Global Information Assurance Certification Paper

NERC Security Assessment for GIAC Enterprises – GCSC Practical Assignment

Abstract

For the GCSC practical assignment I chose to perform a NERC Security Assessment for GIAC Enterprises. My company, GTJD Consulting, went through the proposal process, the project planning and activity process, and the development and presentation of the final deliverable.

NERC (North American Electric Reliability Council) is responsible for the reliability and security of the electricity sector of North America. They have produced a set of guidelines and a set of standards for electricity sector participants, such as GIAC Enterprises, to abide by. GIAC Enterprises is a generation and transmission facility that has many power plants that powered by water, fossil fuels, and nuclear energy.

The assignment was completed in four parts. The first part being an overview of both companies involved, GTJD Consulting and GIAC Enterprises. It includes the details important to developing the sales and implementation approach to successfully win the bid and complete the project.

The second part details the proposal made to GIAC Enterprises in hope to win the project over other competitors. It includes the proposal as submitted to GIAC Enterprises detailing the methodology to be used, when the project is necessary, what qualifications GTJD Consulting has that would be in the best interest of GIAC Enterprises, and the cost and billing details. This part also includes how GTJD Consulting could sell this project to GIAC Enterprises. It discusses items that GTJD Consulting can use as leverage to win the bid over the other competitors.

The third part covers the project performance measures used to control the project. The project plan is created using the Project Management Body of Knowledge and details every step and process included in the project. It includes schedule, resources, tasks, milestones, budget and project control details that are necessary for project completion. Also included in this section is a sample of interview questions to be asked during a meeting, some of the pitfalls of the project including ways to handle them, and what can be done to add value to the project for GIAC Enterprises without increasing costs.

The final part details the project deliverable for GIAC Enterprises. It details the findings and recommendations, as well as, provides the plan that GIAC Enterprises is seeking to implement so they can comply with NERC regulations. A powerpoint presentation for the final presentation is explained and attached.

NERC Security Assessment For GIAC Enterprises

GIAC Certified Security Consultant (GCSC)
Practical Assignment
Version 1.0 (April 19, 2004)

Submitted by: Jim McMillan
September 17, 2004

Part 1: Methodology and Process

Summary of Businesses Involved

GetTheJobDone Consulting (GTJD Consulting)
GTJD Consulting is a national information security consulting firm. GTJD Consulting offers consulting services (managerial, audit, technical) for general and regulatory information security needs to private and government entities. GTJD Consulting has experience in many industries. Law enforcement, healthcare, energy, financial and federal government are some of the industries where GTJD Consulting has provided services. GTJD Consulting was founded in 1997 by a group of independent information security consultants and currently has an employee base of 23 employees. The senior management staff has a combined 60 years of experience in the information security field, 32 years experience in the consulting field. They each hold Certified Information System Security Professional (CISSP), GIAC Security Essentials Certification (GSEC) certifications as well as advanced college degrees in management and business. Other employees at GTJD Consulting have a minimum of three years experience and technical GIAC certifications in their area of expertise (Windows, Unix, Audit, Intrusion Detection, Firewall, Secure Coding, ISO17799, ISM, etc.).

GIAC Enterprises
GIAC Enterprises is an investor owned electric company that provides generation and transmission services to its customers. GIAC Enterprises has a customer base of approximately 2.4 million people. GIAC Enterprises has an employee base of approximately 7500 people at 30 locations. Generation capacity consists mostly of hydroelectric dams followed by some fossil fuel generating plants and two nuclear generation plants. GIAC Enterprises has an immediate interest to create a plan to facilitate the implementation of the North American Electric Reliability Council's (NERC) Security Guidelines for the Electricity Sector (NERC SGES) and be able to fully comply with the NERC Urgent Action Standard 1200 - Cyber Security (NERC 1200) and 1300 - Permanent (NERC 1300) once the plan has been implemented. NERC 1300 is still in the process of being drafted but is expected to be nearly identical to NERC 1200. GIAC Enterprises has approached GTJD Consulting for help in creating such a plan that will meet their needs as well as develop a solid information security program.

Methodology and process used for this opportunity

On April 1, 2004, GIAC Enterprises approached GTJD Consulting with an RFP for a NERC Security Assessment. Shortly after receiving the RFP, GTJD Consulting contacted GIAC Enterprises to set up an initial meeting to discuss the RFP to assure a complete understanding of GIAC Enterprises' needs.

During the initial meeting with GIAC Enterprises on this project, GTJD Consulting discovered several valuable pieces of information to leverage the sell of this project and ultimately complete this project for GIAC Enterprises. One important factor is knowledge of the energy industry. With GTJD Consulting's past proven performance and references in the energy industry there should be no doubt that we have the experience and knowledge they require.

Another key factor is GIAC Enterprises structured project management philosophy. GTJD Consulting follows a very similar structured project management style on projects as well. This should be very appealing to GIAC Enterprises.

During this initial meeting the approach to be used during this project was discussed fully. The approach would consist of an in-depth project management process, interviews of the stakeholders at all levels of the organizational tree, sites tours of each facility, additional study of any applicable regulatory standards and guidelines and study of current business processes and implemented security measures. Once all applicable information is collected it will be compiled for comparison with regulatory guidelines and standards, as well as information security best practices. All of this information will be reiterated in a response to the RFP issued by GIAC Enterprises.

Part 2: Proposal and Pitch

Proposal for GIAC Enterprises

In response to the RFP that was issued by GIAC Enterprises for a NERC Security Assessment, GTJD Consulting responded with this letter and attached proposal to the CEO of GIAC Enterprises.

* Proposal cover letter *

May 5, 2004

Joe Boss, CEO
GIAC Enterprises
1500 Kilowatt Way
SomeTown, SomeState 12345-1234
(555)555-2468

Dear Mr. Boss:

It was a pleasure to meet with you and your staff on April 20th to discuss the RFP you presented to our company. We are excited and happy that you would choose us as a possible candidate to work with you to comply with energy industry regulations. In response to your RFP for a NERC Security Assessment, we submit to you the attached proposal.

As you read through the proposal, you will notice we are well equipped with resources to meet your needs. We have many experiences with the energy industry in consulting engagements, as well as some experience with the NERC standards and guidelines. In addition, we have a broad range of knowledge and experience with information security processes and regulatory compliance.

We are anxious to be able to offer our assistance and work with your company as a team. We pride ourselves in helping our clients succeed because a success for you is a success for us!

Sincerely,
{Signed}
Biz Owner, CEO
GTJD Consulting
BizOwner@GTJDConsulting.com
(555)555-1234
(800)555-4321

* Start of proposal *

{GTJD Consulting header logo}

PROPOSAL

NERC Security Assessment

Prepared for: Joe Boss
CEO
GIAC Enterprises

Prepared by: John Doe
VP of Consulting Services
GTJD Consulting

Date Created: May 5, 2004

{GTJD Consulting footer address logo}

Table of Contents

Executive Summary

In response to your RFP for a NERC Security Assessment dated April 1, 2004, we submit this proposal.

GTJD Consulting proposes to build a plan of action for you to comply with upcoming regulations from the North American Electric Reliability Council (NERC). These standards and guidelines are from two documents, which are the NERC Security Guidelines for the Electricity Sector (NERC SGES) and the NERC Urgent Action Standard 1200 - Cyber Security (NERC 1200).

NERC 1200 is a temporary standard to be replaced by the permanent NERC Standard 1300 – Cyber Security (NERC 1300). However, NERC 1300 is currently being drafted and NERC 1200 is valid until August 13, 2004 with the expectation of a one-year extension to be announced. There has been much speculation that NERC 1300 will be very similar to NERC 1200 with the addition of a larger area of critical asset coverage for compliance. One of the additional assets we expect to be included is the plant control process. We are making this an assumption for this assessment.

We will create a plan of action by performing an in-depth analysis of GIAC Enterprises' Business needs and current information security posture in comparison to the requirements and recommendations of the NERC standards and guidelines. Upon completion of the project, GTJD Consulting will provide GIAC Enterprises with a formal plan of action to comply with the NERC standards and guidelines. This plan will provide steps and recommendations to assist GIAC Enterprises in the creation of an information security program that will bring them into compliance with NERC standards and guidelines. The scope of this engagement will only consist of the plan creation as requested in your RFP and does not include the actual implementation of the plan.

As with other industry's regulations, we understand your need for compliance with these regulations. Since the tragic events of Sept. 11, 2001, the industries that make up the critical infrastructure realize they have a very new threat and protecting their resources is a must.

In the energy industry some of the most critical systems to protect are the reliability authority, interchange authority, balancing authority, transmissions, generation, and our assumption of the plant control systems. All of these processes are critical to the reliability of the electricity sector. In our case of plant control systems, even under normal operation, one can cause serious damage if not properly operated. Thus, it is important to secure these systems so only trained and authorized operators can access them.

According to the document "Common Vulnerabilities in Critical Infrastructure Control Systems" by the Sandia Corporation for the US Depart of Energy's National Nuclear Security Administration, there is great need to secure process control systems (PCS) and supervisory control and data acquisition (SCADA) systems. Sandia reports, "Each

utility should address their PCS as a hypercritical system by using very tight security safeguards. The PCS has enormous value by reducing costs and improving performance through automation, and this value must be reflected in the system's security."[1] And according to the Department of Energy, in their document "21 Steps to Improve Cyber Security of SCADA Networks", "SCADA networks were initially designed to maximize functionality, with little attention paid to security. As a result, performance, reliability, flexibility and safety of distributed control/SCADA systems are robust, while the security of these systems is often weak."[2]

Over the course of time, these systems have grown into corporate networks for the ease of use and remote control functionality networks have given us. The systems are not designed with security in mind for this type of environment. Thus, companies are securing them through obscurity. However, with today's malicious viruses and programs, obscurity is not a security measure we should rely upon. We need to be applying more effective and proven security measures to protect these critical systems. In our plan we will give recommendations to provide these measures.

We anticipate the entire process to build a plan of action will take approximately six to seven weeks. This will fit well into your desired completion date. We will provide three dedicated analysts to work on the project. The total cost of the completed project will be $40,000 plus reasonable expenses. The project will be managed through an in-depth project management methodology. This will reduce the risk of failure, increase the probability of success, and provide a process to manage change.

We feel, with our knowledge and experience with clients from the energy industry, we will be able to provide the quality and level of service you expect to successfully meet your needs. We have recently completed two consulting engagements for other energy industry companies. Through these engagements, we have gained a great deal of general knowledge of the energy industry business and feel we can adjust to the uniqueness of your business quickly.

In addition, we have had several engagements involving various other regulations such as Gramm-Leach-Bliley Act (GLB), Sarbanes-Oxley Act (SOX), and Health Insurance Portability and Accountability Act (HIPAA). This has given us a vast amount of experience in the compliance arena. Many of these regulations have similarities in compliance rules. With our understanding of the NERC standards and guidelines you need to comply with, we feel some of these compliance rules overlap and you can benefit from our experience in this area as well.

We are very excited about this opportunity to help you build a top-notch plan to meet your compliance needs. If you have any further questions about this proposal, please feel free to contact us.

---

[1] Sandia National Laboratories
[2] Department of Energy

Proposed Process and Implementation Plan

The project will be managed through a well-structured project management process. A GTJD Consulting employee with extensive project management background will be assigned as project manager, as well as act as an analyst on the project. The following project management phases will be used to manage this project:

- Initiating processes – scope management – defining purpose, scope, objectives, stakeholders, and authorizing the project.
- Planning processes – defining tasks, assigning resources, identifying risks, budgeting, scheduling, determining communications, quality control, and planning for change.
- Executing processes – managing resources to execute the plan.
- Controlling processes – monitoring the execution of the plan to assure that the plan is progressing according to schedule and identifying any changes or variances to the project.
- Closing processes – Acknowledging the completion of the project and acceptance of deliverables.

We expect this project will take 33 working days to complete. The work for this project will be completed in six high-level phases of work. With the ending of each phase representing a milestone for the project. The six phases that we have identified for the project are:

1. Project Kick-Off Meeting: Meeting to discuss the project processes from beginning to end. The project plan will be discussed in detail as well as the project management methodology. After this meeting everyone should have an understanding of what needs to be done to make the project a success. This phase will take one working day.

2. Review GIAC Enterprises' Business: This phase of the project focuses on providing GTJD Consulting with a good understanding of the business side of GIAC Enterprises. During this phase we will be making trips to various plant sites for tours and information gathering. This phase will take 12 working days.

3. Review GIAC Enterprises' Information Security Program: This phase of the project focuses on providing GTJD Consulting with a good understanding of GIAC Enterprises' Information Security Program. This phase will take two working days.

4. Review NERC information: This phase of the project focuses on a common and correct understanding between GIAC Enterprises and GTJD Consulting of the NERC standards and guidelines being used in the project. This phase will take two working days.

5. Analysis: This phase of the project focuses on compiling and analyzing the information while producing the final deliverable(s). This phase will take 15 working days.

6. Project closure: This phase of the project focuses on the final steps of the project: presentation of deliverable(s), assuring understanding of the information presented, and project sign off. This phase will take one working day.

At completion of the project, GIAC Enterprises will be presented with a Plan of Action that can be implemented to comply with the NERC standards and guidelines. In this plan of action, we will identify each section of the NERC SGES and NERC 1200 and identify our findings as well as general recommendations. Finally, we will detail a plan of action for GIAC Enterprises to follow for implementation of processes that will bring compliance with these NERC standards and guidelines.

During the project, GTJD Consulting will work with GIAC Enterprises to gather the information we need to complete the project. We will have dedicated personnel working on the project. You can expect these personnel to be professional, knowledgeable, and efficient at their responsibilities. Upon completion of the project you can expect a thorough and complete plan that will meet or exceed your expectations. In return, we expect GIAC Enterprises to provide strong support from management by allowing their employees to fully assist us during the project without interruption. In addition, as stated in the RFP, GIAC Enterprises will be providing reliable transportation for the travel expected during this project. Finally, GIAC Enterprises will be providing on hand documentation of current business goals and processes.

We propose the project team consist of three GTJD Consulting employees and four GIAC Enterprises employees. The team members from GIAC Consulting will consist of the VP of Consulting to act as the project manager and lead analyst, a senior security analyst, and another security analyst. After reviewing GIAC Enterprises' organization chart, the team members should consist of two information security administrators, an internal auditor responsible for past information security audits, and a business analyst responsible for records management and human resources. One of the GIAC Enterprises team members should be appointed as the lead member to help coordinate schedules and resolve problems for GIAC Enterprises.

This project team will do the majority of the legwork and information gathering. GTJD Consulting will compile and analyze the information and produce the deliverables. Other employees from GIAC Enterprises will be involved in the project, specifically plant control managers. These employees will be providing information to the project team at various intervals throughout the project.

Qualifications

GTJD Consulting has provided information security services to many companies since 1997. Over the years we have grown considerably and recruited a top-notch staff. We have performed various projects for other companies in the energy industry and can arrange reference calls, if necessary. Recently we have completed a Network Security Assessment for Makmor Power Inc. Prior to that engagement, we completed penetration tests for Gen-Tran Electric Company. Some of the analysts who worked on these projects will also be working on your project.

John Doe, VP of Consulting Services, worked on both projects as the project manager and lead analyst. He will be assigned as project manager of your project. John has an extensive education in management, project management, and information security. In 1989, he graduated from the University of Hifees with a Masters Degree in Management. John is a Certified Information System Security Professional (CISSP). He has GIAC Security Essentials Certification (GSEC), GIAC Systems and Network Auditor (GSNA) certification and holds the Project Management Professional (PMP) certification. John has been with GTJD Consulting since 1998. John has worked on several projects and has extensive knowledge of the energy industry. He leads GTJD Consulting's team of analysts that is responsible for any projects in the energy sector.

Fred Smith, Senior Security Analyst, worked with John on both of our prior consulting engagements for electric companies. Fred graduated from the University of Techknowledgy in 1998 with a Bachelors Degree in Computer Science. Fred has obtained the GIAC Security Essentials Certification (GSEC), GIAC Certified ISO-17799 Specialist (G7799), and GIAC Certified Incident Handler (GCIH) certifications. Similar to John, Fred has a high level of knowledge in the energy sector, including experience with NERC guidelines.

Laura Knight, Security Analyst, is fairly new to the energy team at GTJD Consulting. She was transferred from another team prior to our last engagement with Makmor Power Inc. Laura graduated from the University of Hifees in 1994 with a Bachelors Degree in Computer Science and Mathematics. She currently holds the GIAC Certified Intrusion Analyst (GCIA) and the GIAC Certified Firewall Analyst (GCFW) certifications. She is currently pursuing the GIAC Certified UNIX Security Administrator (GCUX) certification. Laura has a little knowledge of the energy sector, but an extensive amount of knowledge of building and managing security solutions for complex networks. She has previous experience with the GLB and SOX regulations. With Laura's education and experience, we believe she makes an excellent fit with this team.

Cost Analysis

For the six to seven weeks that the project will cover, the cost for us to complete the project will be $40,000 plus reasonable expenses. In the project plan cost estimating and budgeting section, the GTJD Consulting resources will be based on typical billable hourly wages. This will show costs above and beyond the amount you will be charged. You will be able to see a significant savings over the hourly rates. GIAC Enterprises will only pay this fixed price.

However, it must be noted that projects are based on three measures: Cost, time, and quality. If one of these measures must change, a different measure must change to compensate. For example: If the time line for a project needs to be shortened, the cost of the project must go up for added resources to complete the project or the quality of the product must be reduced to allow for a faster work pace. The project was designed to fit your timeline and quality requests. If one of the project measures needs to change for your project, then you must realize another measure will need to be changed. If this happens the price may vary, but not without proper notification and approval.

For expense figures we use the following as typical estimating guidelines. There will be $15 planned for each meal and $60 planned for each night of hotel lodging. These figures will be figured per person. Meals and lodging will only be charged during the travel time for plant site visits. There will be no transportation costs billed because GIAC Enterprises will be covering the transportation expenses for travel to the plant sites. All of these expenses will be budgeted for and forecasted in the project plan.

Our typical billing schedule will be followed unless other arrangements are made. We will bill 30 percent at the start of the project with the remainder due upon completion. The billed amount will be due in 15 days and will have a late charge in the amount of two percent of the unpaid balance compounded monthly.

GTJD Consulting will assign a customer relationship manager to this project to handle all billing details, as well as other relationship issues. Her name is May Q. Hape and can be reached at our main office. All questions and concerns will be handled through her.

* End of proposal *

Pitch

In order to sell this proposal to GIAC Enterprises, GTJD Consulting would leverage their experience and knowledge to gain preference over other competitors. GTJD Consulting would highlight their experience and knowledge in four areas that GIAC Enterprises could see as being beneficial. These four areas are the energy industry's business, project management methodology, the information security profession in general and regulatory compliance.

GIAC Enterprises has indicated time and quality are the two most important factors for this project. GTJD Consulting can show how their project management style has met deadlines in previous projects via references. In addition, highlighting the qualifications of the consultants assigned to this project shows GTJD Consulting is ready to commit a wealth of experience and knowledge to the project to complete it on time and meet or exceed expectations. The consultants assigned to the project will have a high level of education and experience in information security, as well as a background with similar industry companies to support a claim as being the superior choice.

GTJD Consulting would also leverage their price as being very competitive, based on the size and scope of the project. They have the ability to come in at a competitive price because of their experience and knowledge as leverage in keeping the cost down. This allows GIAC Enterprises to receive a wealth of information at a minimum cost.

Part 3: Project Performance

Project Plan

"Project Management is the application of knowledge, skill, tools and techniques to project activities to meet project requirements."[3] Good project management will add value to a project by reducing the risk of project failure and increase project success by providing a way to react to and manage change. The Project Management Institute (http://www.pmi.org) has a guide for project management that was created based on the collective ideas of many professionals as to what is considered project management best practices. "The Project Management Body of Knowledge (PMBOK) is an inclusive term that describes the sum of knowledge within the profession of project management."[4] This guide helps you build a project plan with the generally excepted practices of project management. It keys on the following five processes for successful project management:

- Initiating processes – scope management – defining purpose, scope, objectives, stakeholders, and authorizing the project.
- Planning processes – defining tasks, assigning resources, identifying risks, budgeting, scheduling, determining communications, quality control, and planning for change.
- Executing processes – managing resources to execute the plan.
- Controlling processes – monitoring the execution of the plan to assure that the plan is progressing according to schedule and identifying and changes or variances to the project.
- Closing processes – Acknowledging the completion of the project and acceptance of the deliverable(s).

This is the methodology used to initiate, plan, execute, control and close this project. In the following project plan you will find all information about this project including: purpose, scope, objectives, stakeholders, resources (people and equipment), tasks, schedules, budget, communications, quality monitoring and change controls.

---

[3] Project Management Institute, Pg. 20
[4] Project Management Institute, Pg. 17

* Start of project plan *

NERC Security Assessment for GIAC Enterprises Project Plan

For

{GIAC Enterprises Logo - Large}

GIAC Enterprises

Prepared by

{GTJD Consulting Logo – Small }

GTJD Consulting
June 2004

Table of Contents

PURPOSE STATEMENT

The purpose of this project is to analyze the current information security program of GIAC Enterprises and create a plan from the findings to comply with the security guidelines and urgent action standards issued by the North American Electric Reliability Council (NERC). This project will begin on July 8, 2004 with a completion date of August 23, 2004.

JUSTIFICATION STATEMENT

GIAC Enterprises, an independently owned electric company that provides generation and transmission services, has to comply with regulatory standards created by NERC in the form of NERC 1200 Urgent Action Cyber Security Standard (NERC 1200) and the upcoming NERC 1300 Permanent Cyber Security Standard (NERC 1300). In addition NERC has created the NERC Security Guidelines for the Electricity Sector (NERC SGES) to provide guidance in the general approaches, considerations, practices and planning philosophies to be applied in protecting the electrical infrastructure systems.

A committee was formed and under the direction of the CEO conducted an internal audit of these standards and guidelines. Upon completion of the audit, the committee recommended a study should be conducted on GIAC Enterprises current information security program against what will be required by NERC. In addition, the committee recommended a formal plan of action to be developed to bring GIAC Enterprises' information security program into compliance with the NERC standards and guidelines.

OBJECTIVES

The following objectives have been defined for this project:

- Analyze and understand GIAC Enterprises' business approach and functions.
- Analyze and understand GIAC Enterprises' current information security program.
- Analyze and understand the NERC security standards and guidelines.
- Compare and contrast GIAC Enterprises' information security program to what is recommended/required by NERC.
- Develop a plan of action and make recommendations to GIAC Enterprises for compliance to the NERC standards and guidelines.
- Assure GIAC Enterprises fully understands the content of the deliverables as they are turned over upon project closure.

STAKEHOLDERS

The following are identified as the key stakeholders for this project:

- Customer(s):
  Employees of GIAC Enterprises

- Sponsor(s):
  Joe Boss, CEO, GIAC Enterprises
  GIAC Enterprises' Board of Directors
  Biz Owner, CEO, GTJD Consulting

- Performing Entity:
  GTJD Consulting
  GIAC Enterprises

- Project Team:
  Cindy Mason, Information Security Admin, GIAC Enterprises
  Tom Young, Information Security Admin, GIAC Enterprises
  Max Olson, Senior Business Analyst, GIAC Enterprises
  Lee Jordan, Internal Auditor, GIAC Enterprises
  Fred Smith, Senior Security Analyst, GTJD Consulting
  Laura Knight, Security Analyst, GTJD Consulting

- Project Manager:
  John Doe, VP of Consulting Services, GTJD Consulting

- Other Stakeholders:
  Customers of GIAC Enterprises

SCOPE STATEMENT

The scope of this project will consist of an in-depth analysis of GIAC Enterprises information security program in comparison to the recommendations and requirements of the NERC standards and guidelines. The NERC standards and guidelines to be used are the NERC SGES and NERC 1200. Upon completion of the project, GTJD Consulting will provide GIAC Enterprises with a formal plan of action to comply with the NERC standards and guidelines. This plan will provide steps and recommendations to assist GIAC Enterprises in the creation of an information security program that will bring them in compliance with NERC standards and guidelines. The scope of this project does not include the actual implementation of the plan.

For this project to be completed the following activities and tasks must be accomplished:

- GTJD Consulting must gain a thorough understanding of GIAC Enterprises' business. GTJD Consulting and GIAC Enterprises must work together to assure a detailed and proper understanding of GIAC Enterprises' business organization, culture, goals and processes.

- GTJD Consulting must gain a thorough understanding of GIAC Enterprises' current information security program. GTJD Consulting and GIAC Enterprises must work together to assure a detailed and proper understanding of the current information security program at GIAC Enterprises.

- GTJD Consulting and GIAC Enterprises must have the same thorough understanding of NERC standards and guidelines.

- GTJD Consulting must compare and contrast the differences of GIAC Enterprises' current information security program to the requirements and recommendations of NERC.

- GTJD Consulting must compile findings and formulate a plan of action with recommendations to GIAC Enterprises on the steps needed to comply with NERC standards and guidelines.

- GIAC Enterprises must gain thorough knowledge of this plan from GTJD Consulting.

- GIAC Enterprises and GTJD Consulting must bring closure to this project.

CHANGE CONTROL PROCESS

No matter how much planning goes into a project, there always seems to be some change after the project gets started. Without change control a project scope can grow to a point where the project is completely different than originally intended. With good planning the project scope should be defined well enough so the chance for change is minimal. However, since change is always possible, this section defines the change process and the requirements on how changes are to be handled for this project.

All change requests will be submitted to the Project Manager by electronic mail (e-mail) or in written format where electronic means is inappropriate or not available. The change request must have the sponsor's approval when submitted to the Project Manager. Change requests must contain the following information, at minimum, upon submission to the Project Manager (See APPENDIX for form format):

Request for Change

- Date:
- Requested by:
- Requested change:
- Reason for change:
- Pros and Cons of the change:
- Estimated costs of the change:
- Assumptions:
- Impact if change not implemented:
- Alternatives:
- Sponsor approval for submission to Project Manager:

Upon receiving an approved and signed change request, the Project Manager will review the request for accuracy. If the request is accurate, an appropriate contract and/or project plan amendment will be generated and presented to the sponsor. When the sponsor approves the contract and project plan amendment, the change will be implemented. All amendments to the project plan will be added as they are approved.

Occasionally there will be some small changes that will not impact the project in a manner where time, cost, or quality will change. The Project Manager can make these non-impact changes without sponsor approval. However, the Project Manager will notify the sponsor of these changes. An example of this type of change is: a schedule manipulation of personnel interviews due to an illness, which does not effect a milestone date.

Decisions made for each change requests must be documented and filed with the change request. This document must contain in detail what was decided, what affects it had on the project, how the change was incorporated, and indicate all of the necessary approvals.

Overall Change Control

Overall change control will cover any change to the project plan, ensure that changes are beneficial to the project, and manage those changes. The project manager and project sponsor must evaluate and approve any change to the project plan.

Scope Change Control

Scope change control will determine that a scope change has occurred, assess the influencing factors that create change to the scope to ensure that the changes are beneficial to the project, and manage those changes. The project manager and project sponsor must evaluate and approve any change to the project scope.

Schedule Change Control

Schedule change control will determine that a schedule change has occurred, assess the influencing factors that create change to the schedule to ensure that the changes are beneficial to the project, and manage those changes. The project manager and project sponsor must evaluate and approve any change to the project schedule.

Cost Change Control

Cost change control will define the influencing factors that create changes to the cost baseline to ensure that changes are beneficial, determine that the cost baseline has changed, and manage the changes as they occur. The project manager and project sponsor must evaluate and approve any changes to the cost of the project.

GTJD Consulting's overages, excluding travel cost, to the project shall not exceed ten percent of their original estimate. If the ten percent limit is exceeded GTJD Consulting will complete the project at no additional cost to GIAC Enterprises. Since the information security program review schedule was shortened to save cost, due to the claim of detailed documentation of the program on GIAC Enterprises part, this limitation does not apply to cost overruns for that task as well.

COST MANAGEMENT

To ensure that costs are completed within the allocated budget it is necessary to have a cost management plan for the project. In this section we will look at resource planning, cost estimating and cost budgeting.

Resource Planning

Resource planning involves determining what physical resources (people, equipment and materials) should be used to perform project activities. The following table shows resources to be used on the project and estimated time they will spend on the project.

Resource	Organization	Project Hours
Cindy Mason	GIAC Enterprises	156
Tom Young	GIAC Enterprises	156
Max Olson	GIAC Enterprises	156
Lee Jordan	GIAC Enterprises	156
Joe Boss	GIAC Enterprises	32
Board of Directors	GIAC Enterprises	32
Mark Hightower	GIAC Enterprises	4
Jim Bauer	GIAC Enterprises	4
Tim Selph	GIAC Enterprises	4
Joe Thomas	GIAC Enterprises	4
Lance Huff	GIAC Enterprises	4
Shelly Bach	GIAC Enterprises	4
Larry Phelps	GIAC Enterprises	4
Fred Smith	GTJD Consulting	264
Laura Knight	GTJD Consulting	264
John Doe	GTJD Consulting	200
Passenger Van	GIAC Enterprises	NA
Computers	GIAC Enterprises GTJD Consulting	NA
Conference Rooms	GIAC Enterprises	NA
Projector	GIAC Enterprises	NA

Cost Estimating

Cost estimating involves developing an approximation of the costs of the resources needed to complete project activities. The following table shows estimated cost for each resource being used. This table is also used to track actual costs to easily show any variances.

Resource	Est. Unit(s)	Est. Unit Cost	Est. Total	Actual Unit(s)	Actual Unit Cost	Actual Total	Variance
Cindy Mason	156hrs	$28	$4,368				
Tom Young	156hrs	$28	$4,368				
Max Olson	156hrs	$28	$4,368				
Lee Jordan	156hrs	$28	$4,368				
Joe Boss	32hrs	$50	$1600				
Board of Directors	32hrs each X 7	$350	$11,200				
Mark Hightower	4hrs	$28	$112				
Jim Bauer	4hrs	$28	$112				
Tim Selph	4hrs	$28	$112				
Joe Thomas	4hrs	$28	$112				
Lance Huff	4hrs	$28	$112				
Shelly Bach	4hrs	$28	$112				
Larry Phelps	4hrs	$28	$112				
Fred Smith	264hrs	$100	$26,400				
Laura Knight	264hrs	$80	$21,120				
John Doe	200hrs	$125	$25,000				
Travel	1600 miles	$.35	$560				
Lodging	42 nights	$60	$2,520				
Meals	126 meals	$15	$1,890				

Cost Budgeting

Cost budgeting involves allocating the overall cost estimates to individual work items in order to establish a cost baseline for measuring project performance. The following table shows estimated cost for each activity of the project based on all of the resources to be involved. In addition, this table is used to track actual costs to easily show any variances.

Activity	Est. Time Period	Est. Cost	Actual Time Period	Actual Cost	Time Variance	Cost Variance
Project Kick-Off Meeting	7/8	$6,536				
Review GIAC Enterprises' Business	7/9 – 7/26	$44,186				
Review GIAC Enterprises' Information Security Program	7/27 – 7/28	$6,672				
Review NERC information	7/29 – 7/30	$6,672				
Analysis	8/2 – 8/20	$37,944				
Project closure	8/23	$6,536				

QUALITY MANAGEMENT

Project quality management includes the processes required to ensure that the project will satisfy the needs for which it was undertaken. The project team, having representatives from both sides will be responsible for quality management of this project.

Quality Planning

Quality planning identifies which quality standards are relevant to the project and determining how to satisfy them. The project team will monitor quality of the project by testing the project progress against the project plan for scope compliance, time line compliance and cost compliance. In addition, the team will monitor work on the project for professionalism and content.

Quality Assurance

Quality Assurance evaluates the overall project performance and the product on a regular basis to provide confidence the project and the product will satisfy the relevant quality standards. The project will be evaluated on a weekly basis to assure time lines and costs are meeting or exceeding project expectations. In addition, the project work will be reviewed to assure the content is meeting or exceeding expectations.

Quality Control

Quality Control will monitor specific project and deliverable results to determine if they comply with relevant quality standards and identify ways to eliminate causes of unsatisfactory performance. The project manager and project team will be responsible for identifying, implementing, and documenting the appropriate corrective actions when cases of unsatisfactory performance arise.

The project manager will monitor the project. The project will be measured against the time lines and results of the work done. Any and all quality issues should be reported as soon as possible to the project manager for investigation.

HUMAN RESOURCE MANAGEMENT

Human resource management includes the processes required to make the most effective use of the people involved with the project. It includes all of the project stakeholders, as defined in the STAKEHOLDER section of this project plan.

Organization Planning

Organizational planning involves identifying, documenting and assigning project roles, responsibilities, and reporting relationships.

The Customer(s), employees of GIAC Enterprises will have a few selected participants that report to the Project Manager. Their roles and responsibilities are as follows:

- Provide tours of facilities.
- Provide information on business operations.
- Respond to questions of project team.

The Sponsor(s), Joe Boss, GIAC Enterprises' Board of Directors and Biz Owner roles and responsibilities are as follows:

- Authorize project execution.
- Authorize changes to project.
- Provide information as requested.
- Attend meetings as requested.
- Provide feedback.
- Authorize completion of project.
- Assure resources are available.

The Performing Entity, GTJD Consulting and GIAC Enterprises, take on the following roles and responsibilities:

- Initiate and close the project.
- Assist in project definition.
- Assure appropriate resources are available.
- Assure deliverables are complete and professional.
- Resolve issues in quick and timely manner.

The Project Team will report to the Project Manager. Their roles and responsibilities are as follows:

- Assist in project definition.
- Perform activities and tasks defined for project to produce defined deliverables.
- Monitor quality.
- Promote teamwork.
- Provide status updates.

The Project Manager will report to the CEO of GTJD Consulting. His roles and responsibilities are as follows:

- Manage the project and the project team.
- Work with project team as defined in the schedule.
- Monitor quality.
- Manage change requests.
- Assure communications are effective and efficient.
- Report required information to the sponsors.

Other Stakeholders, customers of GIAC Enterprises, have no roles or responsibilities for this project but they have a vested interest in the reliability of the electricity they use in their daily lives.

Staff Acquisition

Staff acquisition involves getting the human resources needed assigned to and working on the project. Since all human resources required are already on staff at GTJD Consulting or GIAC Enterprises, no staff acquisition will be required for this project. Any replacement staff, if necessary, will be acquired according to the corrective actions outlined under this risk in the Risk Management section.

Team Development

Team development involves developing individual and group skills to enhance project performance. Team members are encouraged to work together as often as possible and have regular team meetings (including lunch meetings). The teams are encouraged to provide feedback amongst one another, as well as coach one another when appropriate for skill transfer. For the duration of the project, all team members will be co-located together at GIAC Enterprises' headquarter building.

COMMUNICATION MANAGEMENT

Communication throughout the project is very important to the success of the project. For communication to be efficient and effective there must be plan in place to communicate during the project. This plan will allow all individuals involved in the project to know what needs to be communicated to whom at what time. Official project communications will occur at weekly status meetings or via electronic mail (e-mail). All communications and other documentation will be stored on a web server at GTJD Consulting's headquarters. Information will be updated regularly via the webmaster for GTJD Consulting. Secure access will be provided to all authorized individuals. The website will be structured as follows:

Home Page (https://clients.gtjdconsulting.com/giacenterprises/in.htm)
- Project Plan
- Schedule
- Accomplishments
- Change Requests
- Communications
- Meeting Notes
- Collected information
- Deliverables
- Forms

Weekly status meetings will be held for the project team and will follow the following agenda:

- Meeting opening – note taker assigned and attendees recorded.
- Review previous week's project update.
  - Report on action items assigned during previous meeting
- Team member status report.
- Discussion of work done – including quality assurance.
- Discussion of upcoming schedule and activities.
- Report and discussion on any new items – change requests and new risks.
- Assign action items of things to do in addition to the scheduled activities.
- Meeting Closure

The following information distribution schedule will be used for the duration of this project:

Information	Recipient(s)	Schedule	Method	Distributed by
Performance Reports	Project Manager	Fridays by 3:00pm	e-mail	Team Members
Project Updates	Stakeholders	Mondays by 9:00am	e-mail	Project Manager
Meeting Minutes	Meeting Attendees	Within 24 hours	e-mail	Designated facilitator
Change Requests	Project Manager	As necessary	e-mail	Requestor
Contract/Project Amendments	Stakeholders	As necessary	e-mail	Project Manager

RISK MANAGEMENT

With any project, there is always some amount of risk something will occur that will affect the project. With appropriate risk management, you can plan for certain risks and have a corrective action planned when the risk occurs. By having planned for the risk, you can minimize the risks impact on the project. When planning for risks, we typically identify the risk, probability it will occur, impact it will have, corrective action to take and who is responsible for that particular risk. With project risks, there are two types of risk events. One type is a negative risk event, which can adversely affect the project. Another type is a positive risk event, which can be used to maximize the project outcome if planned for appropriately. In the following risk identification table, you will see the risks that are identified for this project.

Risk	Prob.	Impact	Corrective Action	Individual Responsible
Negative Risk Events				
NERC Changes guidelines	Low	High	Review plan and make necessary changes if Sponsor wants to proceed	Sponsor
Loss of resource	Low	High	Continue with current resources extending project completion date; replace resource and modify completion date for lost time; replace resource and add additional resources to make up for lost time	Sponsor, Project Manager
Schedule delays	Med	Med	Work on other activities to minimize impact; try to make time up in other areas	Project Manager
Need equipment or materials	Low	Med	Go through normal procurement channels with high or emergency priority request	Project Manager
Positive Risk Events				
Tasks complete early	Low	High	Move resources to next task; allow extra time for future negative risk; finish early and provide savings	Project Manager

PROCUREMENT MANAGEMENT

This section is not needed for this project. Since the resources for this project are all derived of human resources, there is no need to procure any products to accomplish the project. If any material or equipment needs are identified, the corrective action in the Risk Management section will be followed.

ASSUMPTIONS

Throughout the planning process assumptions may have been made about the project. In this section we try to document some of the assumptions that were made while defining the scope of work, scheduling, and other aspects of the project.

- GIAC Enterprises employees will be available as scheduled in the project plan.
- GTJD Consulting employees will be available as scheduled in the project plan.
- Travel arrangements and travel to all locations will go without problem.
- GTJD Consulting's understanding of the energy industry will help in the understanding of GIAC Enterprises business.
- Both companies already have an in-depth and accurate understanding of the NERC standards and guidelines.
- Everyone involved in the project agrees with the project plan and importance of the project, thus they are willing to participate in a manner that will produce a successful project completion.
- The project has been communicated to all employees with an understanding of why the project is being accomplished.
- All necessary material and equipment is on hand.
- The documentation on GIAC Enterprises' Information Security Program provided is accurate and the information security program review can be completed as scheduled.
- As some speculate, NERC 1300 will expand the definition to include assets such as plant control processes.

DETAILED SCHEDULE

The following tasks are defined to help successfully complete the project objectives in a professional and efficient manner. The end of each task is considered a milestone for this project, thus indicating completion of a project objective. The goals, activities, resources, resource hours and timelines are identified for each task. Note that budgeting is covered in the Cost Management Section of this plan.

Task Name: Project Kick-Off Meeting

Goal: The goal of the kickoff meeting is to review the processes of the project. During this meeting we will be discussing how the project will flow from beginning to end. We will go over all of the details in this project plan. Everyone should come out of this meeting with a good idea of what they are expected to do to make this project successful.

Activities, Resources and Timeline:

Task	Activity	Resource	Hours	Duration	Start Date	End Date
Project Kick Off Meeting			72h	1d	Thu 7/8/04	Thu 7/8/04
	Meeting	Board Room			Thu 7/8/04	Thu 7/8/04
		Cindy Mason	8h		Thu 7/8/04	Thu 7/8/04
		Tom Young	8h		Thu 7/8/04	Thu 7/8/04
		Max Olson	8h		Thu 7/8/04	Thu 7/8/04
		Lee Jordan	8h		Thu 7/8/04	Thu 7/8/04
		Joe Boss	8h		Thu 7/8/04	Thu 7/8/04
		Board of Directors	8h		Thu 7/8/04	Thu 7/8/04
		Fred Smith	8h		Thu 7/8/04	Thu 7/8/04
		Laura Knight	8h		Thu 7/8/04	Thu 7/8/04
		John Doe	8h		Thu 7/8/04	Thu 7/8/04

Task Name: Review GIAC Enterprises Business

Goal: The goal of the business review is to give GTJD Consulting a thorough understanding of GIAC Enterprises' business. Even though GTJD Consulting has knowledge of the energy industry as a business, GIAC Enterprises may have unique ways they do business, as well as their own corporate culture. These unique details may have impact on recommendations and how processes are implemented.

Activities, Resources and Timeline:

Task	Activity	Resource	Hours	Duration	Start Date	End Date
Review GIAC Enterprises Business			668h	12d	Fri 7/9/04	Mon 7/26/04
	Meeting to interview on business		56h	1d	Fri 7/9/04	Fri 7/9/04
		Conf Room			Fri 7/9/04	Fri 7/9/04
		Cindy Mason	8h		Fri 7/9/04	Fri 7/9/04
		Tom Young	8h		Fri 7/9/04	Fri 7/9/04
		Max Olson	8h		Fri 7/9/04	Fri 7/9/04
		Lee Jordan	8h		Fri 7/9/04	Fri 7/9/04
		Fred Smith	8h		Fri 7/9/04	Fri 7/9/04
		Laura Knight	8h		Fri 7/9/04	Fri 7/9/04
		John Doe	8h		Fri 7/9/04	Fri 7/9/04
	Travel to Big Bend Hydro Plant		24h	0.5d	Mon 7/12/04	Mon 7/12/04
		Passenger Van			Mon 7/12/04	Mon 7/12/04
		Cindy Mason	4h		Mon 7/12/04	Mon 7/12/04
		Tom Young	4h		Mon 7/12/04	Mon 7/12/04
		Max Olson	4h		Mon 7/12/04	Mon 7/12/04
		Lee Jordan	4h		Mon 7/12/04	Mon 7/12/04
		Fred Smith	4h		Mon 7/12/04	Mon 7/12/04
		Laura Knight	4h		Mon 7/12/04	Mon 7/12/04
	Interview Mark Hightower		28h	0.5d	Mon 7/12/04	Mon 7/12/04
		Conf Room			Mon 7/12/04	Mon 7/12/04
		Cindy Mason	4h		Mon 7/12/04	Mon 7/12/04
		Tom Young	4h		Mon 7/12/04	Mon 7/12/04
		Max Olson	4h		Mon 7/12/04	Mon 7/12/04
		Lee Jordan	4h		Mon 7/12/04	Mon 7/12/04
		Mark Hightower	4h		Mon 7/12/04	Mon 7/12/04
		Fred Smith	4h		Mon 7/12/04	Mon 7/12/04
		Laura Knight	4h		Mon 7/12/04	Mon 7/12/04
	Travel to Lake Coldwater Hydro Plant		24h	0.5d	Tue 7/13/04	Tue 7/13/04
		Passenger Van			Tue 7/13/04	Tue 7/13/04
		Cindy Mason	4h		Tue 7/13/04	Tue 7/13/04

		Tom Young	4h		Tue 7/13/04	Tue 7/13/04
		Max Olson	4h		Tue 7/13/04	Tue 7/13/04
		Lee Jordan	4h		Tue 7/13/04	Tue 7/13/04
		Fred Smith	4h		Tue 7/13/04	Tue 7/13/04
		Laura Knight	4h		Tue 7/13/04	Tue 7/13/04
	Interview Tim Selph		28h	0.5d	Tue 7/13/04	Tue 7/13/04
		Conf Room			Tue 7/13/04	Tue 7/13/04
		Cindy Mason	4h		Tue 7/13/04	Tue 7/13/04
		Tom Young	4h		Tue 7/13/04	Tue 7/13/04
		Max Olson	4h		Tue 7/13/04	Tue 7/13/04
		Lee Jordan	4h		Tue 7/13/04	Tue 7/13/04
		Tim Selph	4h		Tue 7/13/04	Tue 7/13/04
		Fred Smith	4h		Tue 7/13/04	Tue 7/13/04
		Laura Knight	4h		Tue 7/13/04	Tue 7/13/04
	Travel to Deep Water Hydro Plant		24h	0.5d	Wed 7/14/04	Wed 7/14/04
		Passenger Van			Wed 7/14/04	Wed 7/14/04
		Cindy Mason	4h		Wed 7/14/04	Wed 7/14/04
		Tom Young	4h		Wed 7/14/04	Wed 7/14/04
		Max Olson	4h		Wed 7/14/04	Wed 7/14/04
		Lee Jordan	4h		Wed 7/14/04	Wed 7/14/04
		Fred Smith	4h		Wed 7/14/04	Wed 7/14/04
		Laura Knight	4h		Wed 7/14/04	Wed 7/14/04
	Interview Jim Bauer		28h	0.5d	Wed 7/14/04	Wed 7/14/04
		Conf Room			Wed 7/14/04	Wed 7/14/04
		Cindy Mason	4h		Wed 7/14/04	Wed 7/14/04
		Tom Young	4h		Wed 7/14/04	Wed 7/14/04
		Max Olson	4h		Wed 7/14/04	Wed 7/14/04
		Lee Jordan	4h		Wed 7/14/04	Wed 7/14/04
		Jim Bauer	4h		Wed 7/14/04	Wed 7/14/04
		Fred Smith	4h		Wed 7/14/04	Wed 7/14/04
		Laura Knight	4h		Wed 7/14/04	Wed 7/14/04
	Travel to Lake Sunda Hydro Plant		24h	0.5d	Thu 7/15/04	Thu 7/15/04
		Passenger Van			Thu 7/15/04	Thu 7/15/04
		Cindy Mason	4h		Thu 7/15/04	Thu 7/15/04
		Tom Young	4h		Thu 7/15/04	Thu 7/15/04
		Max Olson	4h		Thu 7/15/04	Thu 7/15/04
		Lee Jordan	4h		Thu 7/15/04	Thu 7/15/04
		Fred Smith	4h		Thu 7/15/04	Thu 7/15/04
		Laura Knight	4h		Thu 7/15/04	Thu 7/15/04
	Interview Larry Phelps		28h	0.5d	Thu 7/15/04	Thu 7/15/04
		Conf Room			Thu 7/15/04	Thu 7/15/04
		Cindy Mason	4h		Thu 7/15/04	Thu 7/15/04
		Tom Young	4h		Thu 7/15/04	Thu 7/15/04

		Max Olson	4h		Thu 7/15/04	Thu 7/15/04
		Lee Jordan	4h		Thu 7/15/04	Thu 7/15/04
		Larry Phelps	4h		Thu 7/15/04	Thu 7/15/04
		Fred Smith	4h		Thu 7/15/04	Thu 7/15/04
		Laura Knight	4h		Thu 7/15/04	Thu 7/15/04
	Return to Headquarters		24h	0.5d	Fri 7/16/04	Fri 7/16/04
		Passenger Van			Fri 7/16/04	Fri 7/16/04
		Cindy Mason	4h		Fri 7/16/04	Fri 7/16/04
		Tom Young	4h		Fri 7/16/04	Fri 7/16/04
		Max Olson	4h		Fri 7/16/04	Fri 7/16/04
		Lee Jordan	4h		Fri 7/16/04	Fri 7/16/04
		Fred Smith	4h		Fri 7/16/04	Fri 7/16/04
		Laura Knight	4h		Fri 7/16/04	Fri 7/16/04
	Weekly Project Meeting		28h	0.5d	Fri 7/16/04	Fri 7/16/04
		Conf Room			Fri 7/16/04	Fri 7/16/04
		Cindy Mason	4h		Fri 7/16/04	Fri 7/16/04
		Tom Young	4h		Fri 7/16/04	Fri 7/16/04
		Max Olson	4h		Fri 7/16/04	Fri 7/16/04
		Lee Jordan	4h		Fri 7/16/04	Fri 7/16/04
		Fred Smith	4h		Fri 7/16/04	Fri 7/16/04
		Laura Knight	4h		Fri 7/16/04	Fri 7/16/04
		John Doe	4h		Fri 7/16/04	Fri 7/16/04
	Travel to Garret Fossil Fuel Plant		24h	0.5d	Mon 7/19/04	Mon 7/19/04
		Passenger Van			Mon 7/19/04	Mon 7/19/04
		Cindy Mason	4h		Mon 7/19/04	Mon 7/19/04
		Tom Young	4h		Mon 7/19/04	Mon 7/19/04
		Max Olson	4h		Mon 7/19/04	Mon 7/19/04
		Lee Jordan	4h		Mon 7/19/04	Mon 7/19/04
		Fred Smith	4h		Mon 7/19/04	Mon 7/19/04
		Laura Knight	4h		Mon 7/19/04	Mon 7/19/04
	Interview Lance Huff		28h	0.5d	Mon 7/19/04	Mon 7/19/04
		Conf Room			Mon 7/19/04	Mon 7/19/04
		Cindy Mason	4h		Mon 7/19/04	Mon 7/19/04
		Tom Young	4h		Mon 7/19/04	Mon 7/19/04
		Max Olson	4h		Mon 7/19/04	Mon 7/19/04
		Lee Jordan	4h		Mon 7/19/04	Mon 7/19/04
		Lance Huff	4h		Mon 7/19/04	Mon 7/19/04
		Fred Smith	4h		Mon 7/19/04	Mon 7/19/04
		Laura Knight	4h		Mon 7/19/04	Mon 7/19/04
	Travel to East Ridge Fossil Fuel Plant		24h	0.5d	Tue 7/20/04	Tue 7/20/04
		Passenger Van			Tue 7/20/04	Tue 7/20/04
		Cindy Mason	4h		Tue 7/20/04	Tue 7/20/04

		Tom Young	4h		Tue 7/20/04	Tue 7/20/04
		Max Olson	4h		Tue 7/20/04	Tue 7/20/04
		Lee Jordan	4h		Tue 7/20/04	Tue 7/20/04
		Fred Smith	4h		Tue 7/20/04	Tue 7/20/04
		Laura Knight	4h		Tue 7/20/04	Tue 7/20/04
	Interview Shelly Bach		28h	0.5d	Tue 7/20/04	Tue 7/20/04
		Conf Room			Tue 7/20/04	Tue 7/20/04
		Cindy Mason	4h		Tue 7/20/04	Tue 7/20/04
		Tom Young	4h		Tue 7/20/04	Tue 7/20/04
		Max Olson	4h		Tue 7/20/04	Tue 7/20/04
		Lee Jordan	4h		Tue 7/20/04	Tue 7/20/04
		Shelly Bach	4h		Tue 7/20/04	Tue 7/20/04
		Fred Smith	4h		Tue 7/20/04	Tue 7/20/04
		Laura Knight	4h		Tue 7/20/04	Tue 7/20/04
	Travel to Snow Creek Nuclear Plant		24h	0.5d	Wed 7/21/04	Wed 7/21/04
		Passenger Van			Wed 7/21/04	Wed 7/21/04
		Cindy Mason	4h		Wed 7/21/04	Wed 7/21/04
		Tom Young	4h		Wed 7/21/04	Wed 7/21/04
		Max Olson	4h		Wed 7/21/04	Wed 7/21/04
		Lee Jordan	4h		Wed 7/21/04	Wed 7/21/04
		Fred Smith	4h		Wed 7/21/04	Wed 7/21/04
		Laura Knight	4h		Wed 7/21/04	Wed 7/21/04
	Interview Joe Thomas		28h	0.5d	Wed 7/21/04	Wed 7/21/04
		Conf Room			Wed 7/21/04	Wed 7/21/04
		Cindy Mason	4h		Wed 7/21/04	Wed 7/21/04
		Tom Young	4h		Wed 7/21/04	Wed 7/21/04
		Max Olson	4h		Wed 7/21/04	Wed 7/21/04
		Lee Jordan	4h		Wed 7/21/04	Wed 7/21/04
		Joe Thomas	4h		Wed 7/21/04	Wed 7/21/04
		Fred Smith	4h		Wed 7/21/04	Wed 7/21/04
		Laura Knight	4h		Wed 7/21/04	Wed 7/21/04
	Return to Headquarters		24h	0.5d	Thu 7/22/04	Thu 7/22/04
		Passenger Van			Thu 7/22/04	Thu 7/22/04
		Cindy Mason	4h		Thu 7/22/04	Thu 7/22/04
		Tom Young	4h		Thu 7/22/04	Thu 7/22/04
		Max Olson	4h		Thu 7/22/04	Thu 7/22/04
		Lee Jordan	4h		Thu 7/22/04	Thu 7/22/04
		Fred Smith	4h		Thu 7/22/04	Thu 7/22/04
		Laura Knight	4h		Thu 7/22/04	Thu 7/22/04
	Meeting to interview on business		72h	1d	Thu 7/22/04	Fri 7/23/04
		Board Room			Thu 7/22/04	Fri 7/23/04
		Cindy Mason	8h		Thu 7/22/04	Fri 7/23/04
		Tom Young	8h		Thu 7/22/04	Fri 7/23/04

		Max Olson	8h		Thu 7/22/04	Fri 7/23/04
		Lee Jordan	8h		Thu 7/22/04	Fri 7/23/04
		Joe Boss	8h		Thu 7/22/04	Fri 7/23/04
		Board of Directors	8h		Thu 7/22/04	Fri 7/23/04
		Fred Smith	8h		Thu 7/22/04	Fri 7/23/04
		Laura Knight	8h		Thu 7/22/04	Fri 7/23/04
		John Doe	8h		Thu 7/22/04	Fri 7/23/04
	Weekly Project Meeting		28h	0.5d	Fri 7/23/04	Fri 7/23/04
		Conf Room			Fri 7/23/04	Fri 7/23/04
		Cindy Mason	4h		Fri 7/23/04	Fri 7/23/04
		Tom Young	4h		Fri 7/23/04	Fri 7/23/04
		Max Olson	4h		Fri 7/23/04	Fri 7/23/04
		Lee Jordan	4h		Fri 7/23/04	Fri 7/23/04
		Fred Smith	4h		Fri 7/23/04	Fri 7/23/04
		Laura Knight	4h		Fri 7/23/04	Fri 7/23/04
		John Doe	4h		Fri 7/23/04	Fri 7/23/04
	Meeting to interview on business		72h	1d	Mon 7/26/04	Mon 7/26/04
		Board Room			Mon 7/26/04	Mon 7/26/04
		Cindy Mason	8h		Mon 7/26/04	Mon 7/26/04
		Tom Young	8h		Mon 7/26/04	Mon 7/26/04
		Max Olson	8h		Mon 7/26/04	Mon 7/26/04
		Lee Jordan	8h		Mon 7/26/04	Mon 7/26/04
		Joe Boss	8h		Mon 7/26/04	Mon 7/26/04
		Board of Directors	8h		Mon 7/26/04	Mon 7/26/04
		Fred Smith	8h		Mon 7/26/04	Mon 7/26/04
		Laura Knight	8h		Mon 7/26/04	Mon 7/26/04
		John Doe	8h		Mon 7/26/04	Mon 7/26/04

Task Name: Review GIAC Enterprises Information Security Program

Goal: The goal of the information security program review is to give GTJD Consulting a thorough understanding of current information security practices at GIAC Enterprises.

Activities, Resources and Timeline:

Task	Activity	Resource	Hours	Duration	Start Date	End Date
Review current security			112h	2d	Tue 7/27/04	Wed 7/28/04
	Meeting to interview Information Security Staff and Internal Auditor		112h	2d	Tue 7/27/04	Wed 7/28/04
		Conf Room			Tue 7/27/04	Wed 7/28/04
		Cindy Mason	16h		Tue 7/27/04	Wed 7/28/04
		Tom Young	16h		Tue 7/27/04	Wed 7/28/04
		Max Olson	16h		Tue 7/27/04	Wed 7/28/04
		Lee Jordan	16h		Tue 7/27/04	Wed 7/28/04
		Fred Smith	16h		Tue 7/27/04	Wed 7/28/04
		Laura Knight	16h		Tue 7/27/04	Wed 7/28/04
		John Doe	16h		Tue 7/27/04	Wed 7/28/04

Task Name: Review NERC Information

Goal: The goal of the NERC information review is to ensure that GTJD Consulting and GIAC Enterprises have the same understanding of what the documents issued by NERC mean.

Activities, Resources and Timeline:

Task	Activity	Resource	Hours	Duration	Start Date	End Date
Review NERC information			112h	2d	Thu 7/29/04	Fri 7/30/04
	Meeting on NERC information		84h	1.5d	Thu 7/29/04	Fri 7/30/04
		Conf Room			Thu 7/29/04	Fri 7/30/04
		Cindy Mason	12h		Thu 7/29/04	Fri 7/30/04
		Tom Young	12h		Thu 7/29/04	Fri 7/30/04
		Max Olson	12h		Thu 7/29/04	Fri 7/30/04
		Lee Jordan	12h		Thu 7/29/04	Fri 7/30/04
		Fred Smith	12h		Thu 7/29/04	Fri 7/30/04
		Laura Knight	12h		Thu 7/29/04	Fri 7/30/04
		John Doe	12h		Thu 7/29/04	Fri 7/30/04
	Weekly Project Meeting		28h	0.5d	Fri 7/30/04	Fri 7/30/04
		Conf Room			Fri 7/30/04	Fri 7/30/04
		Cindy Mason	4h		Fri 7/30/04	Fri 7/30/04
		Tom Young	4h		Fri 7/30/04	Fri 7/30/04
		Max Olson	4h		Fri 7/30/04	Fri 7/30/04
		Lee Jordan	4h		Fri 7/30/04	Fri 7/30/04
		Fred Smith	4h		Fri 7/30/04	Fri 7/30/04
		Laura Knight	4h		Fri 7/30/04	Fri 7/30/04
		John Doe	4h		Fri 7/30/04	Fri 7/30/04

Task Name: Analysis

Goal: The goal of the analysis phase is for GTJD Consulting to analyze and compare all the information gathered about GIAC Enterprises to what is required/recommended by NERC. Then with this information, create the project deliverables and the presentation to go along with them.

Activities, Resources and Timeline:

Task	Activity	Resource	Hours	Duration	Start Date	End Date
Analysis			408h	15d	Mon 8/2/04	Fri 8/20/04
	Compile Information		60h	2.5d	Mon 8/2/04	Wed 8/4/04
		Fred Smith	20h		Mon 8/2/04	Wed 8/4/04
		Laura Knight	20h		Mon 8/2/04	Wed 8/4/04
		John Doe	20h		Mon 8/2/04	Wed 8/4/04
	Analyze information		48h	2d	Wed 8/4/04	Fri 8/6/04
		Fred Smith	16h		Wed 8/4/04	Fri 8/6/04
		Laura Knight	16h		Wed 8/4/04	Fri 8/6/04
		John Doe	16h		Wed 8/4/04	Fri 8/6/04
	Weekly Project Meeting		28h	0.5d	Fri 8/6/04	Fri 8/6/04
		Conf Room			Fri 8/6/04	Fri 8/6/04
		Cindy Mason	4h		Fri 8/6/04	Fri 8/6/04
		Tom Young	4h		Fri 8/6/04	Fri 8/6/04
		Max Olson	4h		Fri 8/6/04	Fri 8/6/04
		Lee Jordan	4h		Fri 8/6/04	Fri 8/6/04
		Fred Smith	4h		Fri 8/6/04	Fri 8/6/04
		Laura Knight	4h		Fri 8/6/04	Fri 8/6/04
		John Doe	4h		Fri 8/6/04	Fri 8/6/04
	Compile findings		60h	2.5d	Mon 8/9/04	Wed 8/11/04
		Fred Smith	20h		Mon 8/9/04	Wed 8/11/04
		Laura Knight	20h		Mon 8/9/04	Wed 8/11/04
		John Doe	20h		Mon 8/9/04	Wed 8/11/04
	Compile recommendations		48h	2d	Wed 8/11/04	Fri 8/13/04
		Fred Smith	16h		Wed 8/11/04	Fri 8/13/04
		Laura Knight	16h		Wed 8/11/04	Fri 8/13/04
		John Doe	16h		Wed 8/11/04	Fri 8/13/04
	Weekly Project Meeting		28h	0.5d	Fri 8/13/04	Fri 8/13/04
		Conf Room			Fri 8/13/04	Fri 8/13/04
		Cindy Mason	4h		Fri 8/13/04	Fri 8/13/04
		Tom Young	4h		Fri 8/13/04	Fri 8/13/04
		Max Olson	4h		Fri 8/13/04	Fri 8/13/04
		Lee Jordan	4h		Fri 8/13/04	Fri 8/13/04
		Fred Smith	4h		Fri 8/13/04	Fri 8/13/04
		Laura Knight	4h		Fri 8/13/04	Fri 8/13/04
		John Doe	4h		Fri 8/13/04	Fri 8/13/04

	Develop deliverables		48h	2d	Mon 8/16/04	Tue 8/17/04
		Fred Smith	16h		Mon 8/16/04	Tue 8/17/04
		Laura Knight	16h		Mon 8/16/04	Tue 8/17/04
		John Doe	16h		Mon 8/16/04	Tue 8/17/04
	Prepare presentation		88h	3d	Wed 8/18/04	Fri 8/20/04
	-Brainstorm possible questions		12h	0.5d	Wed 8/18/04	Wed 8/18/04
		Fred Smith	4h		Wed 8/18/04	Wed 8/18/04
		Laura Knight	4h		Wed 8/18/04	Wed 8/18/04
		John Doe	4h		Wed 8/18/04	Wed 8/18/04
	-Build slide show		12h	0.5d	Wed 8/18/04	Wed 8/18/04
		Fred Smith	4h		Wed 8/18/04	Wed 8/18/04
		Laura Knight	4h		Wed 8/18/04	Wed 8/18/04
		John Doe	4h		Wed 8/18/04	Wed 8/18/04
	-Test run of presentation		18h	1.5d	Thu 8/19/04	Fri 8/20/04
		Fred Smith	6h		Thu 8/19/04	Fri 8/20/04
		Laura Knight	6h		Thu 8/19/04	Fri 8/20/04
		John Doe	6h		Thu 8/19/04	Fri 8/20/04
	-Refine Presentation		18h	1.5d	Thu 8/19/04	Fri 8/20/04
		Fred Smith	6h		Thu 8/19/04	Fri 8/20/04
		Laura Knight	6h		Thu 8/19/04	Fri 8/20/04
		John Doe	6h		Thu 8/19/04	Fri 8/20/04
	Weekly Project Meeting		28h	0.5d	Fri 8/20/04	Fri 8/20/04
		Conf Room			Fri 8/20/04	Fri 8/20/04
		Cindy Mason	4h		Fri 8/20/04	Fri 8/20/04
		Tom Young	4h		Fri 8/20/04	Fri 8/20/04
		Max Olson	4h		Fri 8/20/04	Fri 8/20/04
		Lee Jordan	4h		Fri 8/20/04	Fri 8/20/04
		Fred Smith	4h		Fri 8/20/04	Fri 8/20/04
		Laura Knight	4h		Fri 8/20/04	Fri 8/20/04
		John Doe	4h		Fri 8/20/04	Fri 8/20/04

Task Name: Project Closure

Goal: The goal of the project closure phase is to present the plan, answer questions, ensure understanding, turn over responsibility and get sign off on project completion.

Activities, Resources and Timeline:

Task	Activity	Resource	Hours	Duration	Start Date	End Date
Project closure			80h	1d	Mon 8/23/04	Mon 8/23/04
	Final Meeting		80h	1d	Mon 8/23/04	Mon 8/23/04
		Conf Room			Mon 8/23/04	Mon 8/23/04
	-Present deliverables		36h	1d	Mon 8/23/04	Mon 8/23/04
		Cindy Mason	4h		Mon 8/23/04	Mon 8/23/04
		Tom Young	4h		Mon 8/23/04	Mon 8/23/04
		Max Olson	4h		Mon 8/23/04	Mon 8/23/04
		Lee Jordan	4h		Mon 8/23/04	Mon 8/23/04
		Joe Boss	4h		Mon 8/23/04	Mon 8/23/04
		Board of Directors	4h		Mon 8/23/04	Mon 8/23/04
		Fred Smith	4h		Mon 8/23/04	Mon 8/23/04
		Laura Knight	4h		Mon 8/23/04	Mon 8/23/04
		John Doe	4h		Mon 8/23/04	Mon 8/23/04
	-Answer questions		21.6h	1d	Mon 8/23/04	Mon 8/23/04
		Cindy Mason	2.4h		Mon 8/23/04	Mon 8/23/04
		Tom Young	2.4h		Mon 8/23/04	Mon 8/23/04
		Max Olson	2.4h		Mon 8/23/04	Mon 8/23/04
		Lee Jordan	2.4h		Mon 8/23/04	Mon 8/23/04
		Joe Boss	2.4h		Mon 8/23/04	Mon 8/23/04
		Board of Directors	2.4h		Mon 8/23/04	Mon 8/23/04
		Fred Smith	2.4h		Mon 8/23/04	Mon 8/23/04
		Laura Knight	2.4h		Mon 8/23/04	Mon 8/23/04
		John Doe	2.4h		Mon 8/23/04	Mon 8/23/04
	-Review project		7.2h	1d	Mon 8/23/04	Mon 8/23/04
		Cindy Mason	0.8h		Mon 8/23/04	Mon 8/23/04
		Tom Young	0.8h		Mon 8/23/04	Mon 8/23/04
		Max Olson	0.8h		Mon 8/23/04	Mon 8/23/04
		Lee Jordan	0.8h		Mon 8/23/04	Mon 8/23/04
		Joe Boss	0.8h		Mon 8/23/04	Mon 8/23/04
		Board of Directors	0.8h		Mon 8/23/04	Mon 8/23/04
		Fred Smith	0.8h		Mon 8/23/04	Mon 8/23/04
		Laura Knight	0.8h		Mon 8/23/04	Mon 8/23/04
		John Doe	0.8h		Mon 8/23/04	Mon 8/23/04
	-Sign off as completed		3.6h	1d	Mon 8/23/04	Mon 8/23/04
		Cindy Mason	0.4h		Mon 8/23/04	Mon 8/23/04
		Tom Young	0.4h		Mon 8/23/04	Mon 8/23/04

		Max Olson	0.4h		Mon 8/23/04	Mon 8/23/04
		Lee Jordan	0.4h		Mon 8/23/04	Mon 8/23/04
		Joe Boss	0.4h		Mon 8/23/04	Mon 8/23/04
		Board of Directors	0.4h		Mon 8/23/04	Mon 8/23/04
		Fred Smith	0.4h		Mon 8/23/04	Mon 8/23/04
		Laura Knight	0.4h		Mon 8/23/04	Mon 8/23/04
		John Doe	0.4h		Mon 8/23/04	Mon 8/23/04
	-Turn over deliverables		3.6h	1d	Mon 8/23/04	Mon 8/23/04
		Cindy Mason	0.4h		Mon 8/23/04	Mon 8/23/04
		Tom Young	0.4h		Mon 8/23/04	Mon 8/23/04
		Max Olson	0.4h		Mon 8/23/04	Mon 8/23/04
		Lee Jordan	0.4h		Mon 8/23/04	Mon 8/23/04
		Joe Boss	0.4h		Mon 8/23/04	Mon 8/23/04
		Board of Directors	0.4h		Mon 8/23/04	Mon 8/23/04
		Fred Smith	0.4h		Mon 8/23/04	Mon 8/23/04
		Laura Knight	0.4h		Mon 8/23/04	Mon 8/23/04
		John Doe	0.4h		Mon 8/23/04	Mon 8/23/04

PROJECT CHARTER

GIAC Enterprises has been tasked to comply with standards and guidelines put forth by the North American Electric Reliability Council (NERC). Upon the recommendations of the internal NERC Committee, this project was developed to analyze GIAC Enterprises current information security program against NERC requirements and recommendations. Upon completion GIAC Enterprises will have a plan of action and recommendations to follow to become compliant with the NERC standards and guidelines.

I have reviewed the NERC Security Assessment for GIAC Enterprises Project Plan. I approve the plan as defined and for the project team to proceed as planned.

GIAC Enterprises

Name: Joe Boss, CEO

Signature: _____ Date: _____

GTJD Consulting

Name: Biz Owner, CEO

Signature: _____ Date: _____

Attached amendments:

Amendment #	Date	Sponsor Signature	Project Manager Signature

PROJECT CLOSURE

As project sponsor for the receiving organization, I declare that this project has been successfully completed. GIAC Enterprises acknowledges complete understanding of the information provided in the deliverables and accepts ownership and responsibility for further implementation. All resources are hereby released and any contractual obligations contingent on this project closure may be fulfilled.

Name: Joe Boss, CEO, GIAC Enterprises

Signature: _____ Date: _____

APPENDIX

Change Request Form

Project: NERC Security Assessment for GIAC Enterprises Date: _____

Request by: _____

Requested Change:

Reason:

Pros:

Cons:

Estimated Costs:

Assumptions:

Impact if not implemented:

Alternatives:

* Sponsor approval required with submission.

* End of project plan *

Meeting/Interview Facilitation

One of the most important tasks of this project is to gain information about GIAC Enterprises' Information Security Program. To gain this information, the best method is to interview the two information security administrators who are responsible for managing and accomplishing the day to day activities of the program. In addition, a business analyst from the Administration Department and an internal auditor from General Counsel Department will be involved in the interview process. The business analyst deals with human resources and records management issues as part of his job. The internal auditor is a key player of internal security audits. We expect that these two will provide a wealth of additional information to us during the interview.

A two day meeting has been scheduled with these GIAC Enterprises' employees. In this meeting we will be interviewing and discussing the current information security processes. There will be many different areas where questions will be asked of these employees. Below are some of the questions that will be asked. They are in a format to show: 1) The question being asked (Question); 2) The information being sought (Information); 3) The person the question is directed towards (Who); and 4) Why the question was directed at that particular person (Why).

Question:	What type of threats do you consider applicable to GIAC Enterprises?
Information:	We want an idea of what GIAC Enterprises sees as threats to their business. This will give us an idea of what threats to consider that we may have not thought of. It will also give us the ability to expound on things they may not consider a threat, but in actuality is a threat.
Who:	This question is directed at the information security administrators.
Why:	The question is directed at them because they are the ones identifying potential threats. We are also looking to see if the business analyst or internal auditor has any input as to the business side relaying what they see as threats.

Question:	How does GIAC Enterprises respond to incidents as they are in progress where there are few or no mitigation factors in place?
Information:	We are trying to determine what process is used when an incident is taking place. We want to see if there is an incident response plan. This way we can maybe build on it to make it easier for them to incorporate a complete incident response program. Or perhaps, they may already have one that is complete and efficient.
Who:	This question is directed at the information security administrators.
Why:	The question is directed at them because they are the ones that have the skills and training to respond to incidents. They also work closely with system and network administrators and desktop support. So if problems occur due to an incident they would more than likely be informed of it.

Question:	What process(es) does GIAC Enterprises use to assess risk?
Information:	We are trying to determine if a risk assessment methodology is used to measure the amount of risk and what level of mitigation is required to reduce or remove the risk. We want to see whether there are cases in which technology is implemented without regard to the cost of the technology versus the value of the information it is meant to protect.
Who:	This question is directed at all four employees.
Why:	The two information security administrators because they evaluate security technology and recommend the purchase. The business analyst to see if he has information on what is involved in determining the value of the data. And the internal auditor to see if he has addressed this issue in any past audits.

Question:	Does GIAC Enterprises have disaster recovery and business continuity plans? If so, how and how often are they tested?
Information:	We want to see if GIAC Enterprises has plans to recover operations from a disaster (natural or manmade) and how they will continue business in the meantime. These plans should be tested regularly to assure they work. We are looking to see if they test. If they do test, we are also evaluating how the test is performed.
Who:	This question is directed at all four employees.
Why:	All of these employees should be involved or have knowledge of the company's disaster recovery and business continuity plans and the testing process of the plans. Knowing how and being able to recover from disasters while continuing operations is key to the survival of a business.

Question:	What type of policies does GIAC Enterprises have written? How often are they reviewed?
Information:	We want to see what level and type of policies GIAC Enterprises has in place for its employees. In particular, we want to see if policies are written in a standard and easy to read format. Checking the content to see if it is clear and concise. We want to see if there are policies to cover employee behavior as well as business process. In addition, we are trying to determine how often the policies are reviewed for accuracy. We also want to see how often employees have to read and annotate they have read and understand the policies.
Who:	This question is directed at all four employees.
Why:	We want to get a consensus to see if the policies are being disseminated to all employees, if the employees review them regularly, if the employees understand them, if they know where to locate them and if they have to sign off on them.

Question:	Does GIAC Enterprises have a corporate security awareness program? Explain how it works.
Information:	We want to see how GIAC Enterprises educates their employees and customers on information security issues. It is our experience in the energy industry that many companies have an excellent safety program but have not invested in a security awareness program. We try to convey that a security awareness program is much like a safety program. In essence, a security awareness program is a safety program for your information.
Who:	This question is directed at all four employees.
Why:	All of these employees should know about the corporate security awareness program, understand why information security is important and why it is partly their responsibility, know who the security officer is, how to identify and report incidents, as well as protect assets to the best of their ability.

Question:	What types of access controls are used for physical security?
Information:	We are trying to determine how sensitive areas are protected from unauthorized physical access. Specifically locations the business units have designated as critical assets. Such as, computer rooms, wiring closets, physical records storage, plant control rooms, etc….
Who:	This question is directed at all four employees.
Why:	The two information security administrators should know what access controls are implemented to most of the areas that are considered sensitive. The business analyst should be aware of access controls to the records storage area. The internal auditor should have knowledge of physical access controls from past audits.

Question:	What types of access controls are used for electronic access?
Information:	We are trying to determine what methods are implemented to provide secure and monitored access to electronic information. We want to see if appropriate access controls are in place with proper monitoring and possibly alerting in the case of critical assets.
Who:	This question is directed at the information security administrators.
Why:	The information security administrators perform user account setup and maintenance. They also manage permission controls on all of the electronic information.

Question:	In what way does GIAC Enterprises protect its network perimeter?
Information:	We want to see if appropriate methods are in place to protect GIAC Enterprises' network from public networks. In particular, we are looking for information on things such as firewalls, intrusion detection and other monitoring devices.
Who:	This question is directed at the information security administrators.
Why:	The information security administrators are involved with configuring and monitoring these devices.

Question:	How and when does GIAC Enterprises perform vulnerability assessments?
Information:	We are trying to determine if systems are tested for known vulnerabilities. If so, how often the systems are tested, the scope of testing, how the systems are tested and what is done with the testing results.
Who:	This question is directed at the information security administrators.
Why:	We want to identify what GIAC Enterprises' policy and process is for vulnerability testing.

Question:	What method(s) of patch management does GIAC Enterprises use for its computer systems?
Information:	We are trying to determine if systems are patched on a regular basis. We are looking at how patches are tracked, how it is determined if a patch gets applied, what it gets applied to and how the patch gets applied. We want to also determine if the patches are applied with or without testing.
Who:	This question is directed at the information security administrators.
Why:	The information security administrators work closely with the system administrators concerning system security to include patching.

Question:	What type of background screening is performed for new employees?
Information:	We are trying to determine what is done in the hiring process to check out a potential employee's background. We are looking for things like reference checks, medical history, drug testing and criminal background checks.
Who:	This question is directed at the business analyst.
Why:	The business analyst works closely with the HR staff, which is responsible for new hire screening.

Question:	What type of process is followed for terminated employees?
Information:	We are trying to determine what is done when an employee is terminated. We are looking at the various types of terminations for priority differences (retiring, resigning and firing) to see if there is a difference in response time. We are also looking for things such as notifications and removal of physical and electronic access.
Who:	This question is directed at the information security administrators and the business analyst.
Why:	The information security administrators would be responsible for access controls. The business analyst works closely with HR staff, which is responsible for sending notification to the appropriate people.

Potential Pitfalls

One of most difficult things to deal with during a project is an unanticipated problem. However, with good project management practice you can help minimize the adverse effects of these problems. If the project plan has a good risk management process defined, the project team will have a course of action to follow if the problem occurs.

In this project we have defined some risks to the project that could cause major problems if they were to occur. The risks are rated as low but could still cause major project restructuring if they occur. The two negative risks with high impact are if NERC changes their standards or guidelines and if there is a loss of a resource.

If NERC changes their standards or guidelines, there could be considerably more hours added to the project for further evaluation and planning. Or on the opposite end of the spectrum, the project could be canceled. If NERC makes changes, the project manager will have to work with the sponsor to determine what changes need to be made and if the project is to proceed. Throughout the project the project manager will be watching the NERC web site for any news or updates that may indicate an imminent change. The project manager will notify the sponsor immediately if he suspects a change may occur.

Another potential problem that could cause a significant change to the project is the loss of a resource. Since the majority of the resources for this project are people, a loss of a resource will delay the project and could possibly cause a loss of information. To help mitigate this risk, GTJD Consulting will have other analysts that can replace any of their employees in short order. GIAC Enterprises has agreed to have another employee available if one of their project members is lost. Everyone involved on the project has been instructed to document all work and get it to the project manager for review and web site posting. Loss of a resource may not have any warning signs prior to the loss. However, there may be some instances where there are indicators. If anyone senses they may have to leave the project for any reason, whether short or long term, they are to notify the project manager. The project manager will take necessary precautions to ensure another person will be ready to take over.

Value Add

With GTJD Consulting's experience and the gained knowledge from the study of GIAC Enterprises' business, the final plan to be delivered can have additional information added to increase the value of the plan beyond the scope of the project. This can be accomplished with no extra cost to GIAC Enterprises and very little additional time of GTJD Consulting. One added value could be to align the security plan with business goals in addition to the required deliverable alignment with NERC regulations. In addition, GTJD Consulting's experience with ISO17799 can be beneficial in adding value. Since there are several areas of ISO17799 apparent in the NERC regulations, the plan could be aligned with ISO17799 with minimal effort as well.

During the process of evaluating GIAC Enterprises information security program with the NERC regulations there will more than likely be a checklist of some sort created by GTJD Consulting staff. This checklist could be given to GIAC Enterprises at no extra charge in the form of a compliance checklist to be used for future self-assessments. Once again, this adds value to the project for GIAC Enterprises.

With providing a high quality product to GIAC Enterprises and adding value beyond what was expected, GTJD Consulting could possibly open the doors for future opportunities. Some leverage GTJD Consulting may have for future work would include things like knowledge of GIAC Enterprises gained from the business and security study, knowledge of how and why the plan was designed, and a good performance record during this project.

This leverage may open the door for providing consulting services with future projects. For example, there could be another project in the immediate future for helping with the implementation of the plan. Or maybe a little further down the road, there may be potential for a follow-up audit to see how successful the plan was implemented. In addition, there may be potential for other types of security engagements, such as, policy creation, awareness training, incident investigation, and/or vulnerability assessments.

Part 4: Final Deliverable

Section A: Final deliverable.

This section is the final deliverable created from the work described in the project plan.

* Start of final deliverable *

{GIAC Enterprises logo}

Plan of Action

For

GIAC Enterprises'

NERC Security Assessment

Prepared for: GIAC Enterprises

Prepared by: GTJD Consulting

Date: August 23, 2004

********** GIAC Enterprises ********** CONFIDENTIAL **********

Table of Contents

Executive Summary

On July 8, 2004, GTJD Consulting started the NERC Security Assessment project with GIAC Enterprises. This project's goal was to create a plan of action for GIAC Enterprises to follow to become compliant with the NERC Security Guidelines for the Electricity Sector (NERC SGES) and the NERC Urgent Action Standard 1200 – Cyber Security (NERC 1200).

The NERC SGES is a group of guidelines that "describe general approaches, considerations, practices, and planning philosophies to be applied in protecting the electric infrastructure."[5] These guidelines are not required but are provided to assist electricity sector participants in securing their critical assets. As with any guidelines for best practices of information security, it is a living document. Which means the guidelines change over time as security needs and threats evolve.

The NERC 1200 is a standard put forth as a minimal requirement for critical infrastructure participants in the electricity sector. This standard is intended "To reduce risks to the reliability of the bulk electric systems from any compromise of critical cyber assets."[6] It is evolving into a permanent standard, which will be known as the NERC 1300. NERC recently renewed the NERC 1200 with a year extension from August 13, 2004. The NERC 1300 standard first draft is progressing well and is expected to be out soon. It is anticipated this standard will expand the NERC 1200 to define more critical assets such as the plant control process.

During the past 6 weeks, GTJD Consulting and GIAC Enterprises have been working diligently on the project tasks that included:

- Gathering information on the current business environment of GIAC Enterprises,
- Gathering information on the current information security program of GIAC Enterprises,
- Ensuring a common understanding of the NERC standards and guidelines between the two companies, and;
- Generating this plan of action with recommendations to be implemented from the analysis of the information we gather against the NERC standards and guidelines.

[5] NERC SGES
[6] NERC 1200

Our findings indicate GIAC Enterprises is out of compliance in many areas of the NERC standards and guidelines. The majority of the non-compliance ratings come in areas where documentation is required for processes, verification of processes and documentation of training and review. Other areas with compliance issues can be classified into the areas vital to an information security program. These areas are policy, process, and technology.

In the technology area, GIAC Enterprises has a few issues that can be easily corrected. Consolidated and consistent firewall management, expanded intrusion detection monitoring, event log monitoring, encryption and authentication are the most critical areas to improve upon. The majority of these technologies are covered and required by the NERC standards and guidelines.

In the process area, GIAC Enterprises has a few more issues to correct. There are several processes that will need to be created to comply with the NERC standards and guidelines. Areas identified include testing, training, communications, employment processes, and information classification.

In the policy area, GIAC Enterprises has the most work. Policy is the driving force of an information security program. Without policies that reflect the business direction of a company, it is hard to know if you are properly implementing security. Policy tells people the right way and wrong way to perform business processes. With well-written policies, business units can write procedures to guide correct business activity.

Many companies, including GIAC Enterprises, do not have the proper focus in all three areas vital to an information security program. GIAC Enterprises' current information security program focuses mostly on technology with some attention to process. However, it is lacking in all areas. It is lacking in a few areas concerning technology, a bit more in process, and heavily in policy.

The plan of action we have created provides coverage in all of these areas in order to comply with the NERC standards and guidelines. In addition, the plan will help build an information security program to meet information security best practices. It will give you a holistic and manageable program to be proactive to future threats and trends.

To best satisfy compliance with the NERC standards and guidelines, we are proposing a plan of action to create a holistic and managed Corporate Information Security Program. The purpose of any information security program is to create a continual reduction of risks to the business environment. This is a continuous effort because business needs are changing, the technology being used is changing, and regulatory compliance issues are growing.

To have a holistic information security program, you need to have management leading from two perspectives. The first perspective is management of the administration and maintenance of information security processes to maintain the current state of security.

The other perspective involves management of processes to continuously improve security by being proactive to new threats and risks.

The plan of action we propose is comprised of the following three high-level phases.

1. Create an Information Security Department

   In this phase we recommend the creation of an Information Security Department. The senior management official charged with the responsibility of the corporate information security program will head it up. This senior management official will report to the CEO and Board of Directors. The physical and cyber security managers will report to this senior manager and manage their information security processes respectively. All information security processes will be realigned under this department.

2. Create processes for Corporate Information Security Program.

   In this phase we recommend the creation of several information security processes for the corporate information security program. The process identified fall in the following areas and provide compliance with the NERC standards and guidelines. The process areas include risk management, policy, physical security, cyber security, personnel, systems management, testing, training, recovery, threat response, communications, and document management.

3. Run security program as a holistic and managed program.

   This phase will provide information to maintain and manage a proactive information security program. It will also provide responsibilities for self-certification and compliance monitoring.

The plan of action provides details on what needs to be accomplished to form an information security program and gain compliance with the NERC standards and guidelines. It is important to form a holistic and managed information security program. This program will provide measures and processes to maintain the current state of information security. In addition, it will provide the measures and processes to direct program enhancements and to be proactive to threats and trends.

The costs to maintain a holistic information security program are higher than you are currently investing today. But the benefits you will receive from the additional investment will make information security more cost effective in the long run. Noticeable benefits would include things similar to:

- Shareholders being comfortable that their investments are sound due to your commitment to provide due diligence.
- Regulatory compliance entities being comfortable with your protective measures and acknowledgement of the importance to protect sensitive assets.

- Reducing costs by assuring security measures are aligned with business goals and processes.
- Minimize the likelihood of incidents to realize a savings in the reduced time of investigations and recovery. The MSBlast and Nachi worms of 2003 are prime examples.
- By minimizing the likelihood of incidents, you also minimize the costs that are associated with the loss of productivity, equipment, or maybe human life.

Findings and Recommendations

After analyzing all of the information we collected against the NERC standards and guidelines, we have discovered the following information to base the plan of action and our recommendations on. These following findings are grouped together by the sections of the NERC SGES. Information on the intent of the guidelines and some of the processes listed are reiterated from the NERC SGES. After completion of the NERC SGES findings we will cover the NERC 1200 findings.

1. Vulnerability and Risk Assessment:

This guideline is intended to provide a risk management process for what each company considers critical assets. The assets to be considered critical are those assets that if damaged would cause a serious "impact to a large number of customers for a long duration of time, to the reliability of the electrical grid, or cause risk to public safety and health."[5] "The guideline applies to facilities and functions that are considered critical to the support of the electricity infrastructure and the overall operation of the individual company."[5]

Finding: While there is a general consensus on which assets could be critical, the critical assets have not been formally defined and documented. Without proper vulnerability and risk management you may be spending more to protect an asset than is necessary or may not have an asset protected to the appropriate level.

Recommendation: Define and document critical assets by implementing a formal vulnerability and risk management program that has the following minimal processes:

- Identify critical assets.
- Identify the value of each critical asset if lost.
- Identify events that can cause loss of each critical asset.
- Identify the impact of each negative event.
- Identify vulnerabilities of each critical asset.
- Identify existing measures to reduce these vulnerabilities.
- Identify the likelihood of the vulnerabilities.
- Prioritize risks by overall impact versus likelihood.
- Identify potential measures to further reduce the impact of each risk.
- Identify cost of the measure.
- Perform cost/benefit analysis of each measure.
- Implement measures that are beneficial.

[5] NERC SGES

As the above steps indicate, risk management can be broken down into three processes:

- "Risk Assessment – this process includes identifying the risk, evaluating the risk, determining the impact of the risk, and how to reduce the risk.
- Risk Mitigation – this process includes prioritizing the risks, implementing measures to reduce the risks, and maintaining those measures.
- Risk Evaluation – this process includes the continual evaluation of risks."[7]

Vulnerabilities should not only be managed from a new vulnerability stance, but from a change in vulnerability or asset. Hence, there are the following sides to vulnerability management:

- Vulnerabilities are discovered of updated – In this side, either a new vulnerability was announced or a change was made to an existing vulnerability. This should prompt an assessment of the vulnerability as it applies to existing assets.
- Assets are implemented or modified – On this side, either a new asset is introduced or an old asset is modified. Either case may cause risk from a new or old vulnerability. Either type of change should prompt an assessment of the vulnerabilities that may apply to the asset.

Following a proven methodology will be key in developing an effective and efficient risk management program. Since GIAC Enterprises is at the beginning stages of building a risk management program, the OCTAVE Method (http://www.cert.org/octave/) from CERT (http://www.cert.org) would be a good method to use. "OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) is a risk-based strategic assessment and planning technique for security."[8]

2. Threat Response:

This guideline is intended to provide companies with a plan of what to do as the Electricity Sector Threat Alert Levels increase. These plans should explain what additional methods are to be implemented to protect critical assets based on the level of the threat.

Finding: GIAC Enterprises does not have any plans to increase security as the potential threat level increases.

---

[7] SANS Institute
[8] OCTAVE Method

Recommendation: NERC has developed two documents called "Threat Alert Levels and Physical Response Guidelines" and "Threat Alert Levels and Cyber Response Guidelines". It is recommended that GIAC Enterprises should monitor the ThreatCon levels via the Electricity Sector Information Sharing and Analysis Center's (ES-ISAC) website (http://www.esisac.com) or the NERC Critical Infrastructure Protection (CIP) message system (http://www.nerc.com/cip.html). We recommend implementing the recommended measures, in accordance to these documents, to provide an appropriate security posture based on the threat level.

3. Emergency Plans:

This guideline is intended to provide companies with the necessary plans to respond to a variety of threats.

Finding: GIAC Enterprises has a number of emergency action plans to cover threats of natural disasters, equipment failures, and other non-manmade events. These plans cover key issues and provide for testing and training as necessary. However, the emergency action plans need to include new threats such as terrorism, sabotage, or other manmade events.

Recommendation: Develop emergency action plans for manmade threats using current emergency action plans as a template. Also develop a management process for these emergency action plans. This process should define priorities, assign responsibilities, require periodic testing, and a method for regular review and updating.

4. Continuity of Business Processes:

This guideline is intended to provide companies with a method to help reduce the impact of an incident and recover business operations with minimal interruptions.

Finding: GIAC Enterprises has a good Business Continuity Plan in the event that one of their facilities is damaged and cannot continue operations. All areas that pertain to the NERC Guidelines are already covered, except for testing. There has been no testing of the plans.

Recommendation: Create a process to perform periodic testing of the Business Continuity Plans, and document the testing. With the results of the testing make necessary changes and improvements to the plan. Update the plans whenever changes are made to the business processes to assure business can continue in adverse conditions. Testing should be conducted at least once per year. If major changes occur, more frequent testing will be appropriate.

5. Communications:

This guideline is intended to provide communication channels with external organizations that may be providing assistance during emergency situations. In addition, it provides for internal communication of threat conditions at critical operating facilities. There are also requirements for reporting incidents to the National Information Protection Center (NIPC) and ES-ISAC.

Finding: GIAC Enterprises does not have communication interfaces with local emergency agencies such as law enforcement, fire department, and medical response teams. There is no process for communication with NIPC and ES-ISAC. GIAC Enterprises has a good communication plan for their critical facilities using cell phones and mobile radios. There is also good communication of imminent threats of natural disasters between the physical security team and each facility.

Recommendation: Develop liaisons with local, state and federal emergency entities, as well as, with NIPC and ES-ISAC. This will allow familiarization with processes to ease interaction and coordination with these entities in the event of an emergency and for the threats to be communicated to the appropriate authorities for correct setting of the Electricity Sector Threat Alert levels. For internal communication of threat conditions, establish at least two methods of communication and test these methods quarterly.

6. Physical Security:

This guideline is intended to provide a plan and process of implementing physical measures for personnel safety and to prevent unauthorized physical access to critical assets.

Finding: GIAC Enterprises has a sound physical security program that meets all NERC Guideline requirements, with the exception of two observed instances. One instance is the lack of a consistent policy on the use of identification badges from facility to facility. The other involves employees “tailgating” (following another employee) through entrances to critical facilities without using proper authentication.

Recommendation: Create a corporate policy on the implementation and use of identification badges. Train employees and ensure each person is being authenticated at controlled entrances via such methods as card keys or something similar. Do not allow people to enter restricted areas on another person’s credentials. This should be covered in the corporate security awareness program.

7. Cyber Security (Risk Management, Access Controls, IT Firewalls and Intrusion Detection):

This section of the NERC guidelines covers cyber security guidelines that refer to the electronic access, control, and monitoring of critical assets. There are four guidelines

that fall within cyber security. They are risk management, access controls, firewalls and intrusion detection.

7.1 Risk Management

This guideline is similar to the Vulnerability and Risk Assessment guideline with the intent to focus on cyber assets and risks.

Finding: GIAC Enterprises has no formal methodology for managing cyber risks.

Recommendation: Implement a risk management program for managing cyber risks by identifying assets, assessing risks, and applying measures to mitigate those risks that are applicable to cyber assets. Use a similar methodology to the one outlined in section one (Vulnerability and Risk Assessment) above. In accordance to the NERC guidelines, Cyber – Risk Management Page 1 of 3, the cyber risk management program should address the following key elements: system characterization, threat identification, vulnerability identification, control analysis, likelihood determination, impact analysis, risk determination, control recommendations and results documentation. In addition, there should be periodic reviews for changes in threats. This can be accomplished through a process that continuously monitors threats and vulnerabilities, as well as checks the current state of systems for vulnerabilities. Which should be included in a comprehensive risk management program.

7.2 Access Controls

This guideline is intended to establish a baseline for secure access control to cyber assets. It includes logical access to computer systems as well as physical access to the areas where the computer systems are located.

Finding: Physical access to the computer system locations meets all of the NERC guideline requirements. However, eliminate the “tailgating” through the physical access points. Logical access to the computer systems needs to be improved. There were some areas where authentication and monitoring on critical cyber assets was rather weak. The remote connections to the plant control systems are one area that we can identify as unacceptable. Anyone with a valid user id and password can gain remote access and take control of the plant control systems from anywhere within the internal network. This assumes they also have the remote control software installed on the computer they are on. The remote sessions do not provide encryption for protection from wiretapping. Someone could possibly monitor a session to gather critical information, such as a user id and password to access the plant control system. There is logging of the connections but no one is responsible for reviewing the logs. The logs are only reviewed for troubleshooting purposes.

Recommendation: Educate employees about tailgating other employees through access control points. Review requirements for access to critical cyber assets. Implement stronger authentication and encryption to critical cyber assets. In addition, limit access only from the locations where it is absolutely necessary to conduct business. Stronger two factor identification measures should be incorporated into both physical and logical (cyber) access. We recommend implementing a system that can use public key infrastructure (PKI) technology for both types of access. Implement a process for consistent monitoring of the logs for unauthorized access and other events.

7.3 IT Firewalls

This guideline is intended to make companies aware of the electronic perimeter and how to use firewalls to protect the cyber assets within that electronic perimeter.

Finding: GIAC Enterprises uses firewall technology to segment its private network from the Internet. The plants also use firewall technology to segment the plant control systems from the internal network. All firewalls are of the same make. The firewall rules for the firewall between the Internet and internal network has a good rule set. It only allows necessary traffic in and out. If it fails, no traffic is allowed. This is good. The plant firewalls need some work. The rule set for these firewalls allows for unauthenticated and unencrypted remote access from anywhere within the internal network. This is not good. In addition, no process is defined for log monitoring.

Recommendation: Change the plant firewall appliances to a different brand than the Internet firewall. If the Internet firewall is compromised by some vulnerability, then the plant control systems cannot be compromised by the same vulnerability. Also, strengthen the rule set on plant firewalls. Remote access to plant control systems should be authenticated and the communication encrypted prior to the authentication until the session is terminated. GIAC Enterprises should consider using Virtual Private Networks or IPSec technology. Implement a process for consistent log monitoring.

7.4 Intrusion Detection

This guideline is intended to iterate the importance and criticality of intrusion detection technology. It identifies some resources that are available to help develop a better understanding of intrusion detection systems that will help mitigate risks.

Finding: GIAC Enterprises has an intrusion detection system that monitors incoming traffic that originates from the Internet and enters the internal network. There are no other sensors other than this one.

Recommendation: Expand the network-based intrusion detection configuration to watch traffic to and from network segments that house critical cyber assets. The intrusion detection logs should be monitored and responded to appropriately. Monitoring incoming traffic will identify attacks on the critical cyber assets. Monitoring outgoing traffic will help to identify compromised systems. GIAC Enterprises may also want to consider implementing some intrusion prevention technology. With intrusion prevention technology you can respond to certain types of traffic automatically without human intervention. On critical cyber assets, consider implementing host-based intrusion detection.

8. Employment Background Screening:

This guideline is intended to lower the "insider" threat by assuring only trustworthy and reliable personnel have unescorted access to critical facilities. Effective pre-employment screening can help mitigate threats from people on the inside.

Finding: GIAC Enterprises does not perform background screening for any positions.

Recommendation: Start conducting background screening of personnel being consistent with the degree of access they are granted, especially in the areas where employees have access to critical assets.

9. Protecting Potentially Sensitive Information:

This guideline is intended to complement an information classification policy. The policy should address creation, storage, transmission, and disposal of information whether in physical or electronic form. This guideline provides information to help identify and secure sensitive information. It provides several questions to ask when deciding if information is sensitive. In addition, it provides ideas as to how the sensitive information could be secured.

Finding: GIAC Enterprises does not have an information classification policy.

Recommendation: Create an information classification policy to address the creation, storage, transmission, and disposal of information at a minimum. This policy should be communicated to employees through a security awareness program. Implement a process to classify information. Consider using some of the questions from this section the NERC SGES to help identify sensitive information.

Now that we have finished the sections of the NERC SGES, we will focus on the NERC 1200. The following findings are grouped by section found in NERC 1200 – Cyber Security Standard. The requirements and compliance measures listed, as well as the non-compliance levels, come from the NERC 1200 document.

1. Section 1201 - Cyber Security Policy:

This section of the NERC standard requires the entity to create and maintain a cyber security policy. The measures for compliance are:

- The entity shall maintain a written cyber security policy stating their commitment to protect critical cyber assets.
- This policy will be reviewed at least annually.
- The senior management official responsible for the cyber security program will be identified by name, title, phone, address, and date of designation.
- The justification for any deviations or exemptions must be documented the senior management official responsible for the cyber security program.

Finding: GIAC Enterprises does not have a Cyber Security Policy or the responsibility of a cyber security program assigned to a senior management official. This would rate GIAC Enterprises at a level four of non-compliance.

Recommendation: Appoint a senior management official to be responsible for the cyber security program and create and maintain a cyber security policy that is reviewed at least annually. This senior management official should be solely charged with the responsibility of all Information Security management. All information security personnel should report to this official. This person is typically labeled as the Chief Security Officer (CSO). The cyber security policy should cover the minimum requirements found in the section of the NERC 1200.

2. Section 1202 - Critical Cyber Assets:

This section of the NERC standard requires the entity to identify all of its critical cyber assets. The measures for compliance are:

- Maintain a document identifying critical cyber assets.
- Review and update the document at least annually or within 90 days of the addition or removal of a critical cyber asset.

Finding: GIAC Enterprises does not have a document identifying its critical cyber assets. This would rate GIAC Enterprises at a level four of non-compliance.

Recommendation: Identify and document all critical cyber security assets. Create a process to review this document and a control process to identify the addition, modification, or removal of a critical cyber asset. The initial identification of critical cyber

assets can be included with the other critical assets when implementing the risk management program per our recommendation in the NERC SGES section 1 above.

3. Section 1203 - Electronic Security Perimeter:

This section of the NERC standard requires the entity to identify its electronic security perimeter. The measures for compliance are:

- Maintain a document depicting the electronic security perimeter, all interconnected critical cyber assets, and all electronic access points to the interconnected environments. This document must verify that all critical cyber assets are within the electronic security perimeter.
- Review and update this documentation at least annually or within 90 days of modification of the network.

Finding: GIAC Enterprise maintains a network diagram depicting all required information and updates this documentation as changes are made. This would rate GIAC Enterprises as being fully compliant.

Recommendation: Even though GIAC Enterprises is fully compliant, we would recommend that the network diagrams be updated with a dedicated diagram that only highlights all of the critical cyber assets. This document should clearly be able to verify that all critical cyber assets are within the electronic security perimeter. Implement a process to ensure the review process is accomplished annually and any modifications are updated within 90 days.

4. Section 1204 - Electronic Access Controls:

This section of the NERC standard requires the entity to identify and implement electronic access controls for access to critical cyber assets within the electronic security perimeter. The measures for compliance are:

- Maintain a document identifying the access controls and their implementation for each electronic access point to the electronic security perimeter.
- Review and update this documentation at least annually or within 90 days of modification of the electronic security perimeter or electronic access controls.

Finding: GIAC Enterprises does not have a document identifying all access controls and their implementation for each electronic access point to the electronic security perimeter. This would rate GIAC Enterprises at a level four of non-compliance.

Recommendation: Create a document that identifies all access controls and how they are implemented for each access point to the electronic security perimeter. Create a process to review this document and a control process to identify any modifications to the electronic security perimeter or electronic access controls.

5. Section 1205 - Physical Security Perimeter:

This section of the NERC standard requires the entity to identify its physical security perimeters for the protection of critical cyber assets. The measures for compliance are:

- Maintain a document depicting physical security perimeters and all physical access points to every such perimeter. The document shall verify that all critical cyber assets are within the physical security perimeters.
- Review and update this documentation at least annually or within 90 days of modification.

Finding: GIAC Enterprises has a diagram of physical security perimeters and all access points to those perimeters. The diagrams have not been modified to depict changes made recently (within the past 90 days). This would rate GIAC Enterprises at a level one of non-compliance.

Recommendation: Implement a process to ensure the review of these diagrams at least annually and a control process to update these diagrams within 90 days after modifications.

6. Section 1206 - Physical Access Controls:

This section of the NERC standard requires the entity to identify and implement physical access controls for access to critical cyber assets within the physical security perimeter. The measures for compliance are:

- Maintain a document identifying the access controls and their implementation for each physical access point to the physical security perimeter.
- Review and update this documentation at least annually or within 90 days of modification of the physical security perimeter or physical access controls.

Finding: GIAC Enterprises does not have a document identifying all access controls and their implementation for each physical access point to the physical security perimeter. This would rate GIAC Enterprises at a level four of non-compliance.

Recommendation: Create a document that identifies all access controls and how they are implemented for each access point to the physical security perimeter. Create a process to review this document and a control process to identify any modifications to the physical security perimeter or physical access controls.

7. Section 1207 - Personnel:

This section of the NERC standard requires the entity to identify all personnel, including contractors and service vendors, granted electronic or physical access to critical cyber assets. The measures for compliance are:

- Maintain a list of all personnel granted access to critical cyber assets, including the specific electronic and physical access rights to the security perimeters.
- Review the document at least quarterly and update the document within 24 hours of any change.
- Conduct background screening of personnel consistent with the degree of access they are granted, in accordance with federal, state, provincial, and local laws.

Finding: GIAC Enterprises does not maintain a list of personnel granted access to critical cyber access. In addition, no background screening is performed on any personnel. This would rate GIAC Enterprises at a level four of non-compliance.

Recommendation: Create a document that identifies all personnel granted access to critical cyber assets, including the specific electronic and physical access rights to the security perimeters. Create a process to review this document and a control process to identify and make updates of any changes. Start conducting background screening of personnel being consistent with the degree of access they are granted.

8. Section 1208 - Monitoring Physical Access:

This section of the NERC standard requires the entity to monitor physical access to critical cyber assets, 24 hours a day, 7 days a week. The measures for compliance are:

- Maintain a document identifying the tools and procedures for physical access monitoring. This document must verify that the tools and procedures are functioning and being used as planned.
- Document physical access to critical cyber assets via access records. Access records shall be verified against the list of access control rights or be controlled by video or other physical monitoring.

Finding: GIAC Enterprises does not have a document identifying the tools and procedures for physical access monitoring. However, access records are maintained and/or video controlled monitoring is used. There is not a level of non-compliance defined to fit GIAC Enterprises' situation. GIAC Enterprises does not fully comply and the best non-compliance fit would probably be a level one of non-compliance.

Recommendation: Create a document identifying the tools and procedures used to monitor physical access. Verify the recorded access list against the document. Create a process to store the access lists for a three-year period.

9. Section 1209 - Monitoring Electronic Access:

This section of the NERC standard requires the entity to monitor electronic access to critical cyber assets, 24 hours a day, 7 days a week. The measures for compliance are:

- Maintain a document identifying electronic access monitoring tools and procedures. This document must verify that the tools and procedures are functioning and being used as planned.
- Document electronic access to critical cyber assets via access records. Access records shall be verified against the list of access control rights.

Finding: GIAC Enterprises does not have a document identifying electronic access monitoring tools and procedures. The systems are configured to log access attempts in system log files. However, these log files are not being monitored.

Recommendation: Implement tools for log file monitoring. Document these tools and verify that they are functioning and being used as planned. Consider tools that consolidate log file data and provide a reporting mechanism. Assign responsibility to monitor this information and periodically verify and document it is functioning correctly. Create a process to store the access records for a three-year period.

10. Section 1210 - Information Protection:

This section of the NERC standard requires the entity to protect information associated with critical cyber assets and the policies and practices used to keep them secure. The measures for compliance are:

- Maintain a document identifying the access limitations to sensitive information related to critical cyber assets. At as minimum, this document must address access to procedures, critical asset inventories, maps, floor plans, equipment layouts and configurations.
- Review and update the document as necessary and at least annually.

Finding: GIAC Enterprises does not maintain a document identifying access limitations to sensitive information. This would rate GIAC Enterprises at a level four of non-compliance.

Recommendation: Create a document that identifies access limitations to sensitive information. This will require that sensitive information be identified. This should come from a corporate information classification program. GIAC Enterprises should create an information classification program that breaks information into various sensitivity levels. This program should also define the process that new information must go through to be classified, as well as destruction and reclassification procedures.

11. Section 1211 - Training:

This section of the NERC standard requires the entity to train personnel in the areas (see below for minimum training) related to their access to critical cyber assets. Training shall be conducted upon initial employment and reviewed annually. The measures for compliance are:

- Maintain a company-specific cyber security training program that includes at a minimum, the following required items.
  - The cyber security policy.
  - Physical and electronic access controls to critical cyber assets.
  - The release of critical cyber asset information.
  - Potential threat incident reporting.
  - Action plans and procedures to recover or re-establish critical cyber assets following a cyber security incident.
- Maintain a document identifying all personnel who have access to critical cyber assets and the date of the successful completion of their training.
- Document that the training program has been reviewed at least annually.

Finding: GIAC Enterprises does not have a training program. This would rate GIAC Enterprises at a level four of non-compliance.

Recommendation: Create an Information Security Awareness Program under the charge of the CSO. A successful Information Security Awareness program only comes with upper management support. "Without visible executive stewardship, information security awareness programs are doomed to fail."[9] This program should include the above minimum requirements, plus training on other corporate policies and procedures.

12. Section 1212 - Systems Management:

This section of the NERC standard requires the entity to establish systems management policies and procedures for configuring and securing critical cyber assets. The measures for compliance are:

- Maintain a document identifying system management policies and procedures.
- Review and update the document as necessary and at least annually.
- The systems management policies and procedures document shall address all of the following, at a minimum:
  - The use of effective password management that periodically requires changing of passwords, including default passwords for newly installed equipment.
  - The authorization and periodic review of computer accounts and access rights.
  - The disabling of unauthorized, invalidated, expired, or unused computer accounts and physical access rights.
  - The disabling of unused network services and ports.
  - Secure dial-up modem connections.
  - Firewall management.
  - Intrusion detection processes.

[9] Tech Republic

  - Security patch management.
  - The installation and update of anti-virus software.
  - The retention and review of operator logs, application logs, and intrusion detection logs.
  - Identification of vulnerabilities and responses.
- Implement systems management policies and procedures as described in the systems management policies and procedures document.

Finding: GIAC Enterprises does not have systems management policies and procedures documented. This would rate GIAC Enterprises at a level four of non-compliance.

Recommendation: Create a document for systems management policies and procedures to meet the minimum requirements identified above. Charge the CSO with the task, as with the creation of other corporate policies and procedures.

13. Section 1213 - Test Procedures:

This section of the NERC standard requires the entity to establish test procedures and acceptance criteria to ensure critical cyber assets installed or modified comply with the security requirements in the NERC 1200 standard. Test procedures shall require that testing and acceptance be conducted in an isolated test environment. The measures for compliance are:

- Maintain a document identifying test procedures and acceptance criteria for the installation or modification of critical cyber assets.
- Maintain a document verifying that it has implemented the test and acceptance criteria.

Finding: GIAC Enterprises does not have a document identifying test procedures and acceptance criteria or verifying that it has been implemented. This would rate GIAC Enterprises at a level four of non-compliance.

Recommendation: Establish test procedures and acceptance criteria that satisfy NERC 1200 Standard requirements. Document the test procedures and acceptance criteria. Document the verification of the implementation of these test procedures and acceptance criteria. Implement a process that will ensure that critical cyber assets installed of modified go through these tests and meet the acceptance criteria.

14. Section - 1214 Electronic Incident Response Actions:

This section of the NERC standard requires the entity to define electronic incident response actions, including roles and responsibilities assigned by individual or job function. The measures for compliance are:

- Maintain a document defining the electronic incident response action, including actions, roles and responsibilities.
- This document shall require that incidents involving critical cyber assets be reported to the electricity sector information sharing and analysis center in accordance with NERC-NIPC Indications, Analysis, Warnings Program Standard Operating Procedure.

Finding: GIAC Enterprises does not have an electronic incident response program. This would rate GIAC Enterprises at a level four of non-compliance.

Recommendation: Charge the CSO with the creation of a corporate incident response program. This program should incorporate the compliance measures above, as well as a corporate policy on incident response, other accompanying procedures and a reporting method to the electricity sector information sharing and analysis center.

15. Section 1215 - Physical Incident Response Actions:

This section of the NERC standard requires the entity to define physical incident response actions, including roles and responsibilities assigned by individual or job function. The measures for compliance are:

- Maintain a document defining the physical incident response action, including actions, roles and responsibilities.
- This document shall require that incidents involving physical assets used to protect critical cyber assets be reported to the electricity sector information sharing and analysis center in accordance with NERC-NIPC Indications, Analysis, Warnings Program Standard Operating Procedure.

Finding: GIAC Enterprises does not have a physical incident response program. This would rate GIAC Enterprises at a level four of non-compliance.

Recommendation: Include these requirements in the corporate incident response program described in the Electronic Incident Response Actions section above.

16. Section 1216 - Recovery Plans:

This section of the NERC standard requires the entity to create action plans and procedures to recover or re-establish critical cyber assets following a cyber security incident. Each responsible entity shall exercise these plans annually. The plans and procedures shall define roles and responsibilities by individual of job function. The measures for compliance are:

- Maintain a document defining the action plan and procedures used to recover or re-establish critical cyber assets following a cyber security event, including actions, roles and responsibilities.

- Maintain a document verifying that the action plan is exercised via drill at least annually.

Finding: GIAC Enterprises does have some recovery plans developed. However, the plans are not exercised annually. This would rate GIAC Enterprises at a level two of non-compliance.

Recommendation: Disaster recovery plans should be in place for all critical systems, especially the critical cyber assets. For all critical cyber assets, document the action plans and procedures to recover or re-establish critical cyber assets after a cyber security event. Exercise these plans at least annually, documenting the exercise and the results. Make necessary modifications to the plans and procedures as necessary. The CSO should be charged with the creation and management of a corporate disaster recovery program.

Plan of action and further recommendations

This plan provides the recommended actions to take to form a sound corporate information security program that will be prepared to meet your security needs, from general security practices to regulatory compliance with the NERC standards and guidelines.

1. Create an Information Security Department.

    1.1. Hire or appoint a Chief Security Officer (CSO)

    A senior level management representative should be assigned responsibility for the corporate security program. This will include responsibility for all regulatory tasks such as those found in the NERC standards and guidelines.

    In addition, this will show the proper level of support for the program and will give authority at the appropriate level. With all of the different business boundaries that are crossed for information security compliance and enforcement it is difficult, if not impossible, to successfully manage and enforce compliance with an information security program from any other level of authority. We have found it hard to gain support and acceptance by all employees when information security is managed at those lower levels.

    The CSO should be someone with a broad high-level knowledge of information security. They should have an extensive background in the information security profession as well as management experience and a graduate level degree in business or management. Many companies look for certification and military background. Certification as a Certified Information System Security Professional (CISSP) is one of the most popular certifications for a CSO candidate. Military experience is another good requirement due to the multitude and level of security processes involved. Often military experienced personnel will have a more structured and disciplined security posture due to the nature of the military. The CSO should be able to understand the business and identify risks and threats to that business.

    1.2. Work with CSO to build information security architecture.

    Build an information security architecture that will be managed by the CSO. This architecture should align all information security responsibilities under the CSO and allow the CSO to manage and direct the corporate security program appropriately.

Under the CSO should be two managers, one for physical security responsibilities and the other for cyber security responsibilities. The structure should look something like the following:

Chief Security Officer		
	Information Security Program	
Physical Security Mgr. Physical Perimeter, Access Control, and Monitoring. Manage Physical Security personnel and processes.	<<<Responsibility Overlap>>> Policies Security Awareness Audit DR/BCP Risk Management Access Lists Threat and Incident Response	Cyber Security Mgr. Electronic Perimeter, Access Control, and Monitoring. Manage Cyber Security personnel and processes.

1.3. Hire appropriate staff to complete the architecture.

Hire or realign managers under CSO. Hire or realign staff to perform the day-to-day activities of the information security program, as well as perform proactive activities to keep the information security program at an acceptable level of compliance. When considering staff, look for staff with education and experience in the areas they are responsible. In addition, it is highly recommended to seek individuals with security certifications. Certifications not only show demonstrated knowledge in the area, but also show an individuals' ability to start and follow through on a task.

As you are can see, there are many new processes to be created. You will have to hire additional staff for your program, mostly cyber security staff and a few physical security staff, to support these processes. The CSO will be able to gauge what staff is needed in accordance to his/her management style and the skills required.

2. Create process for Corporate Information Security Program

2.1. Implement a comprehensive risk management program.

Risk Management can be broken down into three processes:

- "Risk Assessment – this process includes identifying the risk, evaluating the risk, determining the impact of the risk, and how to reduce the risk.
- Risk Mitigation – this process includes prioritizing the risks, implementing measures to reduce the risks, and maintaining those measures.
- Risk Evaluation – this process includes the continual evaluation of risks."[7]

[7] SANS Institute

Implement a comprehensive risk management program that covers all assets of GIAC Enterprises. Including the critical assets and critical cyber assets. Follow a structured process such as the OCTAVE method to identify assets and vulnerabilities. Then prioritize these in order to evaluate and implement risk mitigation measures.

When performing your risk assessment, mitigation and evaluation processes, ensure you meet all the following processes at a minimum (as defined in the Vulnerability and Risk Assessment section of the NERC SGES):

- Identify critical assets.
- Identify the value of each critical asset if lost.
- Identify events that can cause loss of each critical asset.
- Identify the impact of each negative event.
- Identify vulnerabilities of each critical asset.
- Identify existing measures to reduce these vulnerabilities.
- Identify the likelihood of the vulnerabilities.
- Prioritize risks by overall impact versus likelihood.
- Identify potential measures to further reduce the impact of each risk.
- Identify cost of the measure.
- Perform cost/benefit analysis of each measure.
- Implement measures that are beneficial.

When identifying all critical assets, be sure to document them to satisfy the requirements defined in Section 1202 of the NERC 1200 Standard.

Upon completion of this risk assessment, you will have an initial list of documented critical cyber assets as well as other assets. This document will identify the value, risks, vulnerabilities associated with each asset. At this point, you will be in a position to possibly identify other measures to put in place to mitigate risks in addition to the ones we identify. Anytime new assets are introduced or existing assets are modified, you should perform a risk assessment to assure the assets are properly protected.

2.2. Policy

Policies are very important in providing employees with guidance on what is expected of them in day-to-day operations. They set standards of behavior for the entire company. GIAC Enterprises needs to create policies that cover many aspects of information, both for NERC standards and guidelines as well as everyday business operations. With good policies created the business units can create adequate procedures for their tasks to comply with the policies. Policies should be reviewed upon employment by all employees and at least annually. The review should be document and understanding of the policies acknowledged by the employee signing off on them.

When writing policies the following areas should be addressed at a minimum: Purpose, Scope, Definitions, Enforcement, Exceptions, and Revision Control. The policy should be clear, concise, enforceable and compliant with state and federal laws.

2.2.1 Create a minimum of the following policies to comply with NERC standards and guidelines:

2.2.1.1 Cyber Security Policy – This policy should reflect:
- A statement of commitment to protect critical cyber assets.
- Identify the person responsible for the security program by name, title, phone number, address, and date of designation. This will be your CSO.
- Requirement to review the policy annually.
- Requirement to document any justification for deviations or exemptions to the policy.

2.2.1.2 Physical Access Control Policy – Create a policy that defines the business and regulatory requirements for physical access to facilities and restricted areas. Incorporate our recommendations for use of identification badges.

2.2.1.3 Electronic Access Control Policy – Create a policy that defines the business and regulatory requirements for electronic access to logical assets. Incorporate our recommendations for use of stronger authentication and encryption mechanisms.

2.2.1.4 Information Classification Policy – Create policy that addresses the classification of information into various and appropriate sensitivity levels. This policy should cover the classification of information as it is created, stored, transmitted, and destroyed.

2.2.1.5 Incident Response Policy – Create a policy that addresses what should be done in the event of a physical or cyber incident.

2.2.2 Create the following policies as general good practice:

2.2.2.1 Acceptable Use Policy – Create a policy that defines the acceptable use of electronic assets of the company.

2.2.2.2 Internet Use Policy – Create a policy that defines how the Internet can be used in the business environment.

2.2.2.3 Electronic Mail Policy – Create a policy that defines how electronic mail can be used in the business environment.

2.2.2.4 Privacy Policy – Create a policy that defines how privacy issues will be handled within the company.

2.2.2.5 Remote Access Policy – Create a policy that defines how electronic remote access to company systems is obtained and used.

2.2.2.6 Network connection policy – Create a policy that defines when and how a device can be connected to the network. This should cover new devices and devices that have been away from the network and brought back.

There are many other policies that can be written. You will have to choose the ones that are right for your business. There are many resources available to help define policies. Charles Cressen Wood has an excellent book on polices called "Information Security Policies Made Easy".

When writing these policies keep in mind third party users such as service vendors are contract personnel. Also give some thought to business partners or possible acquisitions.

2.3. Physical Security

GIAC Enterprises already has a good structure for physical security with a manager to manage all aspects of the processes in place. We recommend that you move this management position to report directly to the CSO, bringing all responsibilities for physical security under the Corporate Information Security Program.

2.3.1. Security Perimeter – Continue to maintain diagrams of the physical security perimeters and all access points to those perimeters. Create a process that to review these diagrams periodically and update the diagrams as changes occur.

2.3.2. Access Controls – Create a document that identifies all access controls and their implementation for each access point to the physical security perimeter. Create a process to review this documentation periodically and update the documentation with any changes to the access controls. Create a standard method of employee identification. The use of identification badges with employee photo and information would be one option. Visitors, contractors and vendors could have a visitor badge of a different color (red) so they could easily be identified as a non-employee. These identification badges could be incorporated with a two-factor electronic access control. One token for use in both physical and logical (cyber) access.

2.3.3. Monitoring – Create a document identifying the tools and procedures for physical access monitoring. Document that the tools and procedures have been verified and are functioning as planned. For access to critical cyber

assets in areas that are not controlled by video or physical monitoring an access record must be maintained. This can be accomplished through access devices that digitally record the access via an identification badge swipe or proximity card reader.

2.4. Cyber Security

The cyber security processes for GIAC Enterprises is spread across many areas within your Information Technology (IT) Department. This is common in many companies because many of the processes require the technical skills that are found in the IT department. However, Chief Information Officers (CIO) should not be responsible for information security. According to some information security professionals, "CIOs have to deal with agendas that can conflict with security. They have to balance the needs of the chief operating officer who wants to save money, along with network administrators who want to guarantee open networks regardless of the need for security."[10] With electronic security, the first step is to realign all cyber security processes under the CSO giving the management responsibility to the Cyber Security Manager.

2.4.1. Assign electronic security management responsibility to the CSO. Move or hire personnel responsible for administering information security technology under the Cyber Security Manager who reports to the CSO. These individuals should be encouraged to work with and maintain relations with the IT staff.

2.4.2. Security Perimeter – Continue to keep good documentation of your network and security perimeter. However, make sure all critical cyber assets are depicted on the diagram. Also create a process that will assure all changes are updated within 90 days and the document gets reviewed annually. Keep records of when this documentation was last updated or reviewed for accuracy. Continue the good job you are doing on your external firewall. Change the plant firewall appliances to a different brand from the Internet firewall to prevent a firewall compromise flowing straight through to the plant control systems. Strengthen the rule set on plant firewalls. Apply encryption and stronger two-factor authentication for remote access to plant control systems.

2.4.3. Access Controls – Create documentation that depicts all electronic access controls and their implementation for each access point to the electronic security perimeter. Create a process to update this document when changes are made and to review this document periodically. Document when the last update or review took place.

---

[10] InternetNews

2.4.4. Monitoring – Implement tools for log monitoring on critical cyber assets. Document these tools, as well as the verification that the tools are working as intended. Create a review process to verify this documentation is current and the tools are working as intended. Expand your intrusion detection systems to monitor all critical cyber assets.

2.4.5. Standard configurations and configuration management – Implement a process to configure platforms of the same nature to a company standard. Manage changes to those platforms to ensure consistency. Ensure only authorized software is installed and used on the appropriate platforms. Ensure only authorized devices are attached to the corporate network.

2.4.6. Patch Management – Implement a process to monitor patches for all platforms. This process should identify missing patches, a testing process for new patches, and an upgrade path for applying the new patches.

2.4.7. Vulnerability Assessment – Implement a process to test all platforms for vulnerabilities. This process should provide a mechanism to assess the risk of the identified vulnerabilities and a course of action to handle the vulnerability. Vulnerabilities should be assessed for new systems as well as old systems as they are modified. Any new vulnerability should be reviewed for applicability in your environment.

2.4.8. Antivirus – Implement a process to verify virus updates and current software are being distributed to all necessary devices.

2.4.9. Content filtering – Implement a process to monitor and filter content of web and e-mail traffic as it enters GIAC Enterprises' network from the Internet.

2.5. Personnel

2.5.1. Background Checks – Create a procedure to require successful background checks for new personnel as a condition of their employment.

2.5.2. Terminations – Create a procedure to detail the process that is to be followed when an employee is terminated. This should include revoking the former employee's physical and electronic access.

2.5.3. Access list – Create a document to identify all personnel granted access to critical cyber assets. Create a process to review this document periodically and update any changes immediately.

2.6. Systems Management

Create a document for systems management policies and procedures in accordance with the minimum requirements in Section 1212 of the NERC 1200 standard. This document should contain the following policies and procedures at a minimum:

- The use of effective password management that periodically requires changing of passwords, including default passwords for newly installed equipment.
- The authorization and periodic review of computer accounts and access rights.
- The disabling of unauthorized, invalidated, expired, or unused computer accounts and physical access rights.
- The disabling of unused network services and ports.
- Secure dial-up modem connections.
- Firewall management.
- Intrusion detection processes.
- Security patch management.
- The installation and update of anti-virus software.
- The retention and review of operator logs, application logs, and intrusion detection logs.
- Identification of vulnerabilities and responses.

2.7. Testing

Establish test procedures and acceptance criteria for implementation of changes to critical cyber assets. The testing is to be done in an isolated test environment. The test procedures and acceptance criteria should be documented. Documentation should be maintained on the implementation and verification that these procedures and criteria are being used. In addition, remember to perform a risk assessment of new or changing assets.

2.8. Training

Create a corporate security awareness program that is in accordance with the minimum requirements of section 1211 of the NERC 1200 standard. The training should include the following items at a minimum:

- The cyber security policy.
- Physical and electronic access controls to critical cyber assets.
- The release of critical cyber asset information.
- Potential threat incident reporting.
- Action plans and procedures to recover or re-establish critical cyber assets following a cyber security incident.

In addition, include training on other corporate polices and procedures, security practices, and current security events. Document the training and understanding of the information for each employee at least annually. This documentation should require employee acknowledgement.

Keep security personnel on top of trends in the information security profession. Training, conferences, mail lists, Internet, newsletters, and magazines are all good ways of keeping up to date on what is happening in the world of security. Encourage participation in user groups such as the Information System Security Association (ISSA).

Subscribe to mailing lists to receive information on new vulnerabilities and threats. Securiteam (http://www.securiteam.com/) and US CERT (http://www.us-cert.gov/) both have good mail lists that provide current information on threats and vulnerabilities.

2.9. Recovery

Charge the CSO with creating a corporate business continuity and disaster recovery program.

2.9.1. Business Continuity Planning – Continue to keep up a good business continuity plan. Create a process to be used to test the plans at least annually and make updates as necessary.

2.9.2. Emergency Action Plans – Take the emergency action plans you have for natural disasters and use them to develop emergency action plans for manmade threats. Create a management process for these emergency action plans that defines priorities, assigns responsibilities, requires periodic testing, and has a method for regular review and updating.

2.9.3. Recovery Plans – Create disaster recovery plans for all critical systems. For all critical cyber assets, document the action plans and procedures to recover or re-establish critical cyber assets after a cyber security event. Test these plans at least annually, documenting the testing and the results. Make necessary modifications to the plans and procedures as necessary.

2.10. Threat Response

2.10.1. Electricity Sector Threat Alert Level - We recommend that GIAC Enterprises monitor the Electricity Sector Threat Alert level on the Electricity Sector Information Sharing and Analysis Center (ES-ISAC) website (http://www.esisac.com) and act in accordance to the documents they have pertaining to Threat Alert Levels. The documents are titled “Threat Alert Levels and Physical Response Guidelines” and “Threat Alert Levels and

Cyber Response Guidelines". These guidelines can be found on the ES-ISAC website (http://www.esisac.com/library-guidelines.htm).

2.10.2. Physical and Electronic Incident Response - Create a corporate incident response program. Per the NERC 1200, you must maintain a document defining the physical and electronic incident response actions, including the actions, roles and responsibilities. In addition to the policy created in 2.2.1.5 above, create other accompanying procedures for the policy and a reporting mechanism to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC). Communication procedures for reporting incidents to ES-ISAC can be found in the "Electricity Sector Critical Infrastructure Protection Communications" document found at the ES-ISAC website (http://www.esisac.com/publicdocs/communications/es-isac_communic.pdf).

2.11. Communications

The Physical Security Manager should continue to monitor and improve communication channels for internal communication of threat conditions. In addition, liaisons with local, state and federal emergency entities, as well as NIPC an ES-ISAC, should be developed. Establish two methods for internal communication of threat conditions and test at least quarterly.

2.12. Document management

Create procedures for all of the processes being performed. This will give documentation for compliance needs, as well as allowing for the process to be performed in the event the normal person responsible cannot perform the task.

The NERC standards and guidelines call for documentation of many of the processes that relate to their requirements. Create a documentation management process to track all documentation, document updates, verification documents and review documents for all the items indicated in the findings section above and in accordance with the NERC standards and guidelines.

2.13 Information Classification

Create a process that helps to identify sensitive information. The information classification process should define information into various sensitivity levels. This process should define what process that new information must go through to be classified, as well as the destruction and reclassification procedures for information already classified.

2.14 Procedures, Standards and Guidelines

In addition to all of the procedures created for the Information Security Department, there needs to be standards and guidelines to guide the staff in performing their duties correctly. Standards provide given set of rules that must be followed when completing a task. Guidelines will give general direction in the form of a suggested way of completing a task.

The CSO should promote the other business units to create their own procedures, standards and guidelines in accordance to the guidance from the corporate policies.

3. Run security program as a holistic and managed program.

3.1. Maintain the current state of the Corporate Information Security Program

To maintain the current information security state, the processes in place have to be administered and maintained. The previous sections assisted in building Corporate Information Security program to protect assets in an efficient and cost effective way. The managers are in place and have the staff and processes at their control to administer and maintain the current state of information security.

3.2. Proactively manage Information Security

As threats and technology change over the course of time, it is a must to review processes for applicability and efficiency. In some cases, the processes will need to be changed or possibly replaced over time. The NERC standards and guidelines require a lot of documentation of processes, periodical review of the processes and documentation, documentation showing the processes have been verified and documentation of the review dates. This is accomplished by creating a holistic security program that not only manages current processes, but one that manages future trends and processes in a proactive manner.

In the previous sections we have indicated that a lot of processes that need to be in place to monitor and update as the environment or risks change. Information Security is a continuous reduction of risk. We have given you these recommendations to provide you with the holistic security program it takes to be successful. Being proactive is just as important to information security as is maintaining the current processes you have in place.

3.3. Monitor Compliance

For all requirements in the NERC 1200 standards, the responsible entity is required to demonstrate compliance via self-certification. Certification must be submitted to the assigned compliance monitor annually. The compliance monitor

assigned to your company may perform on site assessments every three years or upon complaint. You must keep these compliance records on hand for three years.

Upon request, you must make the required information for each standard available for inspection to the compliance monitor, in accordance to section four of each standard in the NERC 1200.

Attachments

The following links are to documents that would be attached to this final deliverable when presented to GIAC Enterprises.

NERC Security Guidelines for the Electricity Sector
http://www.esisac.com/publicdocs/Guides/SecurityGuidelinesElectricitySector-Version1.pdf

NERC Urgent Action Standard 1200 – Cyber Security
ftp://ftp.nerc.com/pub/sys/all_updl/standards/Urgent-Req-CyberStnd-3-3121.pdf

Threat Alert Levels and Physical Response Guidelines
http://www.esisac.com/publicdocs/tas_physical_V2.pdf

Threat Alert Levels and Cyber Response Guidelines
http://www.esisac.com/publicdocs/tas_cyber_V2.pdf

Additional Reading

Executive Management of Information Security
http://www.cgi.com/cgi/pdf/cgi_whpr_43_execmanageinfosecurity_e.pdf

Chief Security Officer Guideline
http://www.asisonline.org/guidelines/guidelineschief2003.pdf

The SANS Security Policy Project
http://www.sans.org/resources/policies/

NIST Computer Security Resource Center
http://csrc.nist.gov/index.html

* End of final deliverable *

Section B: See attached Powerpoint presentation of final deliverable.

Slide 1: Opening slide
This slide will be used for the presenter's introduction.

Slide 2: Agenda
This slide will be used to announce the agenda for this presentation.

Slide 3: Presentation Details
This slide will be used to discuss the flow of the presentation. The presenter will give an explanation of the handouts (final deliverable and attachments), protocol for questions, anticipated timeline flow of the presentation, and break information.

Slide 4: Project Details
This slide will give the presenter an opportunity to reiterate the scope of the project and the methodology used to complete the project.

Slide 5: Findings
This slide will be used to discuss the findings of the project. They will be discussed by NERC document used. First the guidelines will be covered followed by the standards.

Slide 6: Plan of Action
This slide will be used to present the plan of action. The plan of action will be presented by phase.

Slide 7: Questions
This slide will be the queue for the presentation and will promote questions from anyone who has a question.

Slide 8: Project Closure
This slide will be used to indicate it is time for the sponsor of the project to acknowledge completion of the project and bring closure by signing off on it.

Slide 9: Next Steps
This slide will be used to provide an opportunity to discuss what happens next.

Slide 10: Future Opportunities
This slide will be used to provoke a discussion of what services GTJD Consulting can offer to assist with implementation.

References

[1] Sandia National Laboratories, “Common Vulnerabilities in Critical Infrastructure Control Systems”, 11 Nov 2003, URL: http://www.ea.doe.gov/pdfs/vulnerabilities.pdf (26 Apr 2004)

[2] Department of Energy, “21 Steps to Improve Cyber Security of SCADA Networks“, URL: http://www.ea.doe.gov/pdfs/21stepsbooklet.pdf (26 Apr 2004)

[3,4] Project Management Institute, “A Guide to the Project Management Body of Knowledge (PMBOK) 2000 Edition”, 2000, URL: http://www.pmi.org/prod/groups/public/documents/info/pp_pmbokguide2000excerpts.pdf (12 May 2004)

[5] NERC SGES, “Security Guidelines for the Electricity Sector”, Version 1.0, 14 Jun 2002, URL: http://www.esisac.com/publicdocs/Guides/SecurityGuidelinesElectricitySector-Version1.pdf (27 Jul 2004)

[6] NERC 1200, “NERC Urgent Action Standard 1200 – Cyber Security”, 13 Aug 2003, URL: ftp://ftp.nerc.com/pub/sys/all_updl/standards/Urgent-Req-CyberStnd-3-3121.pdf (8 Jun 2004)

[7] SANS Institute, SANS Institute Track 13 Security Consultant 13.5, Pg. 3-3

[8] OCTAVE Method, “OCTAVE Information Security Risk Evaluation”, URL: http://www.cert.org/octave/ (12 Jul 2004)

[9] Tech Republic, “Success strategies for security awareness”, 6 May 2004, URL: http://techrepublic.com.com/5100-6300_11-5193710.html (13 Jul 2004)

[10] InternetNews, “Rise of the Chief Security Officer”, 25 Mar 2002, URL: http://www.internetnews.com/ent-news/article.php/7_997111 (13 Jul 2004)