduction in the number of meetings can be accomplished with the assistance of GIAC Enterprises by determining where multiple individuals can be interviewed during a single meeting. This, in conjunction with the scheduling of meetings in contiguous blocks of time can significantly reduce the overall time and resource requirements thereby reducing the overall phase 1 cost. The current pricing is based on a 33 to 38 meeting requirement. If GIAC Enterprises can reduce this number, KBF Consulting may be able to decrease the flat fee pricing by as much as 15%.

1.5.2. Phase 2 – Consulting Services Fees

The specific details of phase 2 of this project will be defined as a result of the completion of the first phase. A complete understanding of the scope of phase 2 will only be possible as phase 1 nears completion. As a result, KBF Consulting cannot establish a flat fee for phase 2 of this project. For the purpose of this RFP response, KBF Consulting will quote a "time and materials" estimate of cost.

Based on work KBF Consulting has previously performed, KBF Consulting expects phase 2 of this project to involve the following:

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Name of Consultant	Hourly Rate	Total Hours	Estimated Expenses
Senior Project Manager	$175.00	240 Hours	$42,000.00
Senior Security Eng.	$165.00	240 Hours	$39,600.00
Network Security Eng.	$165.00	240 Hours	$39,600.00
Systems Security Eng.	$165.00	240 Hours	$39,600.00
Business Analyst	$150.00	240 Hours	$36,000.00
Total Projected Hours and Costs		**960 Hours**	**$196,800.00**

Estimated Phase 2 Fee: $196,800

Note: At the completion of phase 1, KBF Consulting will prepare a flat fee for phase 2. GIAC Enterprises will have the option of accepting the flat fee cost or conducting phase 2 on a time and materials basis as defined in this document.

Estimated Total Project Cost: $563,400

1.6. Payment Terms

For this Statement of Work, consulting fees will be billed following in the following manner.

Phase 1:

- 25 % due at project signing and acceptance
- 25 % due upon completion and acceptance of the Current State document
- 25 % due upon completion and acceptance of the Assessment Summary documents.
- 25 % due upon completion of Phase 1 of this project

Phase 2:

As phase 2 has no fixed price, it will be billed on a monthly basis based on actual hours worked. KBF Consultants will submit weekly reports detailing hours worked.

All invoices are due Net 30.

Payments shall be remitted to: KBF Consulting, P.O. Box 123, East Stroudsburg, PA 18301.

1.7. SOW Approval

By signing below as an authorized representative of GIAC Enterprises, I acknowledge I have read the information contained within this Statement of Work and approve to engage with KBF Consulting to complete it. Furthermore, I agree to the following terms and conditions.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

1. I understand KBF Consulting is responsible for the deliverables defined in the *Deliverables* section of this agreement and any requested or necessary services outside this scope of work will require a change order to complete.
2. GIAC Enterprises agrees to the Product Costs and/or Consulting Service Fees listed in the *Cost Summary* section, the associated Project Assumptions, and the *Payment Terms* information to settle these obligations.
3. GIAC Enterprises and KBF Consulting agree that neither company shall hire, make any employment offers or otherwise seek to employ in any way the personnel of the other party, without the written consent of the other party. This restriction shall extend for one year after KBF Consulting has completely withdrawn its consultants from the engagement with GIAC Enterprises. In the event either party makes an offer of employment or otherwise seeks to employ an employee of the other, the offending party shall pay a penalty equal to the current salary of the employee in question.
4. All employees of KBF Consulting complete legally binding confidentiality agreements to ensure that neither GIAC Enterprises, nor KBF Consulting proprietary information or intellectual property is stolen, misrepresented, transferred or used harmfully against either company in any way. Upon completion of this project, all properties used, lent or borrowed by either KBF Consulting or GIAC Enterprises will be returned.
5. KBF Consulting is retained as an independent contractor, and not an employee or agent of GIAC Enterprises, and shall be responsible for its own work. The employees furnished by KBF Consulting to perform the work shall be deemed to be KBF Consulting's employees exclusively and said employees shall be paid by the KBF Consulting for all services in this connection. KBF Consulting shall be responsible for all obligations and reports covering Social Security withholding, Unemployment Insurance, Workers' Compensation, Income Tax and other reports and deductions required by any applicable State and Federal law, for such employees.
6. This agreement shall be effective for 1 year from the date of the executing of this agreement unless either terminated or extended in accordance with the applicable provisions of this agreement.
7. Notwithstanding anything in this Agreement, it is agreed that NEITHER GIAC Enterprises NOR KBF Consulting shall be liable to the other in any event for any direct, indirect, special, incidental or consequential damages arising out of the services provided hereunder.
8. GIAC Enterprises may terminate this Agreement and be relieved of the payment of any further consideration to KBF Consulting should KBF Consulting materially fail to perform the covenants herein contained in the manner provided, provided GIAC Enterprises shall have given KBF Consulting ten (10) days written notice of intent to terminate and

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

reasonable time to cure the reported failure (24 hours unless extended time is requested by GIAC Enterprises). This Agreement may not be terminated for convenience by either party unless mutually agreed to in writing.

9. Any and all information or data of whatever nature provided, prepared or generated by GIAC Enterprises or by KBF Consulting for GIAC Enterprises in connection with the performance of this Agreement shall be treated as confidential by KBF Consulting and shall not be made available to any individual or organization other than GIAC Enterprises without the prior written direction and approval of GIAC Enterprises.
10. KBF Consulting shall not assign this Agreement or any interest in this Agreement hereunder without the prior written consent of GIAC Enterprises.
11. KBF Consulting shall permit GIAC Enterprises and/or its designated representatives to inspect its facilities and audit KBF Consulting's procedures and non-financial records relating to performance under this Agreement.
12. This Agreement constitutes the entire and integrated agreement between KBF Consulting and GIAC Enterprises and supersedes all prior negotiations, representations, or agreements, either written or oral. This Agreement may be amended only by written instrument signed by both KBF Consulting and GIAC Enterprises.
13. All notices or other communications to either party by the other shall be deemed given upon receipt when made in writing and mailed by certified mail or delivery service, return receipt requested, to:

KBF Consulting
John Smith
President and Secretary
1 First Street
New York, NY 12345

GIAC Enterprises
Sally Jones
GIAC Director
123 Fifth Ave., Suite 1
New York, NY 12345

IN WITNESS WHEREOF, the parties hereto have executed this Agreement as of the last date noted below.

KBF Consulting		**GIAC Enterprises**	
Signature	_____	**Signature**	_____
Printed	_____	**Printed**	_____
Title	_____	**Title**	_____
Date	_____	**Date**	_____

Contract form prepared by KBF Consulting: August 20, 2004

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

2. Pitch

The factor of foremost importance in winning this business is the creation of a relationship between the decision-makers at GIAC Enterprises and KBF Consulting personnel. Security work revolves around the concept of trust. Without trust, winning this business will be significantly more difficult. Building a relationship between KBF Consulting and GIAC Enterprises has additional benefits. People generally buy based on emotion and will more likely buy from people, or an organization, they like.

Assuming that a relationship between KBF Consulting and GIAC Enterprises has been developed to the greatest extent possible, KBF consultants would emphasize KBF Consulting's:

- History of the successful completion of similar projects – KBF Consulting has conducted numerous enterprise-level security related projects including:
  - HIPAA related information security policy development for a major health care provider
  - The use meta-directories and the integration of Unix LDAP and Microsoft Active Directory databases to provide a consolidated authentication and authorization solution for a major pharmaceutical company
  - The performance of a comprehensive information security assessment for a state transportation authority
  - The performance of a 21 CFR Part 11[xxvii] compliance audit and remediation recommendations for a major pharmaceutical company
  - The implementation of a PKI infrastructure for an nation-wide insurance company
- Wide range of expertise and experience – KBF Consulting has experienced professionals including network engineers, system engineers, application developers, information security experts, business analysts and project managers. For security projects, KBF Consulting utilizes personnel from across these disciplines to ensure the most complete and comprehensive skill set on its project team.
- Strong, tested methodology and approach – the approach utilized by KBF Consulting has been tested in a wide range of situations. The initial development of a current state document and subsequent client review ensure that KBF Consulting has a complete and correct understanding of the client environment. In the event that the engagement is the first between KBF Consulting and the client, this step gives the client the opportunity to review KBF Consulting's work product early in the project to increase the level of trust.
- Fixed price projects – offering a fixed price for much of the work performed allows the client to better estimate budgets. It also reduces the risk to the client that the project will become extended beyond a reasonable timeframe.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

- Flexibility – KBF Consulting is able to adapt to meet changing client requirements and adapt to dynamic circumstances. The small project teams recommended by KBF Consulting are able to adjust and react to situations that present themselves to ensure the successful completion of the project.
- Knowledge transfer – KBF Consulting ensures, before completing its projects, that client personnel have been fully briefed on the project and have been provided with the full set of project documentation. By doing so, KBF Consulting seeks to ensure that its clients are capable of utilizing the results of the project without requiring additional KBF Consulting support. KBF Consulting works on a project-by-project basis rather than in a client staff augmentation capacity.

To verify and validate its sales pitch KBF consulting would present GIAC Enterprises with:

- Resumes, bios and portfolios of the consultants that will be assigned to the project
- Letters of recommendation from recognized industry experts and well known previous or current clients
- Client references including contact names, email and phone numbers

Part 3 – Project Performance

1. Project Plan

1.1. Project Plan Overview

The project will be broken down into six stages including:

- Project Planning & Housekeeping
- Current State Development
- Assessment and Recommendations
- Security Program Design
- Roadmap Development
- Final Presentation

This approach allows KBF Consulting to kick off the project, methodically work through the data gathering, collect accurate information and make effective recommendations. It then allows the security program design and roadmap development to be performed based on a complete assessment. The final presentation can then be tailored to provide the client with relevant information in a clear and concise manner.

The project will begin with the development of a formal project plan and the performance of housekeeping tasks such as setting up a work space, getting network access and access to the client facility. Once this has been completed, data will be collected to develop a picture of the current state of client security.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Before proceeding, the current state will be provided to and reviewed by the client. Feedback from the client will ensure that KBF Consulting performs the remainder of the assessment using complete and accurate information. This step also provides the client the opportunity to review KBF Consulting work before the project progresses too far. It ensures that both KBF Consulting and GIAC Enterprises have the same expectations with regard to the type of documentation to be created as part of this project.

After the current state has been reviewed and approved by both parties, the assessment and recommendations phase will begin. During this phase, KBF Consulting will document industry accepted "best practices", gaps between the current state and "best practices" and recommendations for modification to the GIAC Enterprises security environment.

The security program design phase converts the individual detailed recommendations into a strategic security program. Rather that a list of risk mitigation tasks, the program will provide a picture of what the proposed security program will look like.

In order to provide GIAC Enterprises with the ability to implement KBF Consulting's recommendations, KBF will create a series of prioritized projects which, if completed, would allow GIAC Enterprises to achieve the designed program in an acceptable timeframe.

The project will be completed with the submission of project deliverables to client personnel and a presentation of the project outcome to GIAC Enterprises stakeholders. During this presentation, KBF Consulting will provide an overview of the findings and recommendations and will answer any questions posed by client personnel.

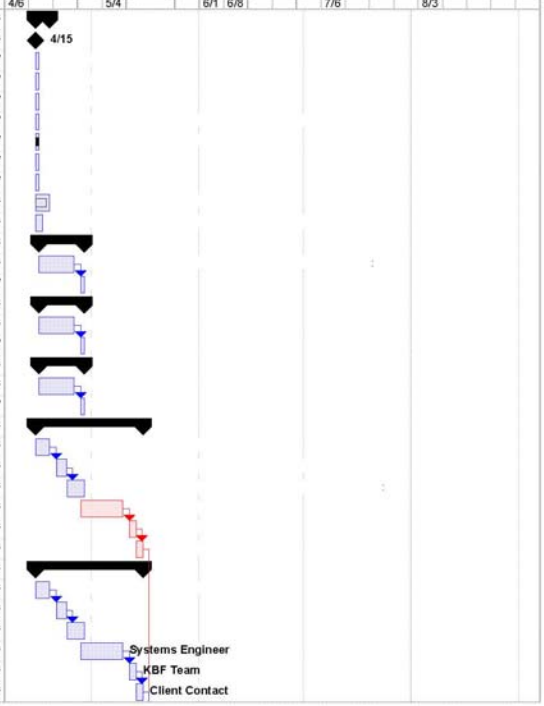
© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

1.2. Project Schedule

Project Secure - GIAC Enterprises

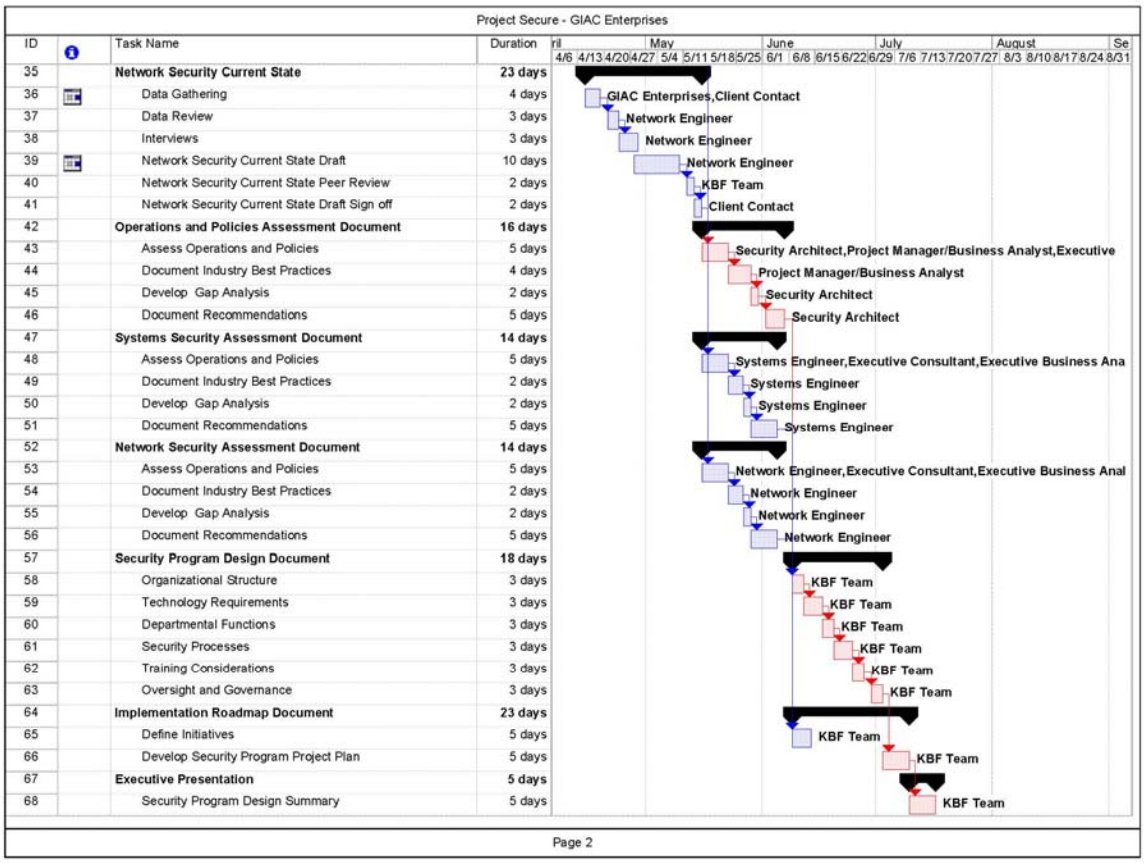
ID	Task Name	Duration
1	**Project Planning/Housekeeping**	**4 days**
2	Kick-Off Meeting	0 days
3	Secure work space	1 day
4	Network connections	1 day
5	Security ID's	1 day
6	Develop Meeting Schedules	1 day
7	KBF Consulting Contact List	1 day
8	GIAC Enterprises Contact List	1 day
9	Email Access	1 day
10	Develop Project Protect Plan	4 days
11	Communication/Document Access	2 days
12	**Operations and Policy Table of Contents**	**9 days**
13	Create Table of Contents for Operations and Policies	8 days
14	Table of Contents Sign off	1 day
15	**Systems Security Table of Contents**	**9 days**
16	Create Table of Contents for Systems Security	8 days
17	Table of Contents Sign off	1 day
18	**Netork Security Table of Contents**	**9 days**
19	Create Table of Contents	8 days
20	Table of Contents Sign off	1 day
21	**Operations and Policies Current State**	**23 days**
22	Data Gathering	4 days
23	Data Review	3 days
24	Interviews	3 days
25	Operations Current State Draft	10 days
26	Operations Policies Current State Peer Review	2 days
27	Operations Current State Draft Sign off	2 days
28	**Systems Security Current State**	**23 days**
29	Data Gathering	4 days
30	Data Review	3 days
31	Interviews	3 days
32	Systems Security Current State Draft	10 days
33	Systems Security Current State Peer Review	2 days
34	Systems Security Current State Draft Sign off	2 days



Page 1

© SANS Institute 20

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.



1.3. Project Goals

Each phase of this project has a specific set of goals and objectives as follows:

- Project Planning & Housekeeping
  - Establish an adequate work area
  - Provide KBF consultants with access to client facilities, personnel and resources
  - Develop and communicate a detailed project plan for the remainder of the project
- Current State Development
  - Collect information about the GIAC Enterprises operations, systems and network security
  - Document the current state
  - Get client signoff of the current state document
- Assessment and Recommendations
  - Collect and document “best practices”
  - Document current state vs. best practices gaps
  - Provide reasonable recommendations for changes to the client security environment
- Security Program Design

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

    - Document a clear description of the recommended client security program
- Roadmap Development
    - Provide the client with an actionable process for achieving the recommended security program
- Final Presentation
    - Ensure client stakeholders understand KBF Consulting recommendations

1.4. Budget Breakdown

This project is being performed using a fixed price model based on estimates by KBF Consulting of the time and resource requirements for the project.

The rates charged on this project were based on a number of both direct and indirect expenses associated with overhead including:

- SG&A - Sales General and Administrative - a category including the cost of sales, commissions, department overhead for order entry, and accounting (payables and receivables)
- Office - Rent/Lease
- Cost of office equipment – Copiers, fax machines, etc.
- Capitol expenses for computer equipment
- Leasehold improvements – i.e. office / work area improvements
- Entertainment (i.e. for clients)
- Training expenses
- Administrative overhead - management / administration
- Insurances - company portions of life / health / dental
- Business Insurances - liability, performance bonds, company vehicles
- Expenses – (i.e. associated with projects including travel, lodging, meals, office supplies, etc.)

In addition, personal time off or PTO get accrued including:

- Paid Holidays
- Vacation time
- Other PTO

To address these costs and expenses, KBF Consulting has developed a formula. This formula involves taking an employee's salary with bonuses and adding a load to it. Generally, the load is 50%. This will give you a load for the person. Take the loaded salary and divide by 2080, the theoretical number of hours that are in a year. That will give you a base cost for a resource per hour. Take the loaded base resource cost and multiply by the number of hours you used for the project. You will have your project cost. Now subtract from your price and you will get your Gross Profit. Note, as the project cost is fixed, if the team runs over on the hours your gross profit will decrease.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

The following table depicts the results of this formula for this project:

Name of Consultant	Hourly Rate (Charged)	Annual Salary	Loaded Salary	Loaded Hourly	Loaded Project Cost	Project Charge	Gross Profit
Senior Project Manager	$175.00	$110,240.00	$165,360.00	$79.50	$57,240.00	$126,000.00	$68,760.00
Senior Security Eng.	$165.00	$95,680.00	$143,520.00	$69.00	$49,680.00	$118,800.00	$69,120.00
Network Security Eng.	$165.00	$95,680.00	$143,520.00	$69.00	$49,680.00	$118,800.00	$69,120.00
Systems Security Eng.	$165.00	$95,680.00	$143,520.00	$69.00	$49,680.00	$118,800.00	$69,120.00
Business Analyst	$150.00	$85,280.00	$127,920.00	$61.50	$33,210.00	$81,000.00	$47,790.00
					$239,490.00	**$563,400.00**	**$323,910.00**

It is important to note that the hourly rates charged to GIAC Enterprises for its consulting services are based on a number of factors including the skill and experience of its consultants, the perceived or stated budget of the client and, most importantly, the "going rate" in the market. KBF Consulting generally prices its services based on value to the customer. The above calculations are made to determine if the engagement will be profitable.

Gross profit is then used to calculate the commission paid to the KBF Consulting sales representative. In this case, the sales person gets paid a commission of 15% of the gross profit for a total of $48,586.50. The remaining $275,323.50 can them be used to pay business expenses, meet payroll for consultants unengaged or "on the bench", etc.

1.5. Project Administration and Communication

KBF Consulting will maintain constant communication with the GIAC Enterprises project owner. This will be accomplished by conducting weekly meetings between the owner and the KBF project manager. The KBF project manager will provide the GIAC project owner with a weekly status report consolidated from weekly reports created by the KBF Consultants. The following is an example of the report format:

Project Weekly Status Report

To: [Client Name]

From: [KBF Consulting Project Manager]

Date: [Week Ending Date]

Copy: [Customer Sponsors]
[KBF Consulting Sponsors]

I. Activities completed and in process for week of [Current Week Start Date]

II. Activities and plans for week of [Next Week Start Date]

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

III. Open Items/Issues and Concerns

Open Item/ Issues & Concerns	Responsibility	Date Entered/ Target Date	Comments/Status

IV. Project Lost Time

Date Entered	Lost Time Event	Hours Lost	Responsibility

In addition to weekly reports and meetings, KBF Consulting will work closely with GIAC Enterprises personnel. This constant communications will allow KBF consultants to react to situations as they occur. The small team approach with and hands-on project manager utilized KBF Consulting allows for rapid adjustments to ever changing situations.

2. Meeting & Interview Facilitation

In order to make effective and relevant recommendations, KBF Consulting must understand not only what is being done with regard to information security, but also the executive viewpoint on security in relation to business operations. This information is necessary so that KBF Consulting can design a security program that deals directly with GIAC Enterprises business risks. Understanding the executive viewpoint on security can also uncover areas where perceived risk does not relate to actual risk.

To collect the necessary information, KBF consultants must meet with a wide range of executive personnel including:

- Chief Information Officer
- Vice President of Corporate Security (physical security)
- Chief Financial Officer
- Director of Internal Audit
- Chief Operations Officer

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

In addition to these specific functional titles, KBF consultants will meet with the owners of GIAC Enterprises business units and profit centers.

The following questions will be posed to the aforementioned GIAC Enterprises personnel:

1. What is your understanding of GIAC Enterprises information security?
2. How important to GIAC Enterprises business do you feel information security is?
3. How effective do you feel your security is?
4. What areas of your business do you feel are at the greatest risk?
5. What are the risks?
6. What would happen to your business unit or organization if these risks were realized?
7. Are you aware of corporate informational assets that, if compromised, would result in significant or catastrophic harm to GIAC Enterprises?
8. What do you feel could be done to improve information security?
9. What are the biggest problems you see in GIAC Enterprises security?
10. Are you kept informed of information security issues related to your area of influence?
11. Do you feel that you are sufficiently involved in information security?

3. Potential Pitfalls

3.1. Pitfall 1 – The Unresponsive Client

3.1.1. Description

When working for a client as a consultant, it is common to experience a lack of response from client personnel. In some cases, they view the consultant as an outsider who is likely to do nothing more than get in the way. Even worse, client personnel may be threatened by a consultant. More often than not, however, client personnel simply have too much to do. In any case, unresponsive client personnel can put the timely completion of the project in jeopardy by introducing excessive delays or, worse, by injecting incorrect data into the project equation. It is critical to understand that this potential problem exists and to act, throughout the course of the project, to mitigate its effects.

3.1.2. Warning Signs

Detecting unresponsive or uncooperative personnel is relatively simple. The following are some indications that you may have a problem:

- Phone calls not being returned
- Emails not being responded to
- Deliverables assigned to client personnel are not complete, late or of poor quality
- Overt client personnel hostility

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

In addition to these more obvious methods, if you have good relationships or a network within the client organization, you may find out from others that a particular individual is either actively or passively resistant.

3.1.3. Handling the Problem

There are basically two ways to address this type of problem. You can put in place controls to react to it if it occurs and you can work to stop it from occurring in the first place.

Generally speaking, stopping this problem from occurring relies on one simple concept, relationships. As a consultant, you must build relationships with your clients. This means not only establishing relationships with the people who sign your checks but also with those who will affect and be affected by the outcome of your project. To the extent possible, include these people in the process and reassure them that you are there to help. If they think of you as being "on their side", they will be less likely to cause problems. If they think of you as someone who will ultimately help them, they will provide you will all the assistance you can. In the event that you detect negativity, resentment or hostility, stop and find out what is wrong. You will not be able to win over everyone or make everyone happy but it is worthwhile to make the attempt.

No matter how hard you try, you cannot make everyone happy. This is realized most obviously in circumstances where client personnel will be negatively affected by your work. This may occur when a recommendation you make reduces someone's power or influence. It can also occur when someone has been taking advantage of a situation and your work will point that out. In these cases, you will have to react to uncooperative client personnel. There are a couple of simple things that can be done to reduce or eliminate the harm caused by these situations. First and foremost, a good proposal should address this type of circumstance before the project begins. If the project is being performed on a time and materials bases, the proposal or statement of work should state that delays caused by client personnel could increase the expected duration of the project or could result in the consultant requiring additional resources to meet specific deadlines. Similarly, the contract for a project being done at a fixed cost should state that client delays may result in a change order. The verbiage of these statements can be made more or less strict based on your relationship with the client.

Having a contract that accounts for client-caused delays will be of little value if you do not communicate with the client about these delays as they are occurring. It will do little to improve your relationship with a client if, at the end of a project, you hand them a large bill based on delays they did not know about and were not given the chance to fix. The client should be kept informed about the status of the project throughout the project. These status updates should include information about successes as well as problems. If specific client personnel are uncooperative, that should be reported to the appropriate client contact giving

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

them the opportunity to address the problem. If they fail to, you will then have the opportunity to reset client expectations accordingly. This could involve increasing the cost of the project, increasing the duration, increasing the resources or reducing the scope of the project to eliminate areas involving unresponsive personnel.

In order to address this problem it is important to determine the root cause for any resistance encountered. There are an almost infinite number of reasons for these types of problems, each requiring a different response. The following are example of problems causes and potential responses:

Root Cause	Resolution Strategy
The client is overworked and does not have the time or the resources to meet your expectations	Do everything you can to reduce the impact to the client. Utilize phone calls or email correspondence instead of face-to-face meetings. Provide the client with specific questions or forms to fill out. Offer to perform the work you are waiting on (either as part of the project or as a change order). If the project is critical to the client, offer to provide staff to augment the client's overworked personnel.
The client has a personal problem with you, a member of your team or your organization	Sit down with the individual to discuss the problem. This meeting should include the individual with the personal problem, the target of the problem, the client personnel sponsoring the project and a supervisor from your organizing. If the problem cannot be resolved, the personnel involved with the project may need to be modified.
The client has a personal problem with your sponsor or the individual who engaged you for the project	Attempt to show the resistant client how the project will benefit them. Also try to build a relationship with the resistant individual so they will view you as a friend or ally. If these attempts fail, the project sponsor will need to be notified of the problem.
The client has a problem with the project itself considering it unnecessary or improper	Show the client the value of the project and re-emphasize why the project was initiated. If this problem originates from personnel involved with supporting the project, the project sponsor may need to be notified. If the problem originates with the sponsor, the project may need to be modified or terminated prematurely.
The client feels threatened by you or the project because of a lack of understanding	Educate the client and show them how they will benefit by the project. If possible, try to find out what the resistant individual is trying to accomplish at work and show them how your project will further their goals.
The client feels threatened by you or the project because they have something to hide	In this case, the client sponsor will need to be notified about the problem. You should avoid telling the sponsor your assumptions about the reason behind the problem. Only tell them what is happening and how it is affecting the project.

Regardless of the cause of the problem, the first step should always be to notify the project sponsor. This keeps them “in the loop” ensuring there are no surprises. At this time, you should not request that the project sponsor get directly involve unless it is absolutely necessary or the sponsor specifically requests to be involved. You should attempt to correct the problem by dealing with the personnel involved. Fixing the problem will allow the project to continue with minimal impact on the project sponsor. If the problem cannot be fixed, the project sponsor needs to be involved. The problem can then be turned over to the sponsor to fix internally. The resolution could also involve both the consultant and the client. Frequently, reassigning client or consulting personnel in relation to the project can achieve the desired results.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

3.2. Pitfall 2 – The Wrong Consultant

3.2.1. Description

In an organization with a single or small number of consultants, it is relatively easy to determine the "right" projects for each consultant. As the number of consultants increases, the chances of placing a consultant on the wrong project grows as well. A "wrong" project could be one for which the consultant lacks the necessary experience or one that does not match the consultant's temperament. Highly technical engineers would be a poor fit for a project involving nothing but policy development.

An ideal consultant may become "wrong" due to personal circumstances. Problems at home, new babies, financial problems and other situations could distract a consultant causing poor work product. Whether because of a poor project fit or external problems, less effective consultants can result in service delivery problems, schedule delays, unacceptable deliverables or unhappy clients. These problems could jeopardize the project, the client relationship or even the reputation of the consulting organization.

3.2.2. Warning Signs

Indications that a consultant may be "wrong" include the following:

- Consultant complaints or expressed dissatisfaction
- Calling in sick or persistent tardiness
- Missing deadlines
- Poor work product
- Not actively engaging in project activities
- Not participating in group conversations or activities
- Lack of questions or communication
- Excessive conversations unrelated to the project

3.2.3. Handling the Problem

The primary method for addressing this type of problem is proper project management. Before the project starts, the project manager should interview the consultants before they are assigned to the project to identify potential problems. Early in the project the project manager should frequently check the progress of consultant work. During the course of the project, frequent status checkpoints should be established to ensure all work is on track and of sufficient quality. Also, throughout the project, the project manager and all project personnel should maintain constant communications. All personnel should be encouraged to report potential problems as quickly as possible.

If a problem is identified, it becomes the responsibility of the project manager to resolve. The simple resolution to "the wrong consultant" is to replace the consultant with one more suited to the project or the situation. This, however, is not always an option and other solutions need to be found.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

The proper solution will depend on the cause of the problem. If the consultant lacks the necessary skills to complete the project and sufficient time is available, the consultant could be sent to training. This training could be provided by others in the consulting organization or by an external training organization. Work assignments could also be modified allowing each consultant to do work they are qualified for and interested in.

In circumstances where external factors are causing the problems, the project manager should meet with the consultant in question. Often, the consultant will appreciate the concern and will respond with renewed effort. Other arrangements such as flexible work schedules could also be made to decrease effect of the external factors.

In the worst case scenarios, the project manager may need to explain the situation to the client and reset expectations. This could involve adjusting the project schedule, modifying the scope of the project, assigning client personnel to the project or adjusting the project price.

4. Value Add

During the course of this project, KBF Consulting personnel will come into contact with a wide range of GIAC Enterprises personnel including those both directly and indirectly involved in information security. During this time, KBF Consulting will identify numerous situations that may not be obvious to client personnel who see the situation from their own limited perspective. These situations include communication breakdowns, lack of education, political resistance and differences in understanding of the goals and objectives relating to information security.

During these contacts, KBF Consultants have the opportunity to provide education and training to GIAC Enterprises personnel where lack of education exists. Consultants can facilitate communication between different organizational units to ensure that everyone is “on the same page” when it comes to information security goals and objectives. As an outside entity, KBF Consultants have the ability to bypass or circumvent political resistance without sacrificing their careers or organizational positions. These communication, education and political benefits can greatly enhance the client organizational drive and commitment to information security. It can also increase the acceptance of project findings and recommendations throughout the client organization. Accomplishing this will not only provide the client with a valuable product but also with an organization ready and able to put it into practice.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Part 4 – Final Deliverable

1. Section A – Security Program Design

1.1. Program Goals and Objectives

The GIAC Enterprises information security program will consist of a number of high level components that provide the foundation for the security of GIAC Enterprises information and related assets. These components include the concepts of risk assessment and risk management, security policies, standards, education, awareness, accountability and oversight. On this foundation, a framework of layered security will be built. These "layers" include technical and administrative controls implemented according to specific GIAC Enterprises security requirements.

1.1.1. Risk Management

The primary goal of the GIAC Enterprises information security program must be to reduce risk to information and related assets to an acceptable level. To be effective, the security program must act to support business operations rather than hinder to them. To these ends, the GIAC Enterprises information security program will be based on the concepts of risk assessment and risk management rather than on risk elimination. A risk elimination strategy attempts to remove all risk. While, in rare cases, this may be possible, the associated costs generally far outweigh the benefits. Risk management is accomplished using a process of risk assessment whereby the likelihood that a threat will exploit a vulnerability causing harm to an asset is determined. Risk assessments generally attempt to determine how much harm a security incident would cause and the expected annual rate of the incident. This value can then be used, in conjunction with the value of the asset(s) in question to determine the resources that can be justifiably used to mitigate the perceived risk. The GIAC Enterprises information security program will revolve around the concepts of risk assessment and risk management.

1.1.2. Risk Assessment

Risk assessments are performed to determine the appropriate level of resources for risk mitigation. These assessments must be factored into each and every aspect of GIAC Enterprises business operations. Assessments must be completed where information or technology is involved. While it is possible to conduct a risk assessment each time a change is made to the GIAC Enterprises computing environment, this is often not feasible nor is it necessary. The majority of situations can be considered in advance of their occurrence and thus proactive risk assessment and mitigation strategies can be developed. These proactive risk mitigation decisions can then be documented in the form of security policies, standards, guidelines and procedures. Once created, policies and standards provide the instructions for reducing risk to an acceptable level. A risk assessment then, only needs to be conducted when a situation has not been

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

adequately addressed by the policies or standards or when deviation from those policies or standards is required.

1.1.3. Security Policies

To ensure the information security program is effective, efficient and comprehensive, a full complement of policies and standards will be required. These documents will address all foreseeable information security and related issues. Policies that will be required include:

- Data Classification
- Data, Information and Systems Ownership
- Risk Assessment
- Information Security Legal Compliance
- Security Certification and Accreditation
- Vulnerability Management
- Policy Management
- Security Audit and Compliance Verification
- Encryption
- Property and Facilities Protection
- Asset Management
- Hardware and Peripheral Protection
- Personnel Security
- Privacy
- Remote Access
- Identification, Authentication and Authorization
- Mobile Computing and Teleworking
- Acceptable Use
- Credential Management
- User Provisioning
- Media Management
- Security Change Management
- Data, Systems and Network Monitoring
- Outsourcing and Managed Services
- Security Awareness, Education and Training
- Incident Handling
- Information Back-up
- Disaster Recovery
- Business Continuity
- Segregation of Duties
- Systems Planning and Acceptance
- Security in Project Management
- Secure Systems and Application Development
- Security Testing

It is important to understand that while there are many policy titles listed, each does not represent a unique, independent policy but rather a part of a comprehensive suite of policies. The suite has been divided into a variety of titles to make the policy suite more easy to use. Many of the policy titles listed refer to and rely on others in the suite.

1.1.4. Security Standards

In addition to policies, which are high-level and business unit or technology independent, GIAC Enterprises will rely on technical or operational standards. These documents are more detailed than policies and refer to specific technologies, applications or business units. They contain minimum secure configuration requirements and operational requirements for the subject addressed. Standards will range in scope from those governing a specific

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

business unit or technology to those involving the entire GIAC Enterprises enterprise. Enterprise standards will be less detailed that those with a more narrow focus. Where enterprise standards and business unit/technology standards overlap, the more specific standards must comply with enterprise standards. Many of these standards will be directly related to the policies. For example, there are policies covering encryption and security testing. There will also be technical an operational standards covering the same topics. While the complete list of standards that will require development is beyond the scope of this document, examples of areas that must be addressed by technical or operational standards include:

- Policy Specific Standards
- Windows NT
- Window 2000
- Cisco routers
- Nortel routers
- Checkpoint Firewalls
- Cisco Firewalls
- IIS Web Server
- Apache Web Server
- Solaris
- Applications (incl. Peoplesoft, etc.)
- Network Architecture
- Systems Architecture

It is important to note that this list does not represent a complete list of GIAC Enterprises standards. Rather, it includes major technologies and applications in use within the GIAC Enterprises enterprise to provide examples of the type of security standards that will be developed. The complete list of standards will require a technology and applications inventory.

It is also important to note that standards will, in many cases, be business unit specific. As business units may use similar technology in different ways, the standards developed for that technology will differ. This scenario is acceptable provided all standards remain in compliance with established GIAC Enterprises policies.

1.1.5. Education and Awareness

Many organizations have gone through the process of documenting security requirements in the form of policies and standards. Frequently, however, these documents are placed in binders on a shelf and serve no useful purpose. For a security program to be effective, it is important that education and awareness be provided to those responsible for organizational security. This begins with the distribution of policies and standards to those governed by them. The distribution must be targeted; providing information only to those requiring that information. This includes distribution to executives, managers, technical staff, security

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

practitioners and to the average user as appropriate. The process cannot end with distribution. It must include education ensuring that recipients have not only received the documents but understand them and their effects. People can be one of the greatest security strengths of an organization. They can also be one of the greatest weaknesses. The difference is the level of training and awareness provided. The GIAC Enterprises security program will include security awareness and education. The process will begin with policy and standards training and will continue as an ongoing part of daily operations. This ensures that everyone, from the average user to the executive is aware of the part he or she plays in information security and has the information necessary to maintain and enhance the information security program.

1.1.6. Oversight

The GIAC Enterprises information security program will not rely on good intentions to achieve adequate security. Oversight will be included in the security program to verify that compliance with security requirements is being achieved. This process of audit and review will involve periodic compliance checks. These checks will not only verify compliance with existing policies and standards, but will also verify the existing policies and procedures successfully mitigate risk to GIAC Enterprises to an acceptable level. The oversight function will be complemented by an increase in accountability for GIAC Enterprises security. Education and awareness will ensure that each individual knows the part he or she plays in GIAC Enterprises security. The oversight process ensures that requirements are being complied with. For this to be effective, individuals will be held accountable for both compliance and non-compliance. This accountability will include recognition for high levels of compliance and appropriate disciplinary action for non-compliance.

1.1.7. Governance

There are many factors that affect the daily operations of the GIAC Enterprises information security program. These include internal influencers such as business requirements, policies and procedures. Additionally, GIAC Enterprises is affected by external factors such as federal, state and local regulations. Internal factors are easily addressed by program components such as oversight. External factors must likewise be addressed. The GIAC Enterprises information security program will include external governance compliance. This will be an ongoing process as regulations are created and/or modified. External governance will play a major role in the development of policies and standards and will affect the risk assessment process.

1.1.8. Layered Security

The GIAC Enterprises security framework is based on the concept of “layered security”. Any given security control will have its own set of strengths and weaknesses. Technical controls are subject to improper configuration and the discovery of weaknesses. Administrative controls are subject to human error. Layered security involves implementing multiple, supplemental controls where

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

the strengths of one layer offset the weaknesses of another. There are many methods of categorizing security layers. The GIAC Enterprises security program will involve the use of three layer models. These models facilitate the performance of risk assessments. When conducting risk assessments, the three models will be used to ensure that adequate controls have been implemented for a particular area of risk. The three models are as follows:

Protection-Detection-Response-Recovery (PDRR)
The PDRR model states that controls provide one or more of the following functions; protection, detection, response and recovery. Protective controls are designed to stop threats from harming assets. Detective controls are designed to identify attempted or successful attacks. Responsive controls reduce or eliminate the harm caused by an attack that has bypassed protective controls. Recovery controls are required to restore business operation as quickly as possible should all other controls fail.

Perimeter-Network-System-Application-Data (PNSAD)
The PNSAD model identifies data or information as being the core asset requiring protection. Surrounding data are layers of controls that support its protection. Data can reside on a particular piece of media. Data is generally accessed using an application. Applications reside on systems (operation systems + hardware). These systems reside on a network. The network has a perimeter delineating trusted environments from untrusted. Security controls can be applied at each of these layers.

Reduce Threat-Reduce Vulnerability-Reduce Harm (RT-RV-RH)
The RT-RV-RH model revolves around the definition of risk as the likelihood that a threat will exploit a vulnerability causing harm to an asset. Given this definition, the way to reduce risk is to address the threats, the vulnerabilities and/or the harm. A reduction in any of these will result in the reduction of risk. Reducing threats involves making the threat less likely to attack. This involves reducing the amount of information available to the threat, developing an environment that is not attractive or simply isolating the assets being protected from the threat. Reducing vulnerabilities involves security technical configuration, security operational procedures, and education and awareness. Reducing harm involves detection, response and recovery.

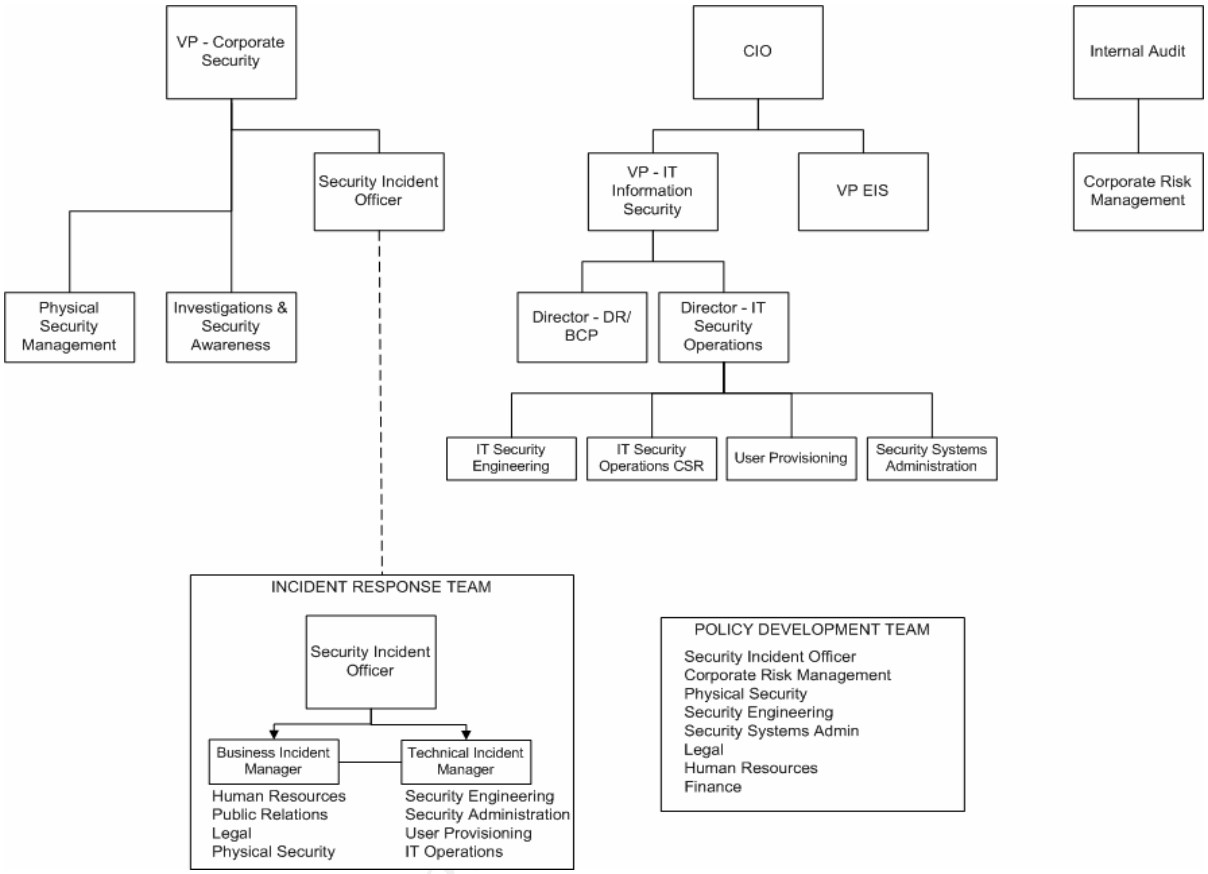
Controls from each layer in each model will be implemented as determined necessary by a risk assessment. A single control may be considered as part of multiple layers from multiple models. The risk assessment will determine if adequate coverage has been achieved thus reducing risk to an acceptable level.

1.2. Organizational Structure

The GIAC Enterprises information security program will require an organizational structure designed to support the security program requirements. The following organizational chart describes such a structure.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

1.2.1. Organization Chart



1.2.2. Organizational Overview

There are three major business units that play a primary role in the proposed information security program; Corporate Security, Information Technology and Internal Audit. In addition, there a number of other business units that play a secondary role including the legal department, finance and the various GIAC Enterprises profit centers (i.e. business unit 1, business unit 2, GIACEnterprises.com, etc.)

1.2.3. Corporate Security

Corporate Security, headed by the Vice President of Corporate Security, consists of two business units; “Physical Security” and “Investigations and Awareness”. The overall goal of Corporate Security is the enforcement of security objectives including the investigations of suspected non-compliance and security breaches. The “Security Incident Officer” position also resides in Corporate Security. This is the executive position that is responsible for leading security investigations and incident management

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

1.2.3.1. Physical Security

Physical security reports to the VP of Corporate Security and is involved with the protection of GIAC Enterprises properties, facilities and personnel. This business unit is concerned with establishing the physical perimeter of GIAC Enterprises facilities. It is responsible for controlling access to those facilities and securing areas within those facilities. Physical Security is also responsible for acting against threats to GIAC Enterprises properties, facilities and personnel and acting as a liaison between GIAC Enterprises and official law enforcement authorities (local police, state police, FBI, Secret Service, etc.).

1.2.3.2. Investigations and Awareness

Investigations and Awareness (I & A) reports to the VP of Corporate Security and is involved in promoting security (physical and information) awareness and education. I & A responds to suspected security breaches and conducts investigations and forensics. I & A acts on behalf of the VP of Corporate Security to enforce compliance with existing security policies and standards.

1.2.3.3. Security Incident Officer

The Security Incident Officer is the executive who leads security investigations. This individual determines when an incident response team is activated, determines which members of the response team are activated and acts as the direct supervisor for all activated team members for the duration of the response.

1.2.4. Information Technology

Information Technology, headed by the Vice President and Chief Information Officer, consists of two business units who are directly involved with information security; "IT Information Security (ITIS)" and "Enterprise Infrastructure Services (EIS)". The overall goal of Information Technology as it relates to security is the design, implementation and administration of security technology and the securing of GIAC Enterprises information assets.

1.2.4.1. Enterprise Infrastructure Services

EIS, headed by the Vice President of Enterprise Infrastructure Services, is responsible for the design, implementation and administration of GIAC Enterprises systems, applications and devices in accordance with established security policies and standards. The VP of EIS reports directly to the CIO.

1.2.4.2. IT Information Security

IT Information Security, headed by the Vice President of IT Information Security, is responsible for performing all disaster recovery, business continuity and security operations functions. Reporting to the VP of IT Information Security are the Director of Disaster Recover/Business Continuity Planning (DR/BCP) and the Director of IT Security Operations.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

1.2.4.3. Disaster Recovery/Business Continuity Planning (DR/BCP)

DR/BCP is concerned with two similar but separate goals. Business Continuity Planning (BCP) is concerned with maintaining critical business operations in the event of a disrupting event. This involves the use of redundant (hot, warm and cold) recovery sites, data backups, off-site storage, evacuation planning and similar technologies and concepts. Disaster Recovery (DR) is concerned with the restoration of normal business activities and the migration of operations from disaster sites to primary operational facilities.

1.2.4.4. IT Security Operations

IT Security Operations consists of four groups; User Provisioning, IT Security Engineering, IT Security Systems Administration and IT Security Operations Customer Service.

User Provisioning

This group is responsible for adding, managing and removing user access on GIAC Enterprises systems and applications. User provisioning involves granting user access to systems and applications in accordance with established policies and standards, maintaining systems authorization records that indicate "who has access to what", modifying user permissions as necessary and removing access permissions in a timely manner.

IT Security Engineering

This group is responsible for the design and development of new security related systems or the security components of systems. This includes the development of encryption toolkits, credit card processing security features, PKI, etc. This group also works with the IT engineering group to ensure that new systems comply with security standards and utilize existing security technology effectively. This group also develops technical security standards in accordance with established policies and ensures that new system designs comply with the policies and standards.

IT Security Systems Administration

This group is responsible for the security administration of Windows, Linux, Solaris, Firewalls, Intrusion Detection Systems, Security Applications, authentication systems and network devices. This group has "root", "administrator" or similar access to all systems and devices. This group grants "least privilege" permissions to other non-security administrators on an as-needed basis. The Security Systems Administration group is responsible for real-time and periodic review of security related log files.

IT Security Operations Customer Service

This group acts as a liaison between the IT security operations and the various business units. The goal of this group is to bring security concerns and

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

requirements to the business units while conveying business unit concerns to IT Information Security.

1.2.5. Internal Audit

1.2.5.1. Compliance Verification

Internal Audit provides the critical risk assessment and oversight functions of this program. Internal Audit verifies compliance with all security policies and that key processes such as new system development and change management have been performed correctly. Internal Audit is empowered to conduct scheduled, formal security audits as well as ad hoc inspections. Internal Audit also has the ability to require that managers conduct information security reviews. This will involve Internal Audit sending a manager a checklist containing security items. The manager will then be required to certify that he or she (and his or her employees) is in compliance. That manager will then be held accountable for that certification.

1.2.5.2. Corporate Risk Management

In the event that a situation occurs that has not been adequately addressed by the implemented policies and standards or that requires non-compliance with the established policies, Internal Audit will assess the level of risk and will determine if, based on the business need, the risk is acceptable.

1.2.6. Human Resources

Human Resources acts as the liaison between IT/Information Security/Physical Security/Audit/Legal and GIAC Enterprises employees. HR is responsible for distributing security related material to new employees and part of a security education and awareness program and for collecting non-disclosure, confidentiality and consent-to-monitoring agreements. HR will be responsible for employee records management including verification of the completion of education or training programs. HR is involved in the review, approval, maintenance, modification and eventual retirement of security policies. HR is also involved when the response to and investigations of a security incident involve interactions with GIAC Enterprises personnel.

1.2.7. Legal

The Legal department is responsible for ensuring knowledge and understanding of and compliance with relevant laws and regulations. These laws include local, state, federal and international regulations affecting information security and the use of technology. Legal should be involved in the review, approval, maintenance, modification and eventual retirement of security policies.

1.2.8. Incident Response Team

This team is formed to deal with information security incidents. The team consists of a set number if individuals. However, various subsets of the members may be called upon do deal with a security incident according to the type and severity of the incident. The team should consist of two distinct

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

functional units, business and technical. Each of these functional units will have an individual designated as its lead. The business and technical unit leads report to the Security Incident Officer (SIO), who, in turn, reports to the Chief Security Officer.

The business team members should consist of representatives from:

- GIAC Enterprises business units
- Human Resources
- Public Relations
- Legal
- Physical Security

The technical team members should consist of representatives from:

- Security Engineering
- User Provisioning
- Security System Operations
- IT Operations
- DR/BCP

The type, severity and scope of the incident affect the members of the incident response team that are activated for a given incident. The Security Incident Officer (SIO) will make this determination. Once the team members are activated, their primary responsibility must be to fill their incident response role. Other, day-to-day job functions must be reassigned or postponed for the duration of the response process. When activated, team members should report to their unit (business or technical) lead and ultimately to the SIO. The SIO must have the authority to activate team members and must be the only individual who can deactivate them.

It is important to note that not all team members will be activated for any given incident.

The incident response team should meet regularly to review their roles and responsibilities. They should receive targeted information about incidents and incident response as part of the overall security awareness and education program. The team should conduct quarterly “mock response” exercises to maintain competency and to ensure the processes in place are effective. , The mock response exercise may be postponed if an actual response involving the majority of team members occurs.

1.2.9. Policy Development Team

This team is responsible for the development, approval, review and distribution of all information security policies. To ensure balanced and effective policies, the team must consist of members from:

- IT Security Engineering
- IT Security System Administration

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

- Legal
- Human Resources
- Investigations and Security Awareness
- Internal Audit
- Physical Security
- Finance

The information security policy management team should be led by the Security Incident Officer. The process of decision making (approving policies, etc.) should require a simple majority.

1.3. Operational Requirements

The GIAC Enterprises information security program is comprised of controls and a support structure. These can be either technological or operational in nature. Operational program components include specific controls and structures required by controls to function efficiently.

1.3.1. Ownership

Ownership is the concept that assigns responsibility to specific individuals or groups. Ownership will be determined for applications, information, systems, devices and security requirements. Establishing ownership serves two critical functions. First, clearly defined ownership allows individuals to be held accountable for performing their assigned security related functions. Lack of clearly defined ownership allows an individual to deny responsibility for non-compliance with security requirements. Second, ownership reduces the risk that individuals or groups will have conflicts over who has control over a specific asset or function. Lack of clearly defined ownership can lead to multiple groups attempting to comply with requirements in different ways, each assuming they have the authority to do so.

The GIAC Enterprises CEO is the ultimate owner of all GIAC Enterprises assets and processes. The CEO, however, can delegate "operational ownership" to appropriate executives. These executives can, in turn, delegate operational ownership downward. The furthest extent to which operational ownership can be delegated is to the level of "department head" or "department manager". End users, unless they are also managers or executives, cannot be designated as owners.

1.3.2. Data Classification

Data classification is the process by which data and related assets are grouped and labeled according to their sensitivity. Each classification group is related to a set of requirements and responsibilities that define how data of that classification is to be protected, handled, transported, stored and disposed of. Without a data classification program, it becomes the responsibility of each GIAC Enterprises employee to independently determine the sensitivity of a particular piece of data and then to understand how it should be handled. Formalized data classification

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

removes much of this ambiguity and promotes proper security for data of that sensitivity.

In the GIAC Enterprises information security program, Data classification will be the responsibility of the data owner or designee. Owners (as described in section 3.1 of this document) must define the classification that will be assigned to the various types of data within their operational unit. Owners can delegate classification labeling requirements, in accordance with established policy, to individuals including end users; however, the owner will be ultimately responsible for compliance.

1.3.3. Oversight

A detailed security program, complete with policies, standards, technology and awareness, will be of little value if there is no oversight. Oversight involves the verification that security requirements are being complied with. The GIAC Enterprises oversight process will involve third-party and internal assessments. Third-party assessments involve compliance verification by an individual or individuals who are not responsible for actual compliance. This function can be fulfilled by the GIAC Enterprises Internal Audit department or by an external, non-GIAC Enterprises entity. As this type of oversight requires significant resources, self-assessments will also be a part of the GIAC Enterprises security program. Self-assessments involve individual business units providing assurance they are following security requirements. The individual providing such assurance will be responsible for the accuracy of the report. These assurances can be verified on an "as needed" basis by GIAC Enterprises Internal Audit.

To be effective, audits must be performed against an established set of policies and standards. Without such formal documentation, audits can be subjective and compliance is left to the discretion of the auditor.

Audits must also be timely. If a business unit or system is audited once every five years, there is a high risk that significant non-compliance will result. While the resources necessary to conduct frequent audits using the Internal Audit department or an external auditor can be costly, self-assessments, where business units certify they are in compliance, can relieve much of the demand. In this scenario, department heads would be furnished with a compliance checklist. They would be responsible for ensuring that their department is fully in compliance or for providing reasons why compliance cannot be achieved. Internal or external auditors would then need only to spot check the business units and hold the department head accountable and responsible for any discrepancies.

1.3.4. Accountability

The GIAC Enterprises information security program will actively involve holding individuals and groups accountable for their assigned security responsibilities. This will involve educating personnel as to their responsibilities and taking action

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

against those who do not comply. Such action will include, as appropriate, reprimands, reassignment, financial consequences, termination, civil or criminal action. Holding individuals accountable provides two distinct benefits to the security of GIAC Enterprises. It allows GIAC Enterprises to address individuals who are responsible for decreases in security or potential compromise. It also provides a deterrence factor, since individuals who know they are likely to be disciplined for non-compliance are less likely to intentionally fail to comply with security requirements.

1.3.5. Incident Response

Due to the dynamic nature of information security, the complexity of the systems involved and the frequency of new vulnerability discovery, it is infeasible to attempt to eliminate the risk of a security breach. Protective measures should be supplemented with the ability to detect security incidents, log and track activities and respond to suspected security incidents in an effective and timely manner. GIAC Enterprises incident response will involve those activities necessary for response preparation, response performance and follow-up. These activities will include:

- Developing network and systems documentation specifically for incident response
- Verifying that monitoring and logging has been effectively implemented
- Addressing monitoring, consent and notification
- Proactively and reactively reviewing security related log and monitor data
- Performing actual incident response
- Initiating investigations
- Suggesting mitigation strategies to reduce the risk of future occurrences
- Reviewing the response process

The goals of GIAC Enterprises incident response will be to:

- Determine if an incident has actually occurred
- Determine if an incident presents a disaster recovery or business contingency problem
- Promote the accumulation of accurate information relating to the security incident
- Protect privacy rights established by law or policy
- Minimize disruption to business operations
- Minimize public relations problems by ensuring accurate understanding and reporting of security incident information
- Allow for legal or civil recriminations against perpetrators
- Provide for accurate reports and useful recommendations

1.3.6. Investigations

“Investigations” is a sub-component of incident response and involves a detailed review of an incident in order to determine what was done, how and by whom. Investigations will involve the collection of evidence that may be used in future administrative, civil or criminal proceedings. The investigations process must be

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

conducted with great care to preserve evidence as, once evidence has been compromised, it frequently cannot be recovered. GIAC Enterprises investigations will involve a variety of technical and non-technical aspects including:

- Evidence handling
- Chain of custody maintenance
- Forensic data duplication
- Network traffic analysis
- Forensic system examination
- Legal review
- Personnel interviews

1.3.7. Policy and Standards Management

Security policies provide the formal and official description of information security requirements and objectives throughout the organization. While policies are designed to be relatively static, they will require management and maintenance. Policies will be reviewed and updated periodically to reflect current GIAC Enterprises business and security objectives. Occasionally, new policies will need to be created and policies, when no longer useful, will need to be retired. A key component of the GIAC Enterprises security program is a formal process for the management of these policies to ensure policy consistency and relevancy throughout the organization. This program will involve the input from affected business units and formal, executive level approval. The process will include a well defined policy lifecycle and review requirements. It will also clearly detail the process and requirements for policy development, approval, implementation, maintenance, review and retirement.

Like policies, standards must be managed. The process for standards management, however, will not be as involved as that for policies as standards are generally more detailed, more closely related to technology and have a more narrow effect. The standards management process will define the standards lifecycle and review requirements. It will also clearly detail the process and requirements for standard development, approval, implementation, maintenance, review and retirement. Technical standards will be owned by the CIO with maintenance delegated to IT departments in conjunction with appropriate business units. For example, the CIO will own the technical standard for the secure configuration and use of Peoplesoft. The maintenance of Peoplesoft security standards will fall on the IT Security Engineering working with Human Resources and Finance.

1.3.8. Education and Awareness

People can be one of an organization's greatest security strengths or one of its greatest weaknesses. Frequently, the difference between the two comes down to education and awareness. An uninformed user may give his or her password to the accounting system to a complete stranger. A user who has been educated

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

will not only refuse to disclose his or her password but will contact the proper GIAC Enterprises security personnel to report the incident.

The GIAC Enterprises security awareness and education program will be targeted to specific users and groups. GIAC Enterprises executives will receive different security information than technical security practitioners. The members of each group will be given the material appropriate for them. This focus ensures that individuals are not overloaded with excessive detail and that they do not get "turned off" by irrelevant information.

The GIAC Enterprises Security awareness and education will be repetitive. Overloading personnel with a massive amount of information will not be effective. Instead, GIAC Enterprises personnel will receive a simple, condensed message that will be repeated and reinforced. This ensures that GIAC Enterprises personnel understand, remember and can use the information provided.

Finally, GIAC Enterprises security awareness and education will be engaging. A pile of black and white documents dropped on and employee's desk will likely end up in the garbage. A colorful newsletter or a security trivia contest will keep the target audience involved.

Security education and awareness will take two distinct forms, competency and security awareness. Competency training will ensure that users are proficient with the tools and technologies they use on a daily basis. A security breach can occur as a result of improper use of an application or security feature as easily as from a technical vulnerability. Targeted competency training will range from the average end user to technical security practitioners. Security awareness training involves ensuring that each individual knows the role he or she plays in the overall GIAC Enterprises security program and why security is important to him or her.

1.3.9. Business Continuity

Traditional information security refers to the "CIA Triad". "CIA" refers to confidentiality, integrity and availability. Business continuity supports the availability aspect of the triad and involves all measures taken to continue business operations in the event of a disruptive event. The GIAC Enterprises business continuity process will involve the use of redundant data, hardware, services and facilities. Most of these components exist at GIAC Enterprises. However, the GIAC Enterprises information security program will expand on the existing features.

The business continuity plans will be documented in detail. In an emergency situation, personnel availability cannot be assured, therefore, the plans must provide information enough for qualified individuals who may be unfamiliar with the plans to be able to execute them. This ensures that, in the event of a severe disruption, documentation is available to be used by individuals capable of

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

reacting even if those individuals have not been previously trained in such a response.

GIAC Enterprises business continuity will enhance their process for providing redundancy and data backup requirements through standardization. GIAC Enterprises will create a set of business continuity service levels that will be applied, as needed to systems, devices and applications. These standard services will specify availability requirements, recovery prioritization, hardware redundancy, data backup type, backup frequency, media storage, rotation schedules, retention timeframes and any other business continuity relevant information.

1.3.10. Disaster Recovery

Disaster recovery is the process by which normal business operations are resumed in primary operational facilities. Disaster recovery occurs during and after the implementation of GIAC Enterprises business continuity contingencies and involves the ordered migration of business operations from disaster sites to the original or replacement primary facilities.

This security program component will involve the documentation of recovery plans. The plan documentation will be comprehensive and detailed enough to allow an individual unfamiliar with the plans to be able to implement it with a reasonable probability of success. This must be done as, in a disaster situation, the availability of personnel cannot be assured. The plan documents must account for this.

A key component of the disaster recovery planning will be the prioritization of systems and services to be restored to normal operations in the event of a disaster. This differs significantly from business continuity prioritization. Disaster recovery prioritization will identify the order in which systems that have been running in “disaster mode” or that have not been running at all will be returned to normal operations.

The disaster recovery plans will include the identification of alternate primary operational facilities to be used in the event that an existing primary operational facility is disabled. These backup facilities may be existing GIAC Enterprises facilities that will, after a disaster, server a dual role, they may be formal “cold sites” that will be converted to primary operational facilities after a disaster or they may be locations that, while no formal arrangements have been made, could serve as an operational facility if necessary.
The security program will also involve the development and training of recovery teams. These teams will have as their objective, the restoration of normal business operations in the event of a disaster.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

1.3.11. Change Management

Change management will not directly be a component of the GIAC Enterprises information security program remaining part of GIAC Enterprises IT operations. It will, however, be greatly affected by the program as security policy and standard compliance and security signoff will be requirements inherent to the change management process. The existing change management framework will remain intact; however, the strengthening of requirements, compliance, signoff, oversight and accountability will greatly enhance the process. Security considerations will be introduced at the beginning of the change management process and compliance with existing security policies and standards will be required. Where existing policies and standards do not adequately address a proposed change or where compliance with existing policies and standards is not possible, a risk assessment will be required. Failure to follow the change management process or to adequately address security considerations will result in disciplinary action.

1.3.12. Application Development

Like change management, new application or new system development will not directly be a component of the GIAC Enterprises information security program but will be greatly affected by it. Unlike change management, however, GIAC Enterprises does not have a formal process for introducing, maintaining and retiring systems or applications. A Systems (Software) Development Life Cycle (SDLC) will be required to supplement the security program.

The GIAC Enterprises SDLC will encompass all of the steps that GIAC Enterprises will follow when developing new applications or systems. The SDLC will include the steps required to be followed, the order of the steps, the business functions or individuals responsible and requirements for records-keeping. The GIAC Enterprises SDLC will contain the following main functions:

- **Conceptual Definition** - A basic description of the new product or program being developed, so that anyone reading it can understand the proposed project.
- **Functional Requirements and Specifications** - A list of requirements and specifications from a business function perspective.
- **Technical Requirements and Specifications** - A detailed description of requirements and specifications in technical terms.
- **Design** - Where the formal detailed design of the product or program is developed.
- **Coding** - The actual development of software.
- **Test** - The formal testing phase.
- **Implementation** - Where the software or product is installed in a production environment.

Each major function consists of several tasks that should be documented in flowchart notation with inputs, outputs, reports, decisions and approvals. GIAC Enterprises should consider building a workflow application to support all of this.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

The SDLC will require security input and information at each phase of the process as follows:

- **Conceptual** - Organization information security principles, policies and strategies
- **Functional Requirements and Specifications** – Functional information security requirements based on the performance of a risk assessment.
- **Technical Requirements and Specifications** – Technical information security requirements based on the performance of a risk assessment.
- **Design** - Enterprise security architecture and security product standards
- **Coding** - Development standards, practices, libraries and coding examples
- **Testing** - Test plans that show how to verify each security requirement
- **Implementation** - Procedures for integrating existing authentication, access controls, encryption, backup, etc.

This process integrates tightly into the change management process as a change to an existing system is an iteration of the life cycle process. When a change is needed, the entire process will start over requiring all of the information, input and validations present in the first time.

The GIAC Enterprises software or systems development life cycle process will include required approval steps at each major function. This will take the form of approval meetings with the appropriate stakeholders present. Security review will be required during the "functional requirements" and "testing" stages of the development lifecycle. This can be accomplished by including an information security representative in meetings occurring at these stages or by providing information security with sufficient information to provide security validation. During all other stages of the lifecycle the project owner will certify compliance with existing security policies and standards. It is important to note that if someone representing information security or risk management is not involved during the life cycle, there is an increased risk that a project lacking some key security component will be approved, only to become a problem in the future.

1.4. Technical Requirements

In addition to operational components, the GIAC Enterprises information security program will consist of technology. These technological components include security-specific software and the security features and functions of software such as operating systems and business applications. The security program technology components involve the implementation of new functionality and the secure configuration and use of existing technology.

1.4.1. Authentication

Information security is concerned with allowing authorized individuals and systems access to GIAC Enterprises data while simultaneously denying access to individuals and systems that are not authorized. The first step in that

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

determination is the identification and identity verification of individuals or systems attempting access. This process is referred to as authentication. Authentication involves two components, identification and identity verification. The more accurately an identity can be presented and verified, the more secure or strong the authentication. Without strong or secure authentication, an attacker can represent himself as an authorized individual and gain access to a protected system. In addition, weak authentication can allow a user to deny having accessed a system thereby making accountability difficult.

Authentication in the current GIAC Enterprises environment is provided using traditional username/password combinations and RSA SecurID[xxviii] two-factor authentication. Both methods have a place in the GIAC Enterprises environment. The GIAC Enterprises information security program will modify or expand each type of authentication.

Username/password – GIAC Enterprises will develop standards for use of secure passwords. These standards will specify minimum length, complexity, maximum lifetime, minimum lifetime and password reuse requirements. The GIAC Enterprises information security program will also include, where possible, technical mechanisms to enforce these requirements. The use of username/password combinations will be eliminated as a mechanism for authentication performing administrative functions on critical systems and devices. Username/password authentication will be conducted in as secure a manner as possible. GIAC Enterprises will prohibit the transmission of username/password information over a network in unencrypted form.

Two-factor Authentication – Two factor authentication will be used as the authentication method of choice for administrative functions on critical systems. Two-factor authentication will include both existing token-based technology and the introduction of digital certificates stored on smart cards.

1.4.2. Authorization

Authorization is the process of determining who can do what. The GIAC Enterprises security program will address authorization from three perspectives, the access control method, the process by which authorization is gained and removed and the technology used to enforce access control.

Role-Based Access Controls

The GIAC Enterprises security program will involve an access control method know as “role-based access control” or RBAC. This involves relating a user’s permissions to his or her job function. Users with the same job functions will generally have similar access requirements. As part of the security program GIAC Enterprises application owners will identify the different functions performed by the users of their systems and the appropriate access control permissions and restriction for each function. As new users are added or as users change functions, they will simply be transferred to a new “role” and will be

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

given a new set of access permissions based on their business function. It is important to note that a single individual can be assigned to more than one role as an individual may perform more that one function for GIAC Enterprises. It will be the responsibility of a user's manager to determine the various functions available on systems and to appropriately assign users to appropriate roles. A portion of the security program education and awareness program will involve providing managers with the education and training necessary to perform this function.

User Provisioning Input
Once a manager has determined the appropriate roles for a given user, changes must be made to the system(s) in question. This process involves an access request, access approval, system modification and access recording. The GIAC Enterprises information security program will include a system that will establish a standardized workflow and an interface for performing these activities. This "user provisioning" solution will provide an interface that managers throughout the GIAC Enterprises enterprise can use to request the addition, modification and termination of user access permissions. This information will be sent to the security administration group who will validate the request and make the appropriate changes.

User Provisioning Accountability
The security administration group will not approve or deny access requests. It is the responsibility of the requesting manager to ensure that access requests are appropriate. Those managers will be held accountable for inappropriate access.

User Provisioning Output
Where possible, the user provisioning system will automate the process of making changes to systems, reducing staffing requirements for the security administration group. Until such a solution can be implemented, the security administration group will make all access control modifications to GIAC Enterprises systems.

Access Tracking
The GIAC Enterprises information security program will involve the recording of user access rights to GIAC Enterprises systems. Where possible, the granular details such as specific access rights and restrictions will be recorded. At a minimum, a listing of which systems each user has access to will be maintained. This will ensure appropriate and timely actions can be taken in the event that user access must be revoked.

1.4.3. Accountability

The GIAC Enterprises information security program will involve an increased use of monitoring and reporting controls. This will serve two functions, it will track what authorized users do to ensure they are not performing inappropriate or unauthorized activities and it will increase the ability of GIAC Enterprises security

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

to detect and respond to security violations or breaches. GIAC Enterprises accountability and monitoring will involve a number of components including:

- **System and Device Logging** – The majority of GIAC Enterprises systems, applications and devices have the capability of tracking and logging events that affect the system. This functionality will be utilized to a greater extent than it has been. Where possible, these log messages will be recorded to a centralized log server. This allows for easy access to the information by GIAC Enterprises security and makes it more difficult for an attacker to compromise the log data.
- **Network Intrusion Detection (NIDS)** – GIAC Enterprises currently utilizes network intrusion detection sensors to monitor network traffic for signs of an attack. The configuration and placement of these sensors will be modified and optimized to increase their effectiveness.
- **Host Intrusion Detection (HIDS)** – GIAC Enterprises monitoring will be enhanced by the use of host-based intrusion detection sensors on mission-critical systems. These sensors will detect and report on signs of attack activity against specific hosts. HIDS provides separate and complementary information to network-based sensors.
- **Integrity Verification** – An additional component of GIAC Enterprises monitoring will be integrity verification. Integrity verification systems monitor the state of data to ensure that unauthorized changes are not made. This type of solution will be applied to network devices and to system configuration files that are expected to remain relatively static. If an attacker compromises a system or device and attempts to modify a protected file or configuration, GIAC Enterprises security will be alerted. Integrity verification systems have an advantage over a manual review of configuration files in that a minor change in a large configuration file can be easily overlooked during a manual review but will be readily apparent to an automated solution.
- **Event Correlation** – The amount of logging and monitoring data that will be collected as a part of the GIAC Enterprises information security program will be significant. The information will be generated by and distributed across a variety of systems throughout the enterprise creating challenges in the collection and review of the data. To address these challenges, the GIAC Enterprises information security program will include an event collection and correlation solution. The solution will receive security related information from systems, devices, HIDS sensors, NIDS sensors and integrity verification systems. The information will be correlated and rated according to severity and interest to GIAC Enterprises security. This will allow GIAC Enterprises security to work with a vast amount of information quickly, accurately and effectively.

1.4.4. Public Key Infrastructure

The GIAC Enterprises information security program will include a public key infrastructure or PKI. A PKI consists of a number of components including one or more certificate authorities, one or more registration authorities, digital

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

certificates, information stores and supporting policies, standards and procedures. The PKI will provide GIAC Enterprises with a variety of enhanced security capabilities. When combined with smart cards, the PKI will provide a single credential that can be used for controlling both physical and logical access where currently multiple credentials administered by multiple business units are currently being used.

Many applications support digital certificates as a method of authentication. Most other applications can be configured or modified to support their use. Enabling certificate-based authentication, where possible, can provide a reduced-sign-on environment where users present their credential once and are granted seamless access to multiple systems. When certificates are stored on smart cards, this creates a more secure environment while decreasing demands on end users.

The PKI will empower end users to utilize encryption while performing their assigned tasks easily and efficiently. This will enhance the ability of end users to comply with data classification and encryption policies and provide an easy to use method for encrypting files, email or other sensitive data. The certificates generated by the PKI will also be used to enable secure, encrypted access to web-based applications and data.

1.4.5. Encryption

Encryption will play an increased role in the GIAC Enterprises information security program. A PKI will provide a method for encrypting email messages and web-based applications. In addition, the security program will include the encryption of data “at rest”. While there are many situations where data may require encryption, the program will focus on two, in databases and on laptop file systems.

The program will require that sensitive data such as credit card information be encrypted when stored in databases of any kind. This will include commonly recognized relational databases such as Oracle or SQL, LDAP databases and any other repository of sensitive information. The GIAC Enterprises information security program will include the development of encryption toolkits that can be used to integrate encryption capabilities into new and existing applications in a consistent format.

GIAC Enterprises laptop computers are highly susceptible to compromise. Once an unauthorized individual has physical possession of a GIAC Enterprises laptop computer they will be able to access any sensitive information stored on it. To reduce this risk, the GIAC Enterprises information security program will include file system encryption for laptops and other mobile computing devices containing sensitive information.

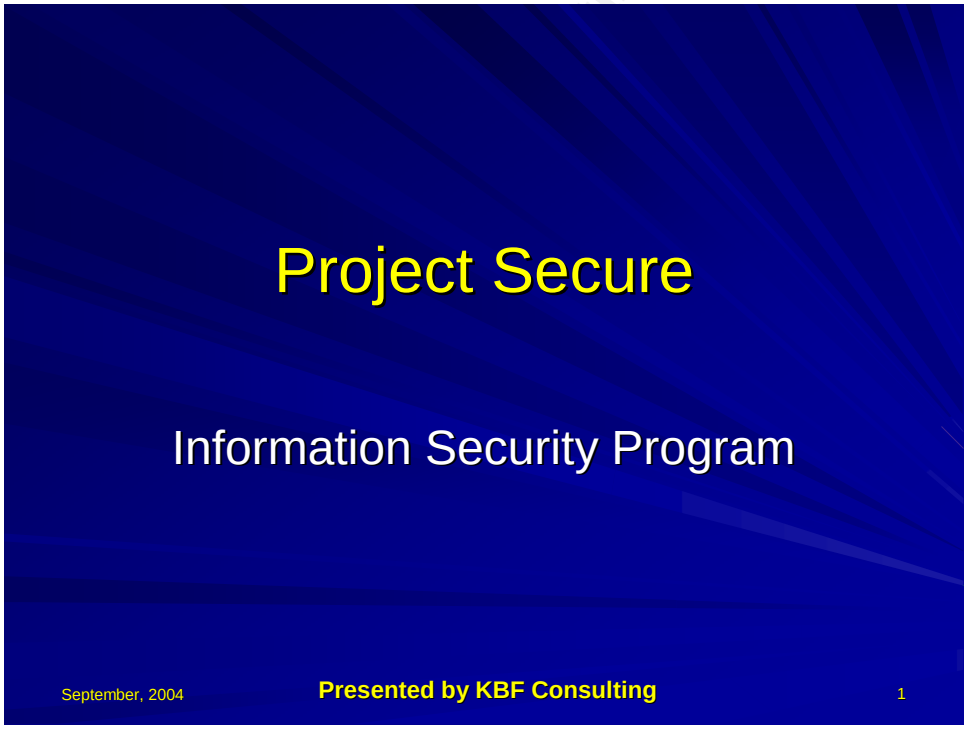
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

1.4.6. Firewalls

Firewalls provide a mechanism for segregating networks of a higher trust level from those less trusted. GIAC Enterprises currently uses a variety of firewall platforms across their enterprise to segregate the internal network from the Internet and to segregate various components of their internal network from each other (i.e. MCN, admin, EBU, etc.). The GIAC Enterprises information security program will continue to rely on the use of firewalls. The administration of these firewalls will be migrated to the information security systems administration group. This group will maintain "administrator" or "root" access to these devices. Permissions to perform specific functions on firewalls will be delegated to members of other groups, as required.

The GIAC Enterprises information security program will also involve the consolidation of firewalls to a limited number of platforms. Ideally, a single standard firewall platform will be identified and the variety of existing platforms will be migrated to this standard. This will decrease the support requirements as those responsible for firewall support and administration will not be required to be familiar with a host of platforms. Additionally, as each firewall platform is subject to the discovery and publication of vulnerabilities requiring the implementation of upgrades or patches, a reduce

2. Section B – Project Overview Presentation



© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

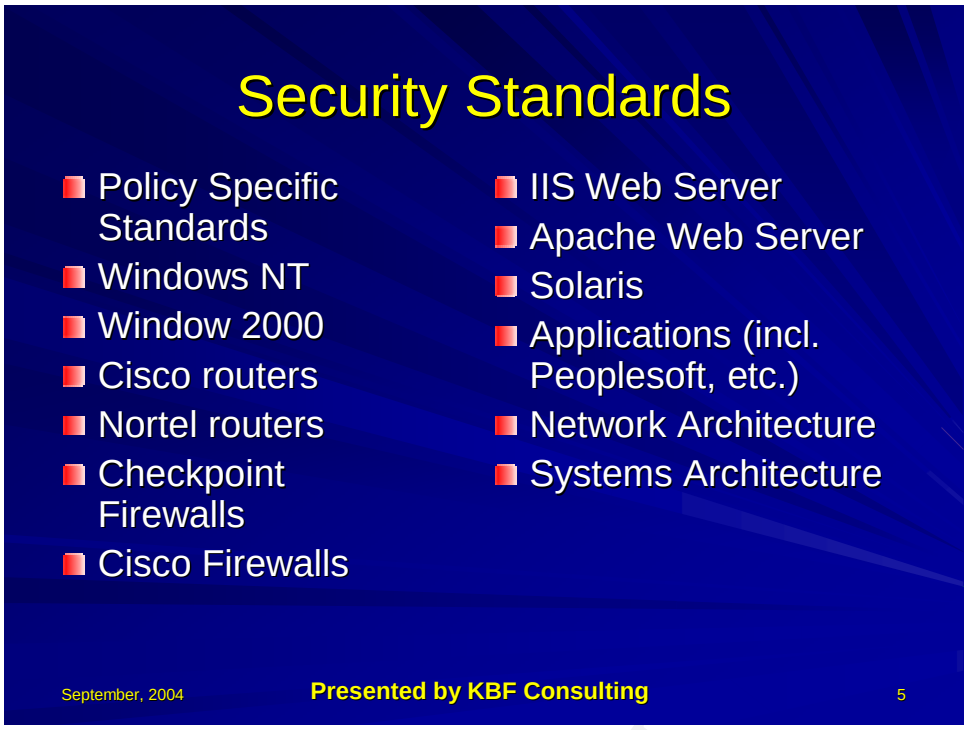
- **Risk Assessment** – The process of reviewing the risks posed to GIAC Enterprises assets and determining if they are acceptable in relation to the potential damage and the cost of mitigation. (Audit)
- **Education and Awareness** – 2 goals – make sure everyone is aware of how they support security and is capable of doing so

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

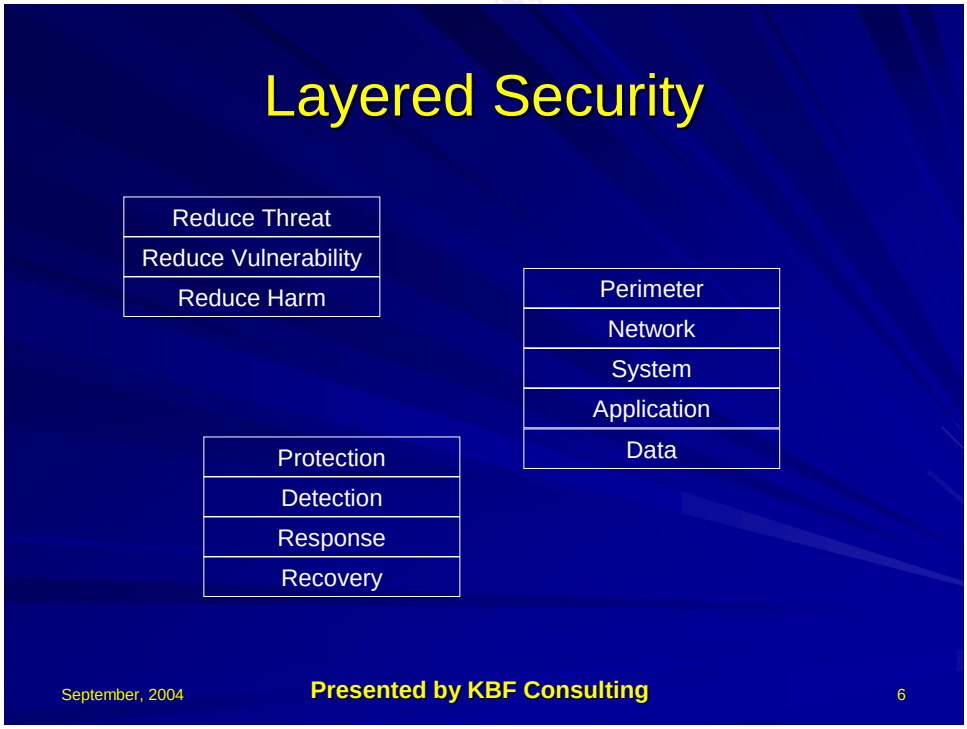
- Includes technical, non-technical, executive, managers, security practitioners and average end users (VP Corporate Security)
- **Governance**
- External – ensure knowledge of and compliance with laws and regulations (legal + audit)
- Internal – ensure GIAC employees knowledge of and compliance with policies, standards, procedures, etc. (business units + audit)
- **Oversight** – trust but verify – self assessments with internal audit review
- **Policies and Standards** – Upcoming slides
- **Layered Security** – Upcoming slides

- Recommended suite of information security policies
- All work together – the effect is a single, large policy broken down into logical sections

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

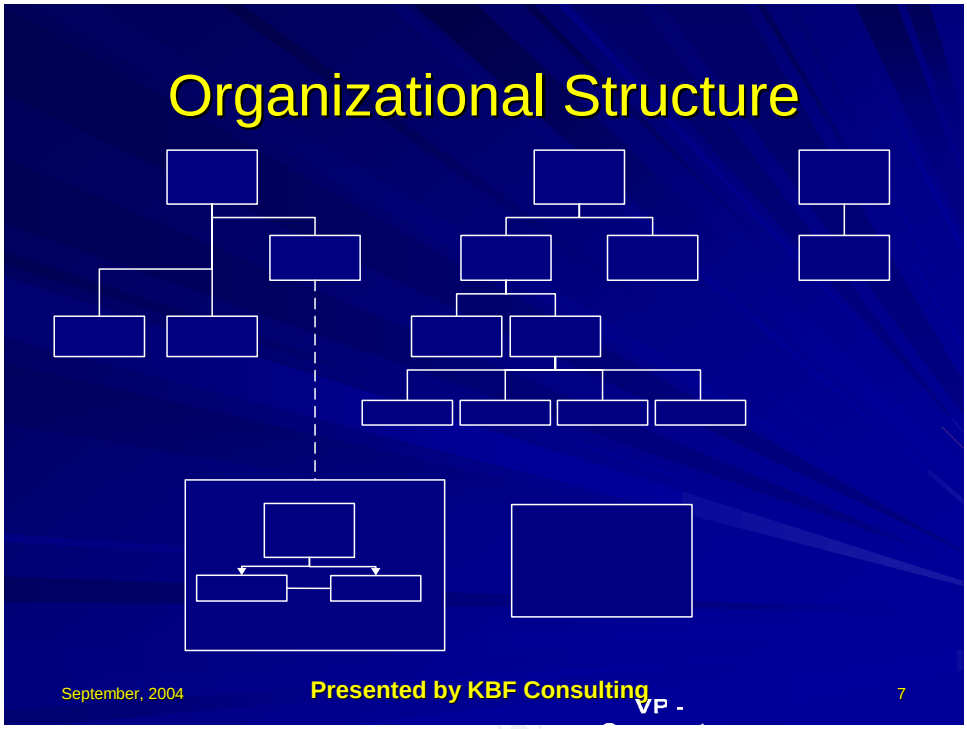


- Representative sample of standards based on prominent technology and applications
- May be business unit specific



© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

- Provide a method of measurement and metrics for audit to use to ensure risk as been reduced to an acceptable level
- Holistic view using three perspectives
- Make audit metrics validate the 3 views



© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Organizational Structure (3)

- Information Technology
  - Enterprise Information Services
  - IT Information Security
  - Disaster Recover/Business Continuity
  - IT Security Operations
    - User Provisioning
    - IT Security Engineering
    - IT Security Systems Administration
    - IT Security CSR

September, 2004 **Presented by KBF Consulting** 9

Organizational Structure (4)

- Internal Audit
  - Compliance Verification
  - Corporate Risk Management
- Legal
  - External Governance
- Human Resources

September, 2004 **Presented by KBF Consulting** 10

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

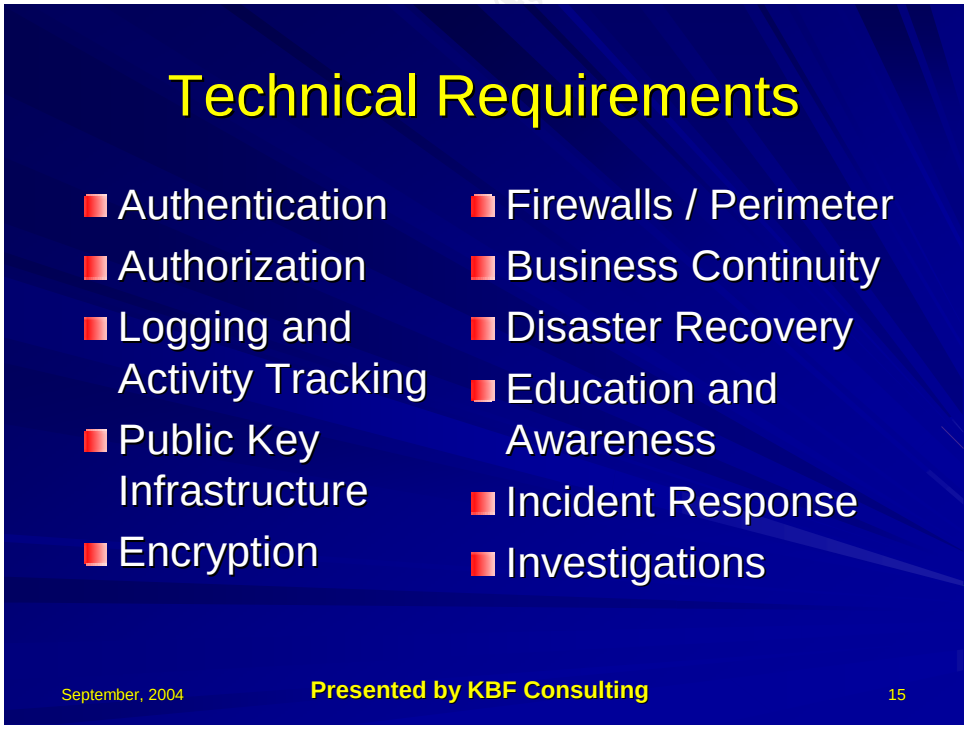
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

- **Ownership** – PeopleSoft, Specific databases, Hardware, etc.
- **Data Classification** – data is classified by owners – validated by audit
- **Secure Change Management** – apply security standards and "stop checks" within the change management process
- **Secure Application Development** – The program documents outlines a systems development life cycle (SDLC) and how security fits
- **Oversight** – Audit produces self audit checklists – owners verify compliance – audit will validate
- **Accountability** – Owners will be held accountable for compliance – non-compliance will be dealt with as needed

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

- DR and BCP fall under the new VP of Information Security
- Education, Awareness, Incident Response and Investigations fall under the VP of Corporate Security



© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

References

[i] Certified Information Systems Security Professional (CISSP) – International Information Systems Security Certification Consortium (ISC)2
URL: http://www.isc2.org

[ii] Cisco Certified Internetworking Expert (CCIE) – Cisco Systems
URL: http://www.cisco.com/en/US/learning/le3/ccie/index.html

[iii] Cisco Certified Network Professional (CCNP) – Cisco Systems
URL:
http://www.cisco.com/en/US/learning/le3/le2/le37/le10/learning_certification_type_home.html

[iv] Cisco Certified Design Professional (CCDP) – Cisco Systems
URL: http://www.cisco.com/en/US/learning/le3/le2/le37/le5/learning_certification_type_home.html

[v] Microsoft Certified Systems Engineer (MCSE) – Microsoft Corporation
URL: http://www.microsoft.com/learning/mcp/mcse/default.asp

[vi] Microsoft Certified Solutions Developer (MCSD) – Microsoft Corporation
URL: http://www.microsoft.com/learning/mcp/mcsd/default.asp

[vii] Microsoft Certified Application Developer (MCAD) – Microsoft Corporation
URL: http://www.microsoft.com/learning/mcp/mcad/default.asp

[viii] Microsoft Certified Database Administrator (MCDBA) – Microsoft Corporation
URL: http://www.microsoft.com/learning/mcp/mcdba/default.asp

[ix] Sun Certified Systems Administrator (SCSA) – Sun Microsystems
URL: http://training.sun.com/US/certification/solaris/sysadmin.html

[x] Sun Certified Network Administrator (SCNA) – Sun Microsystems
URL: http://training.sun.com/US/certification/solaris/netadmin.html

[xi] RSA Certified Security Engineer – SecurID (RCSE) – RSA Security
URL: http://www.rsasecurity.com/node.asp?id=1393&node_id=

[xii] RSA Certified Security Engineer – ClearTrust (RCSE) – RSA Security
URL: http://www.rsasecurity.com/node.asp?id=1396&node_id=

[xiii] GIAC Certified Forensics Analyst (GCFA)
URL: http://www.giac.org/subject_certs.php#GCFA

[xiv] Project Management Professional (PMP) – Project Management Institute
URL: http://www.pmi.org/info/PDC_PMP.asp

[xv] Sarbanes-Oxley
URL: http://corporate.findlaw.com/industry/corporate/docs/publ107.204.html

[xvi] International Organization of Standardization - ISO17799
Brittish Standards Institute, Information Technology – Code of Practice for Information Security Management (BS ISO/IEC 17799:2000, BS 7799-1:2000), February 15, 2001

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

URL: http://www.iso.org/iso/en/ISOOnline.openerpage

[xvii] SysAdmin, Audit and Network Security Institute – SANS

- Center for Internet Security Benchmarks and Scoring Tool for Windows XP Professional, Windows Server 2003, Windows 2000 and Windows NT - URL: http://www.cisecurity.org/bench_win2000.html
- CIS Level-1 Benchmark and Scoring Tool for Solaris - URL: http://www.cisecurity.org/bench_solaris.html
- CIS Level-1 Benchmark and Scoring Tool for Linux - URL: http://www.cisecurity.org/bench_linux.html
- CIS Level-1 / Level-2 Benchmarks and Audit Tool for Cisco IOS Routers and PIX firewalls - URL: http://www.cisecurity.org/bench_cisco.html
- Firewall Checklist - URL: http://www.sans.org/score/checklists/FirewallChecklist.doc
- ISO 17799 Checklist - URL: http://www.sans.org/score/checklists/ISO_17799_checklist.doc
- Windows 2000/XP DSS Auditing - URL: http://www.sans.org/score/checklists/Win2K_XP_Checklist.doc

[xviii] National Security Agency (NSA)

- The 60 Minute Network Security Guide - URL: http://www.nsa.gov/notices/notic00004.cfm?Address=/snac/support/sixty_minutes.pdf
- Defense In Depth – A Practical Strategy for Achieving Informaiton Assurance in Today's Highly Networked Environments - URL: http://www.nsa.gov/notices/notic00004.cfm?Address=/snac/support/defenseindepth.pdf
- Guide to the Secure Configuration of Solaris 8 - URL: http://www.nsa.gov/notices/notic00004.cfm?Address=/snac/os/sunsol/Solaris8.pdf
- Guide to Securing Microsoft Windows NT Networks - URL: http://www.nsa.gov/notices/notic00004.cfm?Address=/snac/os/winnt/winnt_networks.pdf
- Guide to Securing Microsoft Windows XP - URL: http://www.nsa.gov/notices/notic00004.cfm?Address=/snac/os/winxp/winxp.pdf
- Microsoft Windows 2000 Network Architecture Guide - URL: http://www.nsa.gov/notices/notic00004.cfm?Address=/snac/os/win2k/w2k_net_arch_guide.pdf
- Guide to Securing Windows 2000 Group Policy - URL: http://www.nsa.gov/notices/notic00004.cfm?Address=/snac/os/win2k/w2k_group_policy.pdf
- Guide to Securing Windows 2000 Group Policy – Security Configuration Toolset - URL: http://www.nsa.gov/notices/notic00004.cfm?Address=/snac/os/win2k/w2k_group_policy_toolset.pdf
- Group Policy Reference - URL: http://www.nsa.gov/notices/notic00004.cfm?Address=/snac/os/win2k/w2k_group_policy_ref.pdf
- Guide to Securing Windows 2000 Active Directory - URL: http://www.nsa.gov/notices/notic00004.cfm?Address=/snac/os/win2k/w2k_active_dir.pdf
- Guide to Securing Windows 2000 DNS - URL: http://www.nsa.gov/notices/notic00004.cfm?Address=/snac/os/win2k/w2k_dns.pdf
- Guide to Securing Windows 2000 Encrypting File System - URL: http://www.nsa.gov/notices/notic00004.cfm?Address=/snac/os/win2k/w2k_encrypt_file_sys.pdf
- Guide to Securing Windows 2000 File and Disk Resources - URL: http://www.nsa.gov/notices/notic00004.cfm?Address=/snac/os/win2k/w2k_file_disk_resource.pdf
- Guide to Securing Windows 2000 Schema - URL: http://www.nsa.gov/notices/notic00004.cfm?Address=/snac/os/win2k/w2k_schema.pdf
- Guide to Securing Windows NT/9x Clients in a Windows 2000 Network - URL: http://www.nsa.gov/notices/notic00004.cfm?Address=/snac/os/win2k/w2k_winnt_9x_clients.pdf

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

- Guide to Securing Windows 2000 Kerberos Settings - URL: http://www.nsa.gov/notices/notic00004.cfm?Address=/snac/os/win2k/w2k_kerberos.pdf
- Windows Server 2003 Security Guide - URL:http://www.nsa.gov/notices/notic00003.cfm?Address=http://www.microsoft.com/downloads/details.aspx?FamilyId=8A2643C1-0685-4D89-B655-521EA6C7B4DB&displaylang=en
- Router Security Configuration Guide - URL: http://www.nsa.gov/notices/notic00004.cfm?Address=/snac/routers/cisco_scg-1.1b.pdf
- Cisco IOS Switch Security Configuration Guide - URL: http://www.nsa.gov/notices/notic00004.cfm?Address=/snac/os/switch-guide-version1_01.pdf

[xix] National Institute of Standards and Technology (NIST)

- Security Considerations in the Information Systems Development Lifecycle - URL: http://csrc.nist.gov/publications/nistpubs/800-64/NIST-SP800-64.pdf
- Electronic Authentication Guide - URL: http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63v6_3_3.pdf
- Computer Security Incident Handling Guide - URL: http://csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf
- Guide for Mapping Types of Information and Information Systems to Security Catrgories - URL: http://csrc.nist.gov/publications/nistpubs/800-60/SP800-60V1-final.pdf
- Appendix to Guide for Mapping Types of Information and Information Systems to Security Catrgories - URL: http://csrc.nist.gov/publications/nistpubs/800-60/SP800-60V2-final.pdf
- Security Metrics Guide for Information Technology Systems - URL: http://csrc.nist.gov/publications/nistpubs/800-55/sp800-55.pdf
- Use of the Common Vulnerabilities and Exposures (CVE) Vulnerability Naming Scheme - URL: http://csrc.nist.gov/publications/nistpubs/800-51/sp800-51.pdf
- Building an Information Technology Security Awareness and Training Program - URL: http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf
- Wireless Network Security: 802.11, Bluetooth and Handheld Devices - URL: http://csrc.nist.gov/publications/nistpubs/800-48/NIST_SP_800-48.pdf
- Security Guide for Interconnecting Information Technology Systems - URL: http://csrc.nist.gov/publications/nistpubs/800-47/sp800-47.pdf
- Security for Telecommuting and Broadband Communications - URL: http://csrc.nist.gov/publications/nistpubs/800-46/sp800-46.pdf
- Guidelines on Electronic Mail Security - URL: http://csrc.nist.gov/publications/nistpubs/800-45/sp800-45.pdf
- Guidelines on Securing Public Web Servers - URL: http://csrc.nist.gov/publications/nistpubs/800-44/sp800-44.pdf
- System Administrators Guide for Windows 2000 Professional - URL: http://csrc.nist.gov/itsec/guidance_W2Kpro.html
- Guideline on Network Security Testing - URL: http://csrc.nist.gov/publications/nistpubs/800-42/NIST-SP800-42.pdf
- Guidelines on Firewalls and Firewall Policy - URL: http://csrc.nist.gov/publications/nistpubs/800-41/sp800-41.pdf
- Procedures for Handling Security Patches - URL: http://csrc.nist.gov/publications/nistpubs/800-40/sp800-40.pdf
- Contingency Planning for Information Technology Systems - URL: http://csrc.nist.gov/publications/nistpubs/800-34/sp800-34.pdf
- Underlying Technical Models for Information Technology Security - URL: http://csrc.nist.gov/publications/nistpubs/800-33/sp800-33.pdf
- Intrusion Detection Systems - URL: http://csrc.nist.gov/publications/nistpubs/800-31/sp800-31.pdf

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

- Risk Management Guide for Information Technology Systems - URL: http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf
- Engineering Principles for Information Technology Security (A Baseline for Achieving Security), Revision A - URL: http://csrc.nist.gov/publications/nistpubs/800-27A/SP800-27-RevA.pdf
- Security Self-Assessment Guide for Information Technology Systems - URL: http://csrc.nist.gov/publications/nistpubs/800-26/sp800-26.pdf
- Guide for Developing Security Plans for Information Technology Systems - URL: http://csrc.nist.gov/publications/nistpubs/800-18/Planguide.doc
- Information Technology Security Training Requirements: A Role- and Performance-Based Model - URL: http://csrc.nist.gov/publications/nistpubs/800-16/800-16.pdf
- Information Technology Security Training Requirements: Appendix A – D - URL: http://csrc.nist.gov/publications/nistpubs/800-16/AppendixA-D.pdf
- Information Technology Security Training Requirements: Appendix E - URL: http://csrc.nist.gov/publications/nistpubs/800-16/Appendix_E.pdf
- Generally Accepted Principles and Practices for Securing Information Technology Systems - URL: http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf
- An Introduction to Computer Security: The NIST Handbook: URL: http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf

[xx] Center for Internet Security (CIS)
URL: http://www.cisecurity.com/ (see xvii – SANS links)

[xxi] Department of Energy (US DOE)
U.S. Department of Energy Cyber Security Action Plan III - URL: http://cio.doe.gov/Documents/cyber.actionplan.pdf

[xxii] General Accounting Office (US GAO)

- Assessing the Reliability of Computer-Processed Data - URL: http://www.gao.gov/cgi-bin/getrpt?rptno=gao-03-273g
- Investigator's Guide to Sources of Information - URL: http://www.gao.gov/special.pubs/soi/os97002.pdf
- Electronic Law Enforcement – Introduction to Investigations in an Electronic Environment - URL: http://www.gao.gov/special.pubs/d01121g.pdf
- Executive Guide – Information Security Management - URL: http://www.gao.gov/special.pubs/ai9868.pdf
- Executive Guide – Measuring Performance and Measuring Results of Information Technology Investments - URL: http://www.gao.gov/special.pubs/ai98089.pdf
- Federal Information System Controls Audit Manual - URL: http://www.gao.gov/special.pubs/ai12.19.6.pdf
- Information Security Risk Assessment – Practices of Leading Organizations - URL: http://www.gao.gov/special.pubs/ai00033.pdf
- Information Technology: An Audit Guide for Assessing Acquisition Risks - URL: http://www.gao.gov/special.pubs/im814.pdf

[xxiii] Health Insurance Portability and Accountability Act (HIPAA)

- 45 CFR Parts 160, 162 and 164: Health Insurance Reform: Security Standards; Final Rule - URL: http://aspe.os.dhhs.gov/admnsimp/FINAL/FR03-8334.pdf
- 45 CFR Parts 160 - 164: Health Insurance Reform: Privacy Standards- URL: URL: http://www.hhs.gov/ocr/regtext.html

[xxiv] California Senate Bill 1386 – February 12, 2002

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

URL: http://info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html

[xxv] Trusted Computer Security Evaluation Criteria (TCSEC)
URL: http://csrc.ncsl.nist.gov/secpubs/rainbow/std001.txt

[xxvi] Common Criteria
URL: http://csrc.nist.gov/cc/Documents/CC%20v2.1%20-%20HTML/CCCOVER.HTM

[xxvii] 21 CFR Part 11
URL: http://www.fda.gov/OHRMS/DOCKETS/98fr/03-4312.pdf

[xxviii] RSA SecurID
URL: http://www.rsasecurity.com/node.asp?id=1156

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.