Regional Cyber Security and Infrastructure Team

GRADUATE PROJECT

Submitted to the Faculty of
the Department of Computing Sciences
Texas A&M University-Corpus Christi
Corpus Christi, Texas

In Partial Fulfillment of the Requirements for the Degree of
Master of Science in Computer Science

By

Steve Alves
Summer 2011

Committee Members

Dr. John Fernandez
Committee Chairperson

Dr. Ajay Katangur
Committee Member

Dr. Linda Kiltz
Committee Member
ABSTRACT

When evaluating an entity’s computer infrastructure from either an effectiveness or security mitigation perspective, it is necessary to obtain a detailed understanding of the organization. Understanding the organization’s range of services and methods of providing these services is critical to evaluating the entity’s infrastructure and security posture. This project identifies related work on the components necessary to construct a cyber security and infrastructure team. The project outlines the components necessary to create a university managed cyber security and infrastructure team that can assist local nonprofit and governmental entities in addressing their IT infrastructure and security needs.
# TABLE OF CONTENTS

Abstract .................................................................................................................................1

Table of Contents ..................................................................................................................2

List of Tables .......................................................................................................................4

1. Introduction and Background .......................................................................................5
   1.1 Related Work ..............................................................................................................7

2. Regional Cyber Security and Infrastructure Team .........................................................9
   2.1 Requirements ............................................................................................................9

3. Project Design ................................................................................................................14
   3.1 Administrative .........................................................................................................14
   3.2 Legal .........................................................................................................................16
   3.3 Computer Environment Documentation ...............................................................17
   3.4 Assessment Guidelines .........................................................................................20
   3.5 Training ..................................................................................................................21
   3.6 Tools .......................................................................................................................24

4. Project Testing ...............................................................................................................26

5. Conclusion .....................................................................................................................29

6. Future Work ..................................................................................................................31

Bibliography and References ..............................................................................................32

Appendix A. System Development Controls .................................................................34

Appendix B. Application Change Management Controls ..............................................43

Appendix C. Computer Security Controls ..................................................................52
Appendix D. Computer Operations Controls.................................................................59
Appendix E. CSI PowerPoint Presentation.................................................................66
Appendix F. CSI Brochure ....................................................................................70
Appendix G. CSI Engagement Document.................................................................72
Appendix H. Bokencamp Confidentiality Agreement..............................................78
Appendix I. Student Nondisclosure Agreement ......................................................80
Appendix J. Computer Environment Documentation Form ......................................84
Appendix K. Windows Server Security....................................................................89
LIST OF TABLES

Table 3.1. HIPAA standards for administrative safeguards ..................................22

Table 3.2. PCI-DSS Requirement 7 - Restrict access to cardholder data ...............22
1. INTRODUCTION AND BACKGROUND

In order to perform a computer infrastructure or computer security mitigation assessment, it is necessary to obtain a detailed understanding of the organization. Initial steps involve interviews with key management personnel in an effort to identify present and future services to be provided by the organization. The nature of the services the entity provides and the methods of delivery largely influence the makeup of the organization’s computer infrastructure. This, in turn, directly affects the entity’s security posture.

Interviews of key IT personnel, along with the collection of process flow charts, network diagrams and system configuration details are adequate for an infrastructure assessment. To truly produce a useful computer security mitigation assessment of the organization, controls documentation and testing are necessary. This process is generally conducted with the help of various tools (i.e., Nessus, LANguard, Core Impact, etc) and techniques (interviews, observation, and review). Performing this process is necessary to both validate management assertions as well as identify items overlooked during the previous step. Upon completion of data gathering, findings are evaluated in conjunction with the organization’s request and are summarized in a report for management.

The results of an assessment is documented in two separate reports; one is provided to upper management and written in the form of an executive summary, while the second report represents a detailed outlining of the specific items required to address the team’s findings. The second report is delivered to lower IT management since it contains detailed system specifications and settings.
The rationale for this project is to provide benefits to both the university’s students and the local community. This project affords our students an opportunity to apply skills learned in the classroom to real world environments. It is also of assistance to small local governmental entities and nonprofit organizations that are unable to bear the financial burden of such an assessment from a commercial company.
1.1. Related Work

Recently, a number of universities have organized small teams of students to compete in various computer security and infrastructure activities [Ayoub 2005]. The goal is to test the students’ ability to function adequately in a simulated business environment where aspects of the environment are not functioning and are under attack from teams acting as hackers [Conklin 2005] [Hoffman 2005]. Students are not only required to manage their resources as is required in a real business environment, but are also expected to demonstrate an appropriate level of technical skills to maintain, fix and defend their environments. The nature of the skills often tested goes beyond those taught in the typical university computer science program. A typical computer science program emphasizes computer programming and theory, while these competitions test applied knowledge.

In recent years, there has been a change in direction to ensure that students have the skills necessary to function in a real environment. The U.S. Military has supported this change with both the introduction of new programs and labs for their students [Schepens 2004], as well as funding and offering organizational support for university and high school programs (i.e., Collegiate Cyber Defense Completion and the High School Cyber Patriot program).

With the nature of these programs requiring students to demonstrate applied skills, which are often emphasized in computer certifications, a debate has started in the academic world about the value of computer certifications and their purpose [Noble 1997]. CISCO networking and Microsoft operating system certifications not only require
mastering theory, but also the ability to apply concepts in a real world setting [Adelman 2000].

In light of the move to demonstrate applied skills and the industry’s emphasis on computer certifications, it makes sense to expose computer science students to real world computer infrastructure activities in addition to computer programming.
2. REGIONAL CYBER SECURITY AND INFRASTRUCTURE TEAM

The goal of this project is to design and implement a regional cyber security and infrastructure team at Texas A&M University-Corpus Christi, which will assist small local governmental entities and nonprofit organizations in dealing with computer infrastructure and security assessments.

2.1 Requirements

2.1.1 Initial Contact

The initial contact between the team and the outside organization will be conducted by the Computer Science Department Chair and/or Program Director. The purpose of the meeting will be to:

- Outline the extent of the service the University is prepared to perform for the organization.
- Obtain agreement on the extent of services the organization would like the University to perform.
- Identify client confidentiality needs.
- Obtain key contact information.

2.1.2 Business Process Identification

Initial steps will involve interviews with key management personnel in an effort to identify present and future services to be provided by the organization. Details are obtained through interviews of key IT personnel, process flow charts, network diagrams,
and system configuration. This process also involves identifying key applications and
documenting significant aspects of the applications. Moreover, the computer
environment (i.e., hardware, operating system, network configuration and IT function)
supporting the applications must be documented and tested for accuracy.

2.1.3 Controls Identification and Testing

Control Environment Assessment

Prior to performing an assessment of the client’s environment, an assessment of
the client’s computer related business process controls is required. If the client has more
than one location, consideration should be given to completing a separate assessment of
the controls at each environment. For each area of focus, significant features should be
noted based on information from prior work, inquiries of individuals inside and outside
the organization, and knowledge of external and internal factors affecting the entity.

Areas of focus for one control environment assessment may not be relevant to all
engagements or systems. Thus, judgment is necessary when determining the importance
of the area of focus. Additionally, it should be noted that the assessment environments
and areas of focus may not be all inclusive; thus, the individual performing the
assessment may need to improvise. During the controls assessment process, it is
important to determine if exceptions are identified and appropriate action taken.
**Monitoring Controls**

A review of monitoring controls requires documenting system development and implementation efforts, change management, computer security and computer operations. Documents to be used during client engagements contain detailed points beyond the following list and can be found in the appendixes noted below.

- System development controls (see Appendix A)
  - Is there a clear methodology?
  - Do projects have clearly identified management support?
  - Is there adequate status monitoring?

- Change management - Involves a wide range of controls related to changes being made to hardware and software. (see Appendix B)
  - Is there testing of changes prior to their introduction into production?
  - What is the frequency of changes?
  - Who has access to migrate a change into production?

- Computer security (see Appendix C)
  - Are there appropriate security policy and procedure documents?
  - Is there appropriate management support?
  - Do the policy and procedures documents address appropriate regulations, etc?

- Computer operations (see Appendix D)
  - What controls exist to address system availability and downtime?
  - Is there a disaster recovery plan and is it adequate?
What is the system backup process, etc?

2.1.4 Assessment

**Infrastructure Assessment**

Upon completion of the documentation of the client’s environment, it is necessary to perform an evaluation of the current environment in light of the client’s needs. System performance measurements are analyzed and compared to industry norms and customer expectations.

**Computer Security Mitigation Assessment**

Once the organization’s controls have been properly identified and documented, an assessment of their adequacy is performed. Methods utilized range from reviews of system configurations to exercising commercial assessment tools.

2.1.5 Documentation/Reporting

Several types of documentation/reports are necessary to properly perform this function. Team documentation involves documenting everything the team does from start to finish. Examples of these documents are contain in the appendix and will be explained in the project design section that follows. Documentation should be completed as each activity is performed by the team. Report wording must be carefully chosen as the inappropriate choice of words may result in an inappropriate conclusion.

While client deliverables drive the nature of the final reports, two basic documents are generally necessary. First is the need for an executive summary written in language management understands and focuses on the key points. The second document
is generally more technical in nature and very detailed to assist the site’s IT personnel with implementing recommendations.
3. PROJECT DESIGN

The implementation of a university managed Cyber Security and Infrastructure (CSI) team will require the development of various skills and the creation of a number of documents and processes. The project consists of administrative documents, university legal input, development of numerous control and assessment processes, identification of educational and training requirements, and the identification, testing, and evaluating of various assessment tools and techniques.

3.1 Administrative

The CSI team requires the support of various university individuals to provide activity oversight and support. Initial contact with local nonprofit and governmental entities is conducted by the Computer Science Department Chair and/or Program Director. A PowerPoint presentation describing the team structure and services was created for use during the initial contact (see Appendix E). A brochure was also created to promote the program (see Appendix F). This document describes both the team and the services available.

For each engagement, an initial planning meeting is required to identify details necessary to properly develop an engagement plan for the client. A document called the Cyber Security and Infrastructure Engagement document was created to ensure that appropriate information is captured during the engagement planning meeting (see Appendix G). It contains sections for key contact information, deliverables, impact identification, related entity identification, related assessment entity identification,
controls assessment and critical issues.

The first section of the document captures customer name and location information as well as key contact names, phone numbers, email addresses and location information. In addition, the CSI team members involved in the engagement are identified. The second section, “Services”, identifies engagement deliverables and due dates, and the CSI team members assigned to each task. The next section, “Engagement Impact Identification,” facilitates an appropriate engagement design by ensuring the following items are addressed during the planning meetings:

- Sensitive system and computer security issues.
- Significant business developments including industry, regulatory, economic, technology and legal issues.
- Changes in financial, organizational and business activities.
- Recent changes in standards affecting the entity and its systems.
- Significant business risk.

The next section, “Related Entities,” is used to identify all parties related to the entity that might have an impact on the engagement. The “Related Entities” section documents both internal and external auditors, and both internal and external security personnel. The “Controls Assessment” section is used to note control risks associated with system derived accounts and services. Some applications create system accounts at the operating system level and the database level in order to function properly. For example, Oracle Financials, when installed, creates system accounts at both the operating system and database levels. Identifying each application and its related accounts as well as the computer security processes the site has in place to manage these accounts is critical to
securing the environment. The “Critical Issues” section identifies the most important issues to be resolved during the engagement.

In addition to the above, the initial meeting is also used to collect any client required confidentiality documents. Instead of routing each document to the appropriate individuals in the Texas A&M Corpus Christi legal department for their review, it is expedient to have the legal department develop a generic document that will be acceptable to clients in general. A copy of the document that Bokencamp, local nonprofit, requested be signed by CSI participants is contained in Appendix H. This item will be discussed later in this document.

3.2 Legal

Various standard legal documents are necessary to address student nondisclosure requirements, student background investigations, customer engagement agreements, and University limited liability statements. Occasionally students will come in contact with sensitive and confidential information. A student nondisclosure agreement (see Appendix I) is necessary to ensure that the students are aware of the penalty for revealing or misusing the information. The background investigations are necessary to ensure that the students involved in the project meet appropriate standards which are acceptable to both the University and the client. In an effort to limit both the University’s liability as well as that of the students participating in the program, the legal department will be utilized to review agreements when deemed necessary by the Computer Science Department Chair.
3.3 Computer Environment Documentation

As previously stated, in order to properly perform a computer infrastructure or computer security mitigation assessment it is necessary to obtain a detailed understanding of the organization’s environment. Various standardized documents have been created to ensure proper documentation of the client’s computer environment as well as their monitoring, application, and computer controls. The completion of these documents will take place after the initial meetings. These documents are discussed below and shown in the Appendix.

3.3.1 Environment Documentation

A clear understanding of the client’s services provided and the computer environment supporting those services is necessary prior to any infrastructure assessment and/or security review. While process flow charts, network diagrams and system configuration details are often obtainable from the customer, a centralized document is necessary to ensure completeness of information collected. The “Computer Environment Documentation” form was created to ensure the appropriate and standardized collection of information related to the computer environment (see Appendix J). Information collected focuses on key applications, hardware and operating system software, network components, and IT functions. These documents were adopted from my experience at Coopers & Lybrand, Bristol Myers Squibb, SAIC, industry training, and practice over the past twenty years. Documentation of key applications includes a description of their purpose (significant functions, data and transactions), identification of application type
(i.e., in-house or package), module implementation date and patch status, application level security, programming language and user interface description. In addition to the above, identifying system administrators responsible for managing the application and their contact information is critical to facilitate the requirements of the engagement. Identifying system limitations and planned modifications help in revealing known problems and end user functionality needs. Documentation of hardware and operating system software should ensure the capture of hardware manufacturer name and model number, operating system version, communication software, and security. This information assists in the identification of possible computer security issues and/or system implementation limitations. The documentation should also reference an appropriate network diagram. Documentation of the IT function will include organization charts, individual names, titles, contact information, responsibilities, performance monitoring, and business strategy.

3.3.2 Monitoring, Application and Computer Controls

A comprehensive understanding of the client’s computer control environment is necessary prior to any security assessment analysis. Computer controls forms have been created to ensure the appropriate and standardized collection of information related to system development and implementation, application change management, computer security and operations.

System development controls form (see Appendix A) focuses on ensuring that systems development meets the needs of the user community and addresses security issues. The major categories of the system development addressed by the document
include, project management and monitoring, in-house software development and testing, commercial software selection and testing, release management and synchronization, operating system software upgrades, migration to production, and user and technical documentation and training.

While the system development controls form is focused on the development and implementation of new systems, the application change management form (see Appendix B) focuses on the introduction of changes to existing production system. The major categories of this document include software change request process, software version control, testing of software changes, release management and synchronization, transferring of changes into production, programming standards, and user and technical documentation and training.

Computer security document (see Appendix C) is intended to both identify controls and to provide a roll up of detail findings from sub documents utilized for operating system, database, and application specific documents. The major components of the document include security management, operating system level security, database level security, application level security, system utilities, physical access controls, and contract programmers and consultants.

In addition to the controls identified above, more detailed documents have been built where needed, for example see Appendix K for the Microsoft Windows security steps document. This document is intended to assist the student with their security review of a Windows server. Due to the length of the steps only the first section of the documents is included in the appendix. The findings from this document are then summarized under the first bullet of the operating system section of the computer security
document (see Appendix c).

Security assessment guidelines are vast in order to address operating system, database and application level security for the wide range of systems in existence. While some testing techniques have been identified for standard systems, such as Microsoft Windows, other systems will require creativity on the part to the team.

In addition to the above computer controls forms, a computer operations document (see Appendix D) has been created to document and assess system availability and downtime, disaster recovery, system backup, etc. The major sections of the document include documentation of controls concerning operator responsibilities, backup and recovery, batch job processing, media storage library, operational failures recovery, disaster recovery, user support, service bureaus, fire prevention and control, and equipment maintenance and protection.

3.4 Assessment Guidelines

Infrastructure assessment requires the use of a development and implementation document, as well as a change management document to ensure the appropriate level of information is collected to facilitate a proper assessment. As previously stated, the CSI team documentation identifies necessary steps to determine if appropriate control exists such as clear methodology, clearly identified management support, adequate status monitoring, version control, testing, package selection process, release management and synchronization, data conversion, and user documentation and training. The change management document is utilized to capture a wide range of controls related to changes being made to hardware and software. Software change request process, version control,
testing of changes prior to their introduction into production, user documentation and training, and who has access to migrate a change into production are each critical to performing an adequate assessment.

3.5 Training

In order to properly address client needs, certain skill levels have been identified. Some of the major areas will include industry and government controls standards, vulnerability assessment techniques, computer certifications, and applied technologies. There are a number of industry and government standards (i.e., HIPAA, PCI-DSS, SOX, etc.) that entities may need to follow when implementing a new system and securing existing systems. Since these documents are not part of the traditional computer science program, their inclusion in the recently approved Cyber Security and Infrastructure computer science degree option makes the CSI team project viable. The introduction of HIPAA and PCI-DSS documents in CSI curriculum has proven to be viable. Table 1 shows an example of the HIPAA standards for administrative safeguards, while Table 2 shows an example of the PCI-DSS standard concerning restricting access to cardholder data.
Table 3.1: HIPAA standards for administrative safeguards [HIPAA 2011]

<table>
<thead>
<tr>
<th>HIPAA Security Rule</th>
<th>HIPAA Security Rule Standards</th>
<th>Implementation Specifications</th>
<th>NIST SP 800-53 Security Controls</th>
<th>NIST Publication Crosswalk</th>
</tr>
</thead>
<tbody>
<tr>
<td>164.03(a)(1)(6)</td>
<td>Security Management Process: Implement policies and procedures to prevent, detect, contain, and correct security violations.</td>
<td>Administrative Safeguards</td>
<td>RA-1</td>
<td>FIPS 199; NIST SP 800-37; NIST SP 800-18; NIST SP 800-30; NIST SP 800-16; NIST SP 800-53</td>
</tr>
<tr>
<td>164.03(a)(1)(6)(B)</td>
<td>Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following:</td>
<td></td>
<td>RA-2, RA-3, RA-4</td>
<td></td>
</tr>
<tr>
<td>164.03(a)(1)(6)(C)</td>
<td>Sanction Policy: Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity.</td>
<td></td>
<td>RA-2, RA-3, RA-4, PL-6</td>
<td></td>
</tr>
<tr>
<td>164.03(a)(1)(6)(D)</td>
<td>Information System Activity Review: Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.</td>
<td></td>
<td>PS-8</td>
<td></td>
</tr>
<tr>
<td>164.03(a)(2)</td>
<td>Assigned Security Responsibility: Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity.</td>
<td></td>
<td>AU-6, AU-7, CA-7, IR-5, IR-6, SI-4</td>
<td></td>
</tr>
</tbody>
</table>

Table 3.2: PCI-DSS Requirement 7 - Restrict access to cardholder data [PCI 2011]

<table>
<thead>
<tr>
<th>PCI DSS Requirements</th>
<th>Testing Procedures</th>
<th>Steps Performed</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following:</td>
<td>7.1 Obtain and examine written policy for data control, and verify that the policy incorporates the following:</td>
<td></td>
</tr>
<tr>
<td>7.1.1 Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities</td>
<td>7.1.1 Confirm that access rights for privileged used IDs are restricted to least privileges necessary to perform job responsibilities.</td>
<td></td>
</tr>
<tr>
<td>7.1.2 Assignment of privileges is based on individual personnel’s job classification and function</td>
<td>7.1.2 Confirm that privileges are assigned to individuals based on job classification and function (also called “role-based access control” or RBAC).</td>
<td></td>
</tr>
<tr>
<td>7.1.3 Requirement for an</td>
<td>7.1.3 Confirm that an</td>
<td></td>
</tr>
</tbody>
</table>
Vulnerability assessment techniques for various operating systems, databases, and business applications/services represent a vast area. Due to the vastness of this area only a few of the techniques have been included as part of this project. In order to ensure that a proper vulnerability assessment is conducted during a client engagement, a level of training for each of the assessment techniques highlighted has been identified to make certain that team members have an appropriate level of skill.

Computer certifications are a means to indicate that a certain level of knowledge has been achieved in a given area. As a pre-employment requirement, information technology (IT) positions often require one or more certifications. Additionally, existing employees are often required to complete certain certifications prior to being promoted. For example, the City of Corpus Christi requires a CISCO CCENT certification for an entry level network engineering position and a CISCO CCNA for a mid-level position. It would be helpful for team members to obtain certain certifications in an effort to demonstrate a certain level of expertise in a given IT area. As a part of this project Microsoft’s Certified IT Professional (MCITP) [Microsoft 2011], Cisco’s CCNA [Cisco 2011], CompTIA’s Security+ [CompTIA 2011], and ISC2’s CISSP [ISC2 2011] have been identified as being beneficial certifications.

Since the CSI team will be expected to work in the field with the entity’s IT
personnel, it is anticipated that the IT personnel will expect a level of practical knowledge on the part of team members. The extent of skills obtained from the University’s computer science program, Cyber Defense Team and certifications is expected to be sufficient.

Upon hiring a graduate student from a university, a consulting company will generally expect the individual to work full time on various aspects of several customer engagements over the course of three years, prior to assigning them the In-Charge duties for a small engagement. These customer engagements are not only small but also represent repeat jobs that a firm may have with clients. A new In-Charge is not assigned a new customer engagement until they have been assigned the In-Charge task on several existing clients. After working as an In-Charge for a few years, an individual might be promoted to Manager of a small job. Over the next few years, the employee can expect to be assigned larger and more complex engagements. The consulting scenario above presents challenges for a university implemented program because students cannot be expected to work more than 10 to 20 hours per week. For this reason, their development will progress at a much slower pace. Thus, engagement management will represent a challenge and it is expected that students will need to be exposed to engagements very early in the computer science program.

3.6 Tools

A wide range of computer hardware and software is necessary to support this project. An analysis of various types of software necessary to support the project has been performed. Due to budget limitations, various free software packages have been
identified for use by the team. For penetration testing, Backtrack will be utilized until funding can be arranged to purchase a commercial product. With regards to vulnerability analysis, Nessus will be utilized. Each of these products are known to have potential side effects so their use will be limited. Printed copies of the forms created will be utilized by the students until funding can be secured to provide them with laptops for working at the customer’s site. Additional Cyber Defense Team desktops and servers would be necessary to both support the work being done for customers and CSI team training to ensure client confidentiality.

For documenting client environments as well as viewing client provided documents, Microsoft Office will be utilized. Identifying appropriate business applications and system assessment software has been challenging. Identifying dominant business applications (i.e., QuickBooks, Peachtree, Oracle Financial, etc.) and the key functionality that team members must master in order to perform computer infrastructure or computer security mitigation assessment will be ongoing.
4. PROJECT TESTING

Project testing consisted of discussing the concept with a local nonprofit organization, a local medical clinic, classroom testing, and the evaluations of various tools and techniques.

Testing of the project with a local nonprofit organization consisted of presenting the concept to the organization and determining if an interest and/or need exist. The organization’s feedback was positive. Several projects were identified as items of interest by both parties. This initial meeting was utilized to test the concepts via a PowerPoint presentation, brochure and CSI Engagement document. Feedback on the usefulness of the PowerPoint presentation and the brochure were discussed. The response was positive and deemed useful in helping the organization gain a better understanding the team’s purpose and capabilities. The CSI engagement document was also utilized to gather preliminary client information. The documents usefulness as a data collection source proved to be true.

In addition to the nonprofit organization the concept was also presented to the principle of a local medical clinic with similar results. Based on the experience with the nonprofit improvements were made to the PowerPoint presentation and the brochure. These new documents were utilized in the discussion with the medical clinic and once again proved useful in helping the clinic’s management understand the projects concept. The CSI engagement document, unchanged from the nonprofit’s meeting, was utilized to gather preliminary client information. Once again the document proved useful as the engagement’s data collection source.
During last Fall and this Spring several of the concepts discussed in this document were tested in and out of the classroom. The introduction of controls regulations such as HIPAA, PCI-DSS, baseline recommendations from the Center for Internet Security, and CompTIA’s Security+ certification topics proved useful. It was noted that these additions helped clarify real world security concepts and techniques being taught in the classroom. The controls regulations and baselines assisted in illuminating why certain security configurations were necessary. Moreover, they were useful in providing students needed guidance when dealing with systems and/or security settings with which they were unfamiliar. In addition to the above, it was noted though a review of security job postings that hiring managers frequently indicate that computer certifications are valued. It is common to see Microsoft, Cisco, Security+ and CISSP being requested or even required.

Testing of tools and techniques proved valuable. This process helped in identifying the limitation of various tools such as Backtrack, and Nessus, and highlighted the need for good security techniques. Lab testing of Nessus identified that it was good for vulnerability testing, but not for penetration testing. It was clear from last year’s Panoply competition that penetration testing tools such as Backtrack also have limitations. This was further proven in the lab with the testing of Backtrack against patched Linux servers. If the system is properly patched, the use of exploits available in Backtrack has limited value. Thus, concluding that a system is secure based on it passing a Backtrack penetration test is misleading. Lab testing also noted that good manual security testing techniques can identify poor system configurations which can represent
major security problems. It is safe to conclude that various tools and techniques are necessary to truly understand an environment’s security posture.


5. CONCLUSION

Over the past few years we have assembled hardware from various campus sources. The hardware has been made available to the students to enable them to explore an assortment of hardware and software configurations. Unlike some labs, which limit student modifications, this lab encourages the students to disassemble and reassemble the equipment as needed in an effort to expand their knowledge. We have made use of software alliances such as Microsoft and VMware, in an effort to expose our students to software products which will mitigate their learning curve upon entering industry. In addition, we have made several Linux operating systems, Cisco networking and database products available.

As a way to both encourage and expedite the learning process, numerous training labs have been built to allow students to explore a range of operating systems and networking components in a methodical manner. In a very detailed way, each lab walks the student through each exercise step by step. The labs are designed to build on each other and allow the students to move at their own pace. With regards to Microsoft server products, labs have been built for Windows server 2003, 2008 and Server Core. On the Linux side, labs have been built for Fedora, Ubuntu, Debian, FreeBSD, and CentOS. Depending on the type of Linux, labs have been create that will start with the install and configuration process and work their way through various server services such as DHCP, DNS, NFS, Samba, email, etc.

Arrangements have been made for guest speakers from local businesses in an effort to help local industry become acquainted with what our students are learning as
well as expose our students to industry expectations. The organization works to assist students in obtaining IT employment both on and off campus. As a means for improving employment prospects industry certifications are encouraged. During summer months free Cisco CCENT and CompTIA Security+ training has been made available to students.

Going forward additional Window, Linux, Cisco and database labs need to be created to expand the depth of student knowledge. As new labs introduce students to new server services, additional security labs will also become necessary. Certification training beyond those already available to our students should be added. In addition to the above, continuous improvements to the forms included in this document will be necessary. Identifying future engagements which will allow our students to apply the skill they learn in this program are necessary to make this effort successful.

The local nonprofit utilized to test this project was receptive to the program provided the students are appropriately supervised, suitable legal documents are in place, and proper processes have been vetted. Subsequent to the meeting, the program’s introductory PowerPoint presentation, brochure, and engagement documents have been refined and will continue to be revised. Since the construction of the computer environment documents are under the control of the team it is expected that with continued lab testing and customer interaction, they will continue to be refined. Software identification is expected to progress at an adequate pace, however training will be time consuming and challenging.
6. FUTURE WORK

There are several areas where additional work can be pursued. Further work is needed to identify methods to integrate engagement implementation methodology into the classroom process. Doing so will reduce the amount of time it takes for students to achieve a level of engagement independence. Identifying the synergies between program content and industry certifications and standards (i.e., HIPAA, PCI-DSS, SOX, etc.) to more readily enable students to complete key certifications and standards understanding should improve industry acceptance. Finally, creating a mechanism for spotting industry trends to ensure the program stays current.
BIBLIOGRAPHY AND REFERENCES


APPENDIX A – SYSTEM DEVELOPMENT CONTROLS
SYSTEM DEVELOPMENT CONTROLS

1. Project Management/Monitoring
   a. Is project management appropriately skilled?

   b. Is a system design methodology used to ensure that all necessary steps are included in the project plan?

   c. What ensures that appropriate managers and users are involved in project management?

   d. Are there reporting procedures in place to ensure effective monitoring of progress toward successful completion of the project?
      i. Is there an update tracking facility with priority information?
         ii. Is performance benchmarking being used?

   e. What project metrics are being used (i.e., application complexity, number of lines of code, number of programs, number of development days, etc.)?

   f. Are development metrics being used (i.e., performance targets, transaction rates, response times, volume level system can tolerate, network load, CPU and data storage utilization, etc.)?

   g. Are error conditions and abnormal scenarios being anticipated?
2. **Software Development**
   
a. Are suitable managers, users, and IT personnel involved in the development and implementation?

b. What ensures that the design incorporates the appropriate application level controls?

c. What ensures that the source code, used to create the program, corresponds to the current version?

d. Is version control and synchronization exercised over application modules, shell scripts, configuration files, database objects, stored procedures, table definitions, scheduling information?

e. How are modifications to a program, by more than one programmer, coordinated (e.g., through the use of a software librarian or manual procedures)?
   i. Source code locked out until released.
   ii. Source code associated with a change is required to be returned before changes can be promoted to production.

f. Are controls in place to ensure that change requests are appropriately approved?

g. What ensures appropriate coordination of changes when application development spans different development teams?

h. How is the conversion of old transaction data, master data, and the population of new fields controlled?
3. **Software Testing**

*Testing Process*

a. Is there an appropriate level of unit and system wide testing by users and IT personnel to ensure errors are detected and the system will function as planned?

b. Is an appropriate level of regression testing performed to changes made following initial testing?

c. Is there involvement of an independent approval group?

d. What ensures the appropriate testing of converted data by users and IT staff?

*Quality Assurance*

a. Is there evidence of testing, test scripts and/or test plans, evidence of pass/fail status of test cases, evidence of bug discovery and resolution, evidence of user involvement?

b. What ensures user verification of the effectiveness of programmed controls; such as, completeness, accuracy, authorization, validity, error handling, and exception identification?

*Security*

a. Is there proper segregation between development, test and production?

b. What ensures that developers are restricted from access to production data and applications?

c. What would prevent or detect unauthorized modifications being made to a software change after the completion of testing but before transfer into production?
4. Commercial Off The Shelf software (COTS) Acquisition
   a. What ensures that appropriate business and application controls are defined?

   b. Are appropriate senior management, users, and IT personnel involved in the package selection?

   c. Does the package selection process include well-known and widely used products?

   d. How is the conversion of old transaction data, master data, and the population of new fields controlled?

5. COTS’ Testing
   **Testing Process**
   a. Is there an appropriate level of unit and system wide testing by users and IT personnel to ensure errors are detected and the system will function as planned?

   b. Is an appropriate level of regression testing performed to changes made following initial testing?

   c. Is there involvement of an independent approval group?

   d. What ensures the appropriate testing of converted data by users and IT staff?

   **Quality Assurance**
   a. Is there evidence of testing, test scripts and/or test plans, evidence of pass/fail status of test cases, evidence of bug discovery and resolution, evidence of user involvement?

   b. What ensures user verification of the effectiveness of programmed controls; such as, completeness, accuracy, authorization, validity, error handling, and exception identification?
Security
a. Is there proper segregation between development, test and production?

b. What ensures that developers are restricted from access to production data and applications?

c. What would prevent or detect unauthorized modifications being made to a software change after the completion of testing but before transfer into production?

6. Release Management and Synchronization
   Packaging
   a. Is software packaging in use?

   b. What ensures the grouping of components for distribution?
      i. What ensures effective code management (tool, method, technique, etc.)?

   c. What ensures the ability to back out a distribution, if necessary?
      i. Are changes “Packaged” to facilitate easy backouts?

Software Production
a. What ensures that all versions of production software and documentation are understood and recorded?

b. What ensures that all source code is available for each software version?

Documentation Tracking
a. Is documentation for internally developed products maintained and current?

b. Is documentation of third-party products maintained and current?
Synchronization

a. What ensures that all production executables on each workstation/server, are in sync?
   i. How is phased implementation controlled?

b. What ensures that all production workstation and server versions are compatible?

c. What ensures that system software configuration files are in sync as well as other third-party products?

7. System Software Upgrades

Upgrades to existing system software (i.e., operating system, scheduling package, networking, etc.) should not undermine existing system software controls.

a. Are appropriate senior management, users, and IT personnel involved in the system software selection?

b. What ensures the appropriate testing of system software upgrades by users and IT staff prior to being moved into production?

c. In the event of a production problem what ensures that system software changes can be backed out of the production?

8. Migration to Production

a. What ensures that only appropriately tested and approved programs are transferred into production?

b. What ensures that the correct directories are updated with the program change?

c. If software distribution is to occur electronically, what software tool is to be used?
d. What procedures are in place to ensure physical shipping and subsequent loading of programs?

9. User and Technical Documentation and Training

User Documentation

a. Are software reference manuals distributed to affected users and IT staff?
   i. Distribution of release notes to users and/or developers?

b. Does documentation reflect contingency procedures, reconciliation procedures, use of screens, reports, etc.?

c. Are user manuals available for vendor supplied products?

Technical Documentation

a. Is technical documentation (i.e., software comment lines, software librarian) updated to reflect software development?

b. Are comment lines in the code?
   i. Do they contain change history?

c. Does documentation include, field names, field types (numeric, alpha), field length, examples of field values, integrity constraints (i.e., range of acceptable values), etc.?

d. Are operations manuals updated to reflect program functions?

e. Are technical and configuration information manuals available for vendor products?

f. Are high level data flow diagrams showing inputs and outputs to the system maintained?
g. Are process diagrams showing major processing, including location of processing server, maintained?
   i. Due they highlight the flow of key transactions?
   ii. Due they highlight work breakdown, structure, hierarchy as well as detail the make-up of the system?
   iii. Due they highlight application dependencies such as feeder files that need to be received before processing can continue?

h. Will user documentation be available at implementation?

**Training**

a. Are users and IT staff appropriately trained?

b. Is there adequate cross-training of staff?

c. Are training classes available?
APPENDIX B – APPLICATION CHANGE MANAGEMENT
APPLICATION CHANGE MANAGEMENT

1 Software Change Requests
Requests for changes to computer software should be appropriately considered and processed.

- What ensures that user needs are incorporated into a software change request?

- What ensures that software change requests are properly evaluated, authorized, prioritized, and monitored?

- What ensures that approved software change requests are implemented on a timely basis?

- Modifications to operational systems should be appropriately approved.

2 Software Version Control

- What ensures that the source code, used to create the change, corresponds to the current version of the program (e.g., through the use of a software librarian or manual procedures)?

- What ensures appropriate coordination of changes when application development spans different development teams?
3 Testing of Software Changes
Software changes should be tested to ensure that they achieve the end-users’ requirements without negatively impacting existing processes.

Testing Process
- Are changes to in-house software and vendor supplied packages subject to appropriate testing by IT and users to ensure that they will function as intended in production?

- How does management ensures that the level of testing is increased when the level of risk associated with the software change increases?

Quality Assurance
- Is there involvement of an independent approval group (Quality Assurance Group)?

- Is there evidence of testing, test scripts and/or test plans, evidence of pass/fail status of test cases, evidence of bug discovery and resolution, evidence of user involvement?

- What ensures user verification of the effectiveness of programmed controls; such as, completeness, accuracy, authorization, validity, error handling and exception identification.
Security

- Is there proper segregation between development, test and production?

- What ensures that developers are restricted from access to production data and applications?

- Operational files should not be used for testing without appropriate approval. Copies of the files should be made for testing purposes. Confidentiality of sensitive data must be maintained during testing procedures.

- What would prevent or detect unauthorized modifications being made to a software change after the completion of testing but before transfer into production?
4 Release Management and Synchronization

Packaging
- Is software packaging in use?
- What ensures the grouping of components for distribution?
- What ensures the ability to back out a distribution, if necessary?

Synchronization
- What ensures that all production executables on each workstation/server, are in sync?
- What ensures that all production workstation and server versions are compatible?
- What ensures that system software configuration files are in sync as well as other third-party products?
5 Transfers into the Production Environment
The transfer of changes/programs into production should be appropriately controlled.

- What ensures that only appropriately tested and approved changes are transferred into production?

- What ensures that the correct directories are updated with the program change?

- For vendor supplied programs, how are changes transferred into the live environment?

- If software distribution is to occur electronically, what software tool is to be used?

- What procedures are in place to ensure physical shipping and subsequent loading of programs?
6 Programming Standards

- Are written programming standards and procedures for monitoring compliance established?

- Are written processing standards (e.g., naming conventions, storage media, etc.) and procedures for monitoring compliance established?

- Does each operational application have a list of program completion codes and operator actions; if such codes and recovery are "common," a master list will suffice?

- Are appropriate procedures (e.g., label checking and record counts) used to ensure that data files are complete, accurate, and authorized?

- Do edit listings or terminal messages clearly indicate the reason(s) why a transaction record was rejected?

- Does transaction documentation clearly indicate the effect of transaction processing on affected files? Computer-generated transactions should be clearly identified.

- Any transaction, whether accepted or rejected, user-entered or computer-generated, should be traceable back to its source and forward to a control total. If transactions are summarized or the detail is not printed when they are processed, then appropriate detail files should be retained so the transaction history is available.
7 User and Technical Documentation and Training

General
- Are there written procedures defining requirements for promoting changes to production? Documentation supporting all changes should be approved and retained.
- Is all related documentation updated before any change is made operational?

User Documentation
- Are software reference manuals appropriately updated and distributed to affected users and IT staff?
- Is documentation updated to reflect contingency procedures, reconciliation procedures, use of screens, reports, etc.?
- Are user manuals available for vendor supplied products?

Technical Documentation
- Are comment lines in the code?
  - Notes should be included in each source module which describe the function of the module, major subroutines and any coding which might not be readily understood.
  - Do they contain change history?
- Does documentation include, field names, field types (numeric, alpha), field length, examples of field values, integrity constraints (i.e., range of acceptable values), etc.?
- Are operations manuals updated to reflect program changes?
- Are technical and configuration information manuals available for vendor products?
- Are high level data flow diagrams showing inputs and outputs to the system maintained?
- Are process diagrams showing major processing, including location of processing server, maintained?
- Due they highlight the flow of key transactions?
- Due they highlight work breakdown, structure, hierarchy as well as detail the make-up of the system?
- Due they highlight application dependencies such as feeder files that need to be received before processing can continue?

**Training**

- Are users and IT staff appropriately trained?
- Is there adequate cross-training of staff?
- Are training classes available?
APPENDIX C – COMPUTER SECURITY CONTROLS
COMPUTER SECURITY CONTROLS

1 Security Management
Access control policies, which are based on the level of risk associated with financially significant applications and data, should be implemented by management. Management should ensure the maintenance of detailed logs for critical and sensitive transactions and applications.

   a. Do written security policy and procedures exist?

   b. Has security administration been clearly defined?

   c. Have data owners been clearly identified and documented?

   d. Are sensitive transactions appropriately logged and reviewed?

   e. Are unsuccessful login attempts logged and reviewed on a frequent basis?

   f. Is a user stamp of activity (i.e., time & date) logged?
2 Operating System Level Access
System level access should be appropriately restricted.

a. What ensures that access to the operating system is appropriately limited (i.e., Linux, Windows, etc.)?
   i. What prevents users from escaping from their application and obtaining a command line?

b. How is access to system directories and files restricted?
   i. Is access to development, test and production environments, commensurate with employee job responsibilities?

c. How is access restricted to key programs (startup and shut down scripts, job scheduling, etc.)?

d. Is appropriate security monitoring procedures in place?

e. How is remote access restricted and network transmissions protected?

f. When employees transfer or terminate what ensures that their access is changed accordingly.
   i. Are quarterly access reviews performed to ensure access is commensurate with job responsibilities?
3 **Database Level Access**

Database level access should be appropriately restricted.

a. How is access restricted to the database?

b. How is access to system directories and files restricted?
   i. Is access to development, test and production environments, commensurate with employee job responsibilities?

c. How is access restricted to key programs (startup and shut down scripts, job scheduling, etc.)?

d. Is appropriate security monitoring procedures in place?

e. How is remote access restricted and network transmissions protected?

f. When employees transfer or terminate what ensures that their access is changed accordingly.
   i. Are quarterly access reviews performed to ensure access is commensurate with job responsibilities?
4 Application Level Access
Access to a particular and functions within the applications (i.e., the issuance of credit memo’s) should be appropriately restricted to ensure segregation of duties.

a. How is access to a particular application restricted (i.e., application login security)?

b. How is access to particular functions within an applications restricted (i.e., application function security)?

c. What ensures the effectiveness of application level password controls (i.e., unique user-IDs and password disciplines)?

d. Is access to development, test and production environments commensurate with employee job responsibilities?

e. Is appropriate security monitoring procedures in place?

f. How is remote access restricted and network transmissions protected?

g. When employees transfer or terminate what ensures that their access is changed accordingly.
   i. Are quarterly access reviews performed to ensure access is commensurate with job responsibilities?
5 System Utilities
The use of system utilities, such as powerful passwords and utilities should be limited.

a. How is access to system utilities limited and monitored?

b. Are employees with access to system utilities restricted from accessing company assets?

6 Physical Access
Physical access to the data center should be appropriately controlled.

a. How is access to the data center and backup tapes controlled?

b. Ensure that routine access is limited to computer operators, media librarians, control clerks, vendor maintenance personnel and supervisory personnel.
   i. User personnel should be granted routine access only after written approval of the IT Director.

c. Ensure that a log is maintained for recording non-routine access and is reviewed and approved periodically by the IT Director.

d. Ensure that locks and combinations on doors and storage units are changed periodically.

e. How is the distribution of sensitive reports (i.e., payroll) controlled?
7 Contract Programmers and Consultants

a. There should be a written contract approved by the IT Director and the appropriate legal counsel for all services provided by contract programmers and consultants.

b. The contract should contain clauses relating to the proprietary and confidential nature of corporate and division systems and to the access to and use of data processing resources, with provisions for indemnification in the event of breach, where feasible.

c. Procedures should be employed to limit contract programmers and consultants' exposure to documentation and other resources not required to accomplish their assigned tasks.
1 Server Managers Responsibilities

- Do server managers have the appropriate skills?

- What ensures that server managers have the appropriate written supporting documentation to carry out their duties?
  - Procedures should include system startup and shutdown, routine operations, system recovery, emergency responses and security.

- Restart and recovery instructions should be developed for all critical systems and tested at least annually.

- Sensitive processes (e.g., A/P and payroll checks) run under data center control should not be run on an unsupervised shift.

- What ensures that the server manager activities comply with their job responsibility?

- What ensures that problems are quickly identified and resolved (i.e., performance metrics)?
2 **Backup and Recovery**
For emergencies and historical searches up-to-date backups of programs and data should be available. In addition, tested recovery procedures are necessary to ensure that the critical applications can be recovered in the event of a disruption.

- Do backup procedures include operating systems, applications and data.
- Does the site utilize off-site locations for backup storage?
- Are recovery procedures routinely tested to ensure that they will work when required?
- Are backup and recovery procedures appropriately documented?
- Are backup and recovery failures appropriately documented?

3 **Batch Job Processing**
Batch processes should be appropriately documented and scheduled.

- What guarantees batch processes are appropriately scheduled?
- What ensures appropriate approval of changes to batch processes?
- Are batch cycles reviewed to ensure successful completion?
  - Significant deviations between job scheduled times and processed times should be logged and reviewed by appropriate management.
- Reruns should be logged and reviewed by an appropriate manager.
- What guarantees that the information needed for each batch process is present prior to the process starting?
- Do operations manuals appropriately documented each batch process?
  - Are operations manuals updated to reflect changes to the batch process?
4 Media Storage Library

- Storage media (tapes, disks, optical media) should be stored in a locked area.

- Magnetic media can be adversely affected by paper dust. Thus, printers should not be located where tapes or disks are located.

- The library should have a sufficient fire protection system.

- Eating, drinking and combustible cleaning materials should not be allowed in the library.

- Access to the library should be appropriately controlled.

- Are there appropriately written policies and procedures governing the removal of media from the datacenter?

- Does the site perform a semi-annually inventory of the media?

- Media should contain appropriate labeling to ensure proper identification.

- Does the media disposal process ensure the erasure of data prior to disposal?
5 Operational Failures Recovery

- Are suitable measures in place to escalate and appropriately resolve operational failures?

- Are suitable managers, users, and IT personnel involved in operational failure resolution?

- Are operational failures appropriately documented?
  - A report should be prepared when processing is interrupted, identifying the cause and action taken.
  - Copies should be routed to appropriate management for review and approval to ensure that problems are identified, analyzed and addressed in a judicious manner.

- What guarantees that the cause of an operational failure is identified?
6  **Disaster Recovery**  
Management should ensure that the critical business processes can be recovered in the event of a disaster.

- Does a formalized plan exist?
- Have exposures been defined (threat analysis)?
- Have disaster prevention capabilities been assessed in light of known threats?
- Is there an off-site storage for data and programs?
- Does the system recovery plan incorporate systems, networks, communications and end users?
- Have off-site processing capabilities been arranged?
- Is periodic disaster recovery training performed?
- Are periodic drills performed?

7  **User Support**

- Is there a central support site (i.e., Help Desk)?
- Is there end user computer support for LAN, printers, third party software, and hardware repairs?
- Are incidents logged and reviewed by management?  
  - Are problems analyzed to determine appropriate corrective action?
- Are adequate procedure manuals available?
8  **Service Bureaus**

- There should be a written contract approved by appropriate management for all services provided by third parties.

- Does the contract contain data security protections and appropriate indemnification provisions.

- Contracts should permit audits of the service bureau procedures.

- Where appropriate does the service bureau have an appropriate disaster recovery plan?

9  **Fire Prevention and Control**

- Is there adequate fire prevention equipment
  - Is it appropriately maintained?
  - Smoke detectors should be installed in the ceiling where feasible.
  - Does the facility contain adequate fire extinguishers?

- Is semi-annual fire prevention and control training conducted?
  - Are instructions for emergency shut-down appropriately posted?

- The datacenter should be neat, clean and free of eating and drinking.

- Flammable cleaning materials should be avoided.
APPENDIX G – CSI ENGAGEMENT DOCUMENT
Cyber Security and Infrastructure Engagement Document

Year: _____________

| Client Name: |  |
| Primary Location: |  |
| Secondary Location: |  |

<p>| Key Contacts |  |  |  |  |</p>
<table>
<thead>
<tr>
<th>Name</th>
<th>Phone</th>
<th>Email</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| CSI Team |  |
| Department Chair |  |
| Director |  |
| Manager |  |
| Team Lead |  |
## Services

<table>
<thead>
<tr>
<th>Deliverables</th>
<th>Description</th>
<th>Due Dates</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

## Members

<table>
<thead>
<tr>
<th>Name</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Engagement Impact Identification

1. Sensitive system and computer security issues.

2. Significant business developments including industry, regulatory, economic, technology, and legal issues.

3. Changes in financial, organizational, and business activities.

4. Recent changes in standards affecting the entity and its systems.

5. Significant business risk.
## Related Entities
(Auditors, Security Personnel, etc.)

<table>
<thead>
<tr>
<th>Entity’s Name:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Parties:</td>
<td></td>
</tr>
<tr>
<td>Description:</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Entity’s Name:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Parties:</td>
<td></td>
</tr>
<tr>
<td>Description:</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Entity’s Name:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Parties:</td>
<td></td>
</tr>
<tr>
<td>Description:</td>
<td></td>
</tr>
</tbody>
</table>
### Controls Assessment

<table>
<thead>
<tr>
<th></th>
<th>Application</th>
<th>System Accounts (GL, AR, AP, ETC)</th>
<th>Risk Assessment</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Critical Issues

<p>| | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Confidentiality Documents (attach copies)

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
APPENDIX H – BOKENCAMP CONFIDENTIALITY AGREEMENT
LUTHERAN SOCIAL SERVICES OF THE SOUTH, INC.
CONFIDENTIALITY AGREEMENT

Employees, volunteers and/or subcontractors who work in or with programs and facilities operated by Lutheran Social Services of the South, Inc. (LSSS) need and will have access to personal information about clients/residents/families. Federal and state laws require that LSSS carefully guard all private information. By signing this agreement, you agree to abide by the following conditions and requirements:

I will only use private information about clients/residents/families as needed to fulfill my assigned job or service. I agree to access and use only the minimum amount of information necessary. I will not seek access to information I do not need.

I will not disclose this information to others, especially those outside the agency. I will not discuss private information unless it is required to conduct my job task. I will not gossip about or inappropriately discuss client/resident/family information.

I will not sell any client/resident/family information.

I will not remove client/resident/family information in any form from a facility without prior supervisory approval.

I understand that failure to meet the above standards may constitute grounds for discharge or cancellation of subcontract.

I have received a signed copy of this agreement.

__________________________________________
Employee/Volunteer/Sub-contractor                     Date

__________________________________________
Program or Location

__________________________________________
LSSS Staff Witness
APPENDIX I – STUDENT NONDISCLOSURE AGREEMENT
This Confidentiality Agreement (this "Agreement") is made effective as of July 05, 2011, between Texas A & M Corpus Christi, of Ocean Drive, Corpus Christi, Texas 78412, and Student, of TBD, Corpus Christi, Texas 78413.

In this Agreement, the party who owns the Confidential Information will be referred to as "TAMUCC", and the party to whom the Confidential Information will be disclosed will be referred to as "_________________________".

TAMUCC is engaged in Education. _________________________ is engaged in Student. Customer Information. TAMUCC has requested that _________________________ will protect the confidential material and information which may be disclosed between TAMUCC and _________________________.

Therefore, the parties agree as follows:

I. CONFIDENTIAL INFORMATION. The term "Confidential Information" means any information or material which is proprietary to TAMUCC, whether or not owned or developed by TAMUCC, which is not generally known other than by TAMUCC, and which _________________________ may obtain through any direct or indirect contact with TAMUCC.

A. Confidential Information includes without limitation:
   - business records and plans
   - financial statements
   - customer lists and records
   - trade secrets
   - technical information
   - product design information
   - computer programs and listings
   - source code and/or object code
   - copyrights and other intellectual property
   and other proprietary information.
II. PROTECTION OF CONFIDENTIAL INFORMATION.

_________________________ understands and acknowledges that the Confidential Information has been developed or obtained by TAMUCC by the investment of significant time, effort and expense, and that the Confidential Information is a valuable, special and unique asset of TAMUCC which provides TAMUCC with a significant competitive advantage, and needs to be protected from improper disclosure. In consideration for the disclosure of the Confidential Information,_________________________ agrees to hold in confidence and to not disclose the Confidential Information to any person or entity without the prior written consent of TAMUCC. In addition,_________________________ agrees that:

i. No Copying/Modifying. ______________________ will not copy or modify any Confidential Information without the prior written consent of TAMUCC.

ii. Unauthorized Disclosure of Information. If it appears that ______________________ has disclosed (or has threatened to disclose) Confidential Information in violation of this Agreement, TAMUCC shall be entitled to an injunction to restrain ______________________ from disclosing, in whole or in part, the Confidential Information. TAMUCC shall not be prohibited by this provision from pursuing other remedies, including a claim for losses and damages.

III. RETURN OF CONFIDENTIAL INFORMATION. Upon the written request of TAMUCC, ______________________ shall return to TAMUCC all written materials containing the Confidential Information. ______________________ shall also deliver to TAMUCC written statements signed by ______________________ certifying that all materials have been returned within five (5) days of receipt of the request.

IV. NO WARRANTY.

_________________________ acknowledges and agrees that the Confidential Information is provided on an AS IS basis. TAMUCC MAKES NO WARRANTIES, EXPRESS OR IMPLIED, WITH RESPECT TO THE CONFIDENTIAL INFORMATION AND HEREBY EXPRESSLY DISCLAIMS ANY AND ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT SHALL TAMUCC BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL, OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH OR ARISING OUT OF THE PERFORMANCE OR USE OF ANY PORTION OF THE CONFIDENTIAL INFORMATION. TAMUCC does not represent or warrant that any product or business plans disclosed to ______________________ will be marketed or carried out as disclosed, or at all. Any actions taken by ______________________ in response to the disclosure of the Confidential Information shall be solely at the risk of ______________________.
V. LIMITED LICENSE TO USE.  _________________________ shall not acquire any intellectual property rights under this Agreement except the limited right to use set out above.  _________________________ acknowledges that, as between TAMUCC and _________________________, the Confidential Information and all related copyrights and other intellectual property rights, are (and at all times will be) the property of TAMUCC, even if suggestions, comments, and/or ideas made by _________________________ are incorporated into the Confidential Information or related materials during the period of this Agreement.

VI. GENERAL PROVISIONS.  This Agreement sets forth the entire understanding of the parties regarding confidentiality.  Any amendments must be in writing and signed by both parties.  This Agreement shall be construed under the laws of the State of Texas.  This Agreement shall not be assignable by either party, and neither party may delegate its duties under this Agreement, without the prior written consent of the other party.  The confidentiality provisions of this Agreement shall remain in full force and effect after the effective date of this Agreement.

Information Owner:
Texas A & M Corpus Christi

By:  __________________________________________
Texas A & M Corpus Christi

Recipient:
Student

By:  __________________________________________
Student
APPENDIX J – COMPUTER ENVIRONMENT DOCUMENTATION
# Computer Environment Documentation

Year: ____________

<table>
<thead>
<tr>
<th>Client Name:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary Location:</td>
<td></td>
</tr>
<tr>
<td>Current Location:</td>
<td></td>
</tr>
</tbody>
</table>

**Organization Charts Obtained?**

<table>
<thead>
<tr>
<th>Key Applications</th>
<th>Application Name</th>
<th>Supporting Hardware</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Application

<table>
<thead>
<tr>
<th>Application Name:</th>
<th>Circle one: COTS or In-house</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Application Purpose (Significant functions, data, transactions)

### Application Information

**Vendor Name:**

<table>
<thead>
<tr>
<th>Module Name</th>
<th>Description</th>
<th>Imp Date</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Briefly describe any application level security:

Programming Language:

User Interface Description:

### System Administrators Contacts Information

<table>
<thead>
<tr>
<th>Name and Title</th>
<th>Phone</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## System Development

<table>
<thead>
<tr>
<th>System Limitations:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Planned Modifications:</td>
</tr>
</tbody>
</table>

## Hardware

<table>
<thead>
<tr>
<th>Vendor/Model</th>
<th>Operating system/Version</th>
<th>System Administrator</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Briefly describe performance monitoring methods:

<table>
<thead>
<tr>
<th>Application/Operating system security</th>
</tr>
</thead>
</table>

Briefly describe application level security

Briefly describe operating system security
High level Network/Communication Diagram
## WINDOWS SERVER SECURITY

### User Identification & Password Controls

<table>
<thead>
<tr>
<th>A</th>
<th>Legal Notice</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Is there a notice in place that is a warning to possible intruders?</td>
</tr>
<tr>
<td></td>
<td>a. Make sure the initial message does not provide any information such as the company name, operating system version, etc.</td>
</tr>
</tbody>
</table>

### Account Policies

<table>
<thead>
<tr>
<th>B</th>
<th>Account Policies</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Maximum password age</td>
</tr>
<tr>
<td>2</td>
<td>Minimum password age</td>
</tr>
<tr>
<td>3</td>
<td>Minimum password length</td>
</tr>
<tr>
<td>4</td>
<td>Are unique passwords required?</td>
</tr>
<tr>
<td>5</td>
<td>Is the intruder attempt (failed login attempts) value greater than specified?</td>
</tr>
<tr>
<td></td>
<td>a. Is the lockout time to low?</td>
</tr>
<tr>
<td></td>
<td>b. Users locked by intruder detection.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>c.</td>
<td>Evaluate procedures for enabling an account after a user has been locked out via the INTRUDER DETECTION facility.</td>
</tr>
<tr>
<td>d.</td>
<td>Review and test the documented <strong>procedures</strong> for assigning a new password when an authorized user forgets his or her password.</td>
</tr>
<tr>
<td>6</td>
<td>Are time restrictions in use at this site (forcibly disconnect when logon hours expire).</td>
</tr>
<tr>
<td>a.</td>
<td>Is there a forcible disconnect when logon hours expire.</td>
</tr>
<tr>
<td>b.</td>
<td>Identify temp and contractors without time restrictions.</td>
</tr>
<tr>
<td>7</td>
<td>Must logon to change password.</td>
</tr>
<tr>
<td>a.</td>
<td>Identify users not allowed to change their password.</td>
</tr>
<tr>
<td>8</td>
<td>Users accounts with no expiration date.</td>
</tr>
<tr>
<td>9</td>
<td>Is user information complete?</td>
</tr>
<tr>
<td>10</td>
<td>Are users restricted to their workstation?</td>
</tr>
</tbody>
</table>

**User Setup**

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>C1</td>
<td>Ensure that the steps followed to grant a user account agrees to those indicated in the Security Policies and Procedures document.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>1</td>
<td>a. Determine the procedures followed in the event emergency access privileges are required.</td>
</tr>
<tr>
<td></td>
<td>2 Determine if each user is assigned a unique User Account across the entire network, and that these ID’s are not shared.</td>
</tr>
<tr>
<td></td>
<td>3 Verify that policies and procedures require the use of passwords.</td>
</tr>
<tr>
<td></td>
<td>a. Check for missing passwords.</td>
</tr>
<tr>
<td></td>
<td>4 Verify that the policies require passwords that are not easy to guess.</td>
</tr>
<tr>
<td></td>
<td>a. Check for easily guessed passwords.</td>
</tr>
<tr>
<td></td>
<td>b. Ensure that passwords are not set equal to the user ID.</td>
</tr>
<tr>
<td></td>
<td>5 Determine if each user has a home directory?</td>
</tr>
<tr>
<td></td>
<td>a. Ensure that only the user has full rights to their home directory.</td>
</tr>
<tr>
<td></td>
<td>6 Determine if all users have a login script.</td>
</tr>
<tr>
<td></td>
<td>a. Evaluate those users who should have a login script but do not.</td>
</tr>
<tr>
<td></td>
<td>b. Ensure that the login script exists on the system.</td>
</tr>
<tr>
<td></td>
<td>c. Ensure that each start-up script has the correct permissions.</td>
</tr>
<tr>
<td></td>
<td><strong>d.</strong> Identify users who can exit to their own login script.</td>
</tr>
<tr>
<td>----</td>
<td>------------------------------------------------------------</td>
</tr>
<tr>
<td>7</td>
<td><strong>Obtain a list of all Mandatory (.MAN) Profiles and their properties.</strong></td>
</tr>
<tr>
<td>8</td>
<td><strong>Select specific users who have been terminated or changed functions. Determine that their User Accounts have been deleted or changed when they were terminated or transferred.</strong></td>
</tr>
<tr>
<td></td>
<td><strong>a.</strong> Check user ID's against the list of authorized users and application logon IDs.</td>
</tr>
<tr>
<td></td>
<td><strong>b.</strong> Evaluate the list of inactive users. Dormant accounts should be deactivated.</td>
</tr>
<tr>
<td>9</td>
<td><strong>Trace a sample of users to authorization evidence.</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th><strong>NT Specific</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><strong>Determine if the last user ID is hidden.</strong></td>
</tr>
<tr>
<td>2</td>
<td><strong>Determine if the shutdown from the logon dialog box is enabled.</strong></td>
</tr>
<tr>
<td>3</td>
<td><strong>Determine if Run is disabled in the file menu.</strong></td>
</tr>
<tr>
<td>4</td>
<td><strong>Determine if Save Settings Now and Save Settings on Exit are disabled.</strong></td>
</tr>
</tbody>
</table>
5. Determine whether there is automatic logon of a User Account implemented in the Registry via a system boot up demonstration.

   a. Evaluate the appropriateness of automatic logon.
   
   b. Evaluate the Properties of a sample of the User Accounts

---

6. **Advanced User Rights Policy**

   Obtain a list of the users with direct (non group) Advanced Rights assignment and evaluate for appropriateness.

---

<table>
<thead>
<tr>
<th>E</th>
<th><strong>Built-in Accounts – Administrator</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Determine if the Administrator account has been renamed.</td>
</tr>
<tr>
<td>2</td>
<td>The Administrator password should be unique on each host.</td>
</tr>
<tr>
<td>3</td>
<td>The Administrator password should be changed every 15 – 30 days.</td>
</tr>
<tr>
<td>4</td>
<td>The Administrator password should be kept in a sealed envelope and stored in a locked box.</td>
</tr>
</tbody>
</table>

   a. Evaluate password assignment for the Administrator account.
5. Determine whether or not each administrator also has a separate user name, without administrative rights, for other non-administrative functions.

<table>
<thead>
<tr>
<th>Built-in Accounts – Guest</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Verify that the Guest account has been disabled on sensitive systems by logging onto each server’s Guest account with a blank password.</td>
</tr>
<tr>
<td>2. Evaluate password assignment for the Guest account.</td>
</tr>
<tr>
<td>3. Determine if the guest account has been renamed.</td>
</tr>
<tr>
<td>4. Determine if the guest account is a member of unauthorized groups.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>F</th>
<th>Groups</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Evaluate the standards and practices for the creation and use of Local and Global groups.</td>
<td></td>
</tr>
<tr>
<td>2. Verify that management authorization and documentation is present for groups.</td>
<td></td>
</tr>
<tr>
<td>3. Evaluate the procedures for adding and removing group members.</td>
<td></td>
</tr>
<tr>
<td>4. Group membership associated with dormant/deactivated uses should be removed.</td>
<td></td>
</tr>
<tr>
<td>5. Review site’s policies for separation of incompatible functions.</td>
<td></td>
</tr>
</tbody>
</table>

| Local Groups |
6 **Groups – Administrator**

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>a.</td>
<td>Determine whether the Administrator account has been appropriately assigned.</td>
</tr>
<tr>
<td>b.</td>
<td>Select a sample of the users and confirm their membership has been appropriately authorized.</td>
</tr>
<tr>
<td>c.</td>
<td>Determine whether or not each member also has a separate user name, without administrative rights, for other non-administrative functions.</td>
</tr>
</tbody>
</table>

7 **Groups – Server Operators**

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>a.</td>
<td>Evaluate the appropriateness of user rights assigned to this group.</td>
</tr>
<tr>
<td>b.</td>
<td>Determine whether the group has been appropriately assigned.</td>
</tr>
<tr>
<td>c.</td>
<td>Select a sample of the users and confirm their membership has been appropriately authorized.</td>
</tr>
<tr>
<td>d.</td>
<td>Determine whether or not each member also has a separate user name, without advanced user rights, for other non-administrative functions.</td>
</tr>
</tbody>
</table>

8 **Groups – Account Operators**

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Groups – Backup Operators</td>
</tr>
<tr>
<td>---</td>
<td>--------------------------</td>
</tr>
<tr>
<td></td>
<td><strong>a.</strong> Evaluate the appropriateness of user rights assigned to this group.</td>
</tr>
<tr>
<td></td>
<td><strong>b.</strong> Determine whether the group has been appropriately assigned.</td>
</tr>
<tr>
<td></td>
<td><strong>c.</strong> Select a sample of the users and confirm their membership has been appropriately authorized.</td>
</tr>
<tr>
<td></td>
<td><strong>9</strong> Groups – Backup Operators</td>
</tr>
<tr>
<td></td>
<td>a. Evaluate the appropriateness of user rights assigned to this group.</td>
</tr>
<tr>
<td></td>
<td>b. Evaluate the appropriateness of each user’s membership.</td>
</tr>
<tr>
<td></td>
<td>c. Select a sample of the users and confirm their membership has been appropriately authorized.</td>
</tr>
<tr>
<td></td>
<td><strong>10</strong> Groups – Users</td>
</tr>
<tr>
<td></td>
<td>a. End-users should be grouped according to job functions.</td>
</tr>
<tr>
<td></td>
<td>b. For groups with advanced rights evaluate the appropriateness of each user’s membership.</td>
</tr>
<tr>
<td></td>
<td>c. Select a sample of the users and confirm their membership has been appropriately authorized.</td>
</tr>
<tr>
<td></td>
<td><strong>11</strong> Groups – Everyone</td>
</tr>
</tbody>
</table>

d. Verify that the Everyone group has been eliminated on sensitive systems.