

**Professional Services Proposal**

*Proposal to serve:*

Greater Buffalo Saving Bank

*Information Security Assessment and Network Penetration Review*

March 19, 2007

March 19, 2007



**Control Solutions International**

400 Amherst Street

Nashua, NH 03063

Phone: (603) 598-0700  
Fax: (603) 598-8345

Jphn Doe

Greater Buffalo Saving Bank

2421 Main Street

Buffalo, New York 14214

Dear Mr Doe:

Control Solutions International (“Control Solutions”) is pleased to have the opportunity to submit this proposal to provide Greater Buffalo Saving Bank (“GBSB”) assistance with its internal audit needs – specifically, to conduct a security assessment that will allow GBSB to:

* Conduct an assessment of the IT systems that have a presence on the GBSB network.
* Identify potential security weaknesses in the organization’s network servers and connectivity.

In this document you will find information about Control Solutions, our dedicated and trusted engagement team, our quality approach to internal audit consulting and our commitment to build a long-term partnership with GBSB. We are excited about the prospect of developing a long-term relationship with your organization as it is our goal to exceed your expectations.

To ensure the success of your engagement, we are committed to a philosophy of collaboration and joint accountability – a true partnership. First and foremost we are business partners, then internal auditors. Control Solutions delivers a unique combination of thought leadership, technical knowledge and practical experience. We are committed to our philosophy of tailoring our approach and methodology to meet your unique requirements.

I am confident that our consultants can easily work with you and your team in an efficient, cost-effective and professional manner. We will achieve our delivery by offering expert consultation on complex topics, using senior-level professionals, providing regular communication and implementing proven methods designed to help you achieve your objectives.

We look forward to serving you in your internal audit initiatives. Thank you once again for making this opportunity available to Control Solutions.

Very truly yours,

**Control Solutions International**

Robert Carucci

Partner

**Contents**

Section 1: Overview of Control Solutions 4

Section 2: Our Experience 6

Section 3: Executive Summary 7

Section 4: Scope Approach, & Methodology 8

Section 5: Project Management Approach 18

Section 6: Deliverables 19

Section 7: Technical Tools and Utilities 23

Section 8: Detailed and Itemized Pricing 25

Section 9: Terms and Conditions 28

Appendices

1 – Overview of Control Solutions

**A. Overview**

Control Solutions has been a leading co-sourced and out-sourced Information Technology internal audit provider since 1991. To date, we have helped over 400 public companies comply with the requirements of the Sarbanes-Oxley Act. Additionally, we currently support over 200 Internal Audit organizations. Our firm specializes in Information Technology risk management, Network Vulnerability Analysis and Penetration Studies, Security Policies and Standards, applications process reviews along with operational and financial controls. Our Information Technology professionals have a minimum of eight years working experience and most hold higher professional certifications (CISA, CISSP, and CISM).

We offer clients the knowledge, experience and methodology of a global services firm as well as the dedicated service and customized approach of a boutique firm. As the first firm solely dedicated to providing internal audit services, we continue to set the benchmark for internal audit partnering and Section 404 readiness.

**B. Our Relationships, Clients and Services**

We adopt a very flexible approach in the way we work with our clients. The key to our success is our customized working arrangements that meet individual needs. We provide all of our clients with high-impact business process, financial and operational, control, compliance and information technology review services. Our internal audit practice is divided between assurance services and consulting services which include:

**IT Internal Audit and Security Services**

|  |  |
| --- | --- |
| * Technical Assessments * IT Enterprise Risk & Compliance * Threat Vulnerability Analysis * Policy & Program Reviews | * ERP Implementation Reviews * Healthcheck Assessment Services * Continuous Control Monitoring |

Control Solutions is currently providing Internal Audit and IT Risk Assessment consultancy services to the following leading organizations, among others:

|  |  |  |  |
| --- | --- | --- | --- |
| *Alcan*  *Anthem BCBS*  *Artesyn Technologies*  *Avid Technologies*  *Bank of Hawaii*  *Becton Dickinson*  *Benihana Restaurants*  *Bon-Ton Stores*  *Bristol Myers Squibb*  *California Savings Bank*  *Clean Harbors*  *Charles River Associates*  *Computer Associates*  *Cytec Industries*  *Dover Technologies*  *Dow Chemical*  *EDO Corporation*  *Finlay Enterprises*  *Ford Motor Company* | *Forrester Research*  *Fresenius Medical Care*  *GATX Corporation*  *Gerber Scientific*  *Gemplus International*  *Genzyme*  *Guardian Life*  *Guidant*  *Gymboree*  *Harley Davidson*  *Harvard University*  *Hartmarx Corporation*  *Imperial Chemical Industries*  *IDX Systems Corporation*  *Home Properties of New York*  *Imagistics International*  *Interpublic Group*  *Intrawest Corporation*  *John Hancock* | *Journal Register Company*  *Keane*  ***L 3 Communications***  *Legal & General*  *Linens ‘n Things*  *Maine Yankee Power*  *Marsh & McLennan*  *MasterCard*  *Midas, Inc.*  *NEC Electronics*  *Newpark Resources*  *Northrop Grumman*  *OSI Pharmaceutical*  *Pegasystems*  *Pepsi Bottling Group*  *Pitney Bowes*  *Phase Forward*  *Placer Dome*  *Polaroid Corporation* | *Progress Rail Services*  *Qualcomm*  *Radian*  *Rayovac*  *Reebok International*  *Sonus Networks*  *SPSS Inc.*  *Standard Parking*  *Stolt-Nielsen Transportation*  *Sycamore Networks*  *Stanford University*  *Steinway Musical Instruments*  *The Princeton Review*  *Timberland*  *Todhunter International*  *Walgreen Company*  *Watts Water Technologies*  *World Bank*  *XL Global Services* |

2 – Our Experience

Controls Solutions’ Security Consultants have over 15 years in the information security field. Our consultants have been published in leading security publications and have been lead Instructors at leading security conferences and seminars (i.e. - SANS Institute and Learning Tree). These courses include – Identity Theft, Wireless, Network Security and Intrusion Detection.

We have been involved in a range of engagements; some recent Information Technology projects that relate to your current Network Security audit requirements include:

* Major Financial Services Firm – IT Security Risk Assessment to identify vulnerabilities within client’s existing network and application infrastructure;
* Major Health Care Insurance Carriers – external security penetration testing, as well as internal network and host vulnerability assessments with a review of physical and logical access controls;
* IT Operations and Processes – application development, program change control, disaster recovery plans, and operations center management. IT Infrastructure and Risk Assessments – Focusing on security and capability to support business transactions, social engineering reviews and IT attack & penetration testing;
* Major Health Care Insurance Carrier - Audit of the StrategicInformation Technology Plan (and the processes involved with creating the plan);
* Sarbanes-Oxley 404 compliance – Managed the entire Information Technology SOX process including the identification, remediation and testing of key IT controls; and
* Social Engineering – Social Engineering Penetration test to gain access both logically and physically to the organizations network and premises.

3 – Executive Summary

Greater Buffalo Savings Bank is a locally operated community savings bank, founded in 1999. GBSB currently operates 14 full-service banking offices in Western New York. GBSB is interested in conducting a security assessment that will allow it to:

* Provide an assessment of the IT systems that have a presence on the GBSB network.
* Identify potential security weaknesses in the organizations network servers and connectivity.

These activities are part of GBSB’songoing risk management program and are focused on identifying the risk GBSB is currently exposed to so that an appropriate set of responses to those threats can be developed. GBSB is seeking to identify and select an outside independent organization to perform the activities listed above. Control Solutions understands that the scope of this project will be the GBSB networks which are located at the bank’s headquarters which houses all the major networking components. This includes both the internal and external networks as well as several points of internet presence such as firewall, email servers, etc.

In response to GBSM risk assessment, the organization has chosen to conduct a Network Security Assessment (internal and external) to determine its exposure to network vulnerabilities and threats from the Internet. In performing a Network Security Assessment we complete four key activities; **first** is the identification of your critical IT assets; **second** is the analysis of your network vulnerabilities, **third** is performing the penetration tests; and **finally**, we will report on our findings. The goal of first two activities is to create a comprehensive understanding of your network infrastructure which includes the servers and connectivity. This knowledge will assist us in testing your security controls exploitation of identified vulnerabilities within GBSB network.

The IT consultants that we employ have more than 15 years experience in IT Security and Networking. Several of our consultants are instructors (with SANS, MIS Training Institute and Learning Tree) and have published articles on security and auditing and will be more willing to insure a knowledge transfer of their skills and expertise to GBSB Internal Audit Staff. Our consultants will work with your personnel to accomplish your objectives and to develop a presentation and set of deliverables that explains our results in not only technical terms but also in a way that the non-technical executive can easily understand. The following explains, in detail, our approach and methodology to serving GBSB.

4 – Scope Approach & Methodology

**Scope**

Control Solutions understands that the scope of this project will be the GBSB internal and external networks which are located at the bank’s headquarters (HQ). We understand that HQ houses all the major networking components. Control Solutions recommends that the following components and processes be included in our audit scope:

* Identification of possible risk areas in internal and external network infrastructure and assess the effectiveness of their controls to manage these risks;
* Identification of all components and associate risks in the DMZ, LAN and wireless network infrastructure and assess the effectiveness of their controls to manage these risks; and
* Use of mutually agreed upon scanning tools to assess network vulnerabilities.

**Approach and Methodology**

Our approach consists of the following operational phases:

* Phase I – Identification of Critical Information Technology Assets
* Phase II – Internal and External Network Vulnerability Analysis
* Phase III – Internal and External Network Penetration

**Network Security Assessment and Penetration – Audit Approach: Figure I**



Phases I and II are designed to create a comprehensive, detailed understanding of your organization’s external-facing networks. Within Phase II there are several tasks which include – Wireless Reviews, Firewalls, Host Based Analysis

Phase III will be designed to exploit the vulnerabilities identified in the earlier phases.

Control Solutions will identify all vulnerabilities and focus on the areas where a compromise would have the greatest impact, and thus the highest risk, to GBSB. We also understand industry-related policies and regulations that drive the need for security. *Our analysis will be non-disruptive to GBSB, with minimal or no impact on staff productivity.*

**Phase I – Identify Critical Information Assets**

In Phase I Controls Solutions will develop an inventory of GBSB’s critical information assets. These assets could include physical and logical assets such as data center application systems, employee computers, network communications devices and channels, remote work areas such as employee’s home computers, customer data, employee data, and intellectual property.

This inventory will be used as a basis for performing the internal and external Network Vulnerabilities Analysis in Phase II. In gathering and developing an inventory of critical information assets, Control Solutions consultants will perform the following steps / tasks:

* Identify key business processes and associated applications systems;
* Interview key business owners to obtain their perspective of the criticality of identified business processes;
* Identify physical IT assets and their locations;
* Identify network and logical connectivity; and
* Correlation of the physical IT assets to key business processes.

Critical information assets are then ranked based on their value. On a scale of 1 to 4, asset value will be ranked as follows:

1. ***Catastrophic*** – catastrophic failure is possible if the asset is destroyed / compromised;
2. ***Critical*** – the asset is considered “mission critical” to business operations;
3. ***Marginal*** – the asset marginally affects business operations; some degradation of service is likely if the asset is destroyed **/** compromised; and
4. ***Negligib****le* – destruction / compromise of the asset will have a negligible effect on business operations.

The assets identified and ranked as categories 1-3 are used as the basis for the next step – Phase II – Identify Network Vulnerabilities.

**Phase II – Identify Internal and External Network Vulnerabilities**

Control Solutions will perform an internal and external network vulnerability assessment in Phase II. We have included several tasks within this phase to identify the various network vulnerabilities .The tasks are enumerated below:

**A. Footprint Analysis and Information Gathering**

In this task we will create a detailed blueprint of GBSB Internal and External network and its associated Internet security profile. This allows us to achieve a thorough mapping and overcome any blind spots you might have. We will gather domain names, IP network ranges, and information about hosts, such as operating systems and application systems.

The Footprint Analysis/Information Gathering includes the following steps:

* Network Enumeration
* DNS Interrogation
* Topology Identification and Mapping
* Host Identification
* Service Scan
* Information Retrieval
* Wireless Access Point Identification

***Network Enumeration*** *–* Control Solutions uses structured methodologies, public tools, and our proprietary toolset to identify domain names, networks, and IP address ranges associated with your company. Techniques include querying InterNIC and American Registry for Internet Numbers databases.

***DNS Interrogation*** – Control Solutions queries your Domain Name Services (DNS) for all available information about your company’s network presence. We search for all host records via zone transfers of your company’s DNS servers and look for any domain name records that might provide enticement information or represent misconfigurations.

***Topology Identification and Mapping*** – Control Solutions systematically determines access paths into your company’s infrastructure by trace routing networks and selected hosts.

***Host Identification*** – Our security professionals use tools such as strobe, scanline, and NMAP to thoroughly map your company’s Intranet presence. Control Solutions tools use TCP pings in addition to the ICMP pings found in typical host identification tools.

***Service Scan*** – After identifying live systems connected to the Internet, Control Solutions performs an assortment of service scans. Scan types rely primarily on normal TCP and UDP packets and use source-porting techniques. We adapt the scanning method to satisfy time windows and the amount of stealth required for the test. These scans discover which TCP and UDP service ports are present and listening – a critical step to determining the operating systems and application systems present on the network.

***Information Retrieval*** – Once we establish which listening ports are available to the Internet, we extract as much information as possible from the target systems. This includes the operating system, as determined via our proprietary operating system detection utilities. We also enumerate banners or other information specific to a listening port, such as protocol versions for SSH and OpenSSL.

***Wireless Access Point Identification***– will involve the monitoring of airwaves around CTC facilities to look for authorized and unauthorized wireless access points (AP’s). We will be looking for SSID (Service Set Identifiers) which is the WLAN’s name. We will use wireless tools such as NetStumber and Kismet, which can discover SSID’s and other detailed information about wireless access points. NOTE AS PER YOUR REQUEST WE ADDED THE WIRELESS AS AN OPITIONAL ITEM. PLEASE SEE ITEM F FOR DETAILS.

**B. Verification of Footprint Analysis and Network Design Review**

The results of previous tasks are reviewed with the appropriate GBSB Network and System administrators to verify our findings and analyses. This verification ensures that we have properly identified all critical internet facing components, such as firewalls, web, and email servers which make up the network perimeter. We will compare our results with your internal/external network diagrams and known hosts.

Once the footprint Analysis has been performed a high level design review will be performed. This will included an analysis of the various networking components and the placement of the DMZ zones. In addition we will examine the various security policies and standards that have need implemented to support the network.

**C. Network Vulnerability Scan**

We will meticulously scan GBSB internal and external network perimeter for known vulnerabilities with commercial and proprietary tools. Our tools use focused scans based on available services and operating system type, rather than blind, broadcast sweeps for vulnerabilities. In addition, our assessment of the network perimeter will focus on the following areas network infrastructure components:

* Web Servers
* External DNS Servers
* External Email Servers
* Perimeter Firewalls
* VPN Access Points
* Networks Devices - (Routers/Switches)

We will use open source tools that are widely available on the Internet as well as third party commercial and proprietary tools.

**D. Firewall Diagnostic Review**

As part of our Review Controls Solutions proposes to review GBSB’s firewall systems (which include external routers) by executing the following steps:

* Develop background information about the GBSB s Firewalls and routers in use. This includes obtaining documentation such as firewall/router configurations, network diagrams and specific firewall security policies which are implemented by GBSB systems administrators. Review the expectations/goals/strategies of the firewall have been identified.
* Firewall Designed Review – We will review the design of the firewall systems to ensure that design meets the identified expectations/goals/strategies.
* Firewall Logical access – Review of logical access to the various components (routers, firewall software) are restricted to the appropriate individual. This includes reviewing password management, access approvals and logical connections to the firewall components.
* Firewall System Configurations – During this activity a detailed examination of the GBSB firewall configuration will be conducted. Ingress and egress rules will be examined to ensure that only traffic which is required for business reasons traverses the firewall. Recommended configuration changes will be provided to the client.
* Review and Test the Rule Base Design - Review the rules set design and determine that the firewall lockdown rule sets have been properly implemented.
* Firewall logging – We will review that firewall logging is enabled and reviewed and followed up by management personnel.
* Firewall Testing – We will port scan the firewall from both the internal network and external internet, scanning for ICMP, UDP and TCP. There should be no open ports and the firewall should not be able to reply to ping requests.
* Firewall Traversal Testing – This activity involves identifying any perimeter security devices such as routers and firewalls and mapping their access control lists (ACLs). This involves such techniques as “firewalking” or attempting to connect to known IP addresses and port numbers beyond the firewall.

**E. Host Based Assessment**

As part of this review Controls solutions will perform a host bases Assessment of the IT Systems that are on the outside of the firewall on the DMZ and have a presence on the GBSB internal network. This assessment will examine the security setting and security lockdowns that may have been performed on the servers. Items that we will examine as part of this host based Assessment include:

* Networking Services;
* Patch Level;
* Operating System Security Setting;
* User Access Controls to include Password Setting; and
* Use of industry Hardening Standards (i.e. – Center for Internet Security)

**F. Wireless Assessment - Optional**

Controls Solutions will perform a wireless (adhoc) assessment of GBSB Headquarters by executing the following two step approach:

The information gathering process focuses on identifying the key wireless access points and their associated business units. The information gathering phase consists of the following:

* Interviews with business managers and technical staff, and review of documentation relating to wireless information security and information technology assets (including network topology);
* Reconnaissance – will involve the monitoring of airwaves around GBSB facilities to look for authorized and unauthorized wireless access points (AP’s). We will be looking for SSID (Service Set Identifiers) which is the WLAN’s name. We will use wireless tools such as NetStumber and Kismet, which can discover SSID’s and other detailed information about wireless access points; and
* Review of the Electronic Environment – A detailed review of the environment that was identified in the previous step. This will include an analysis of access points identified.

One the key area’s that we will be looking for at GBSB is rogue networks, which are unauthorized access points (AP) and wireless clients attached to GBSB network.

Wireless threats cannot impact assets unless the assets are vulnerable to those threats. Mitigating controls may be in place, reducing the likelihood of a threat exploiting a given access point or wireless vulnerability. The following wirelesses vulnerabilities will be examined as part of our assessment:

* Integration of wireless access points into the overall network architecture
* The use of traditional firewalls to segregate wireless network segments
* Use of encryption for sensitive data
* War-X Defense
  + - MAC Address authentication with regulated DHCP registration
    - Authenticated AP (Bluesocket)
    - WEP Keys
* Wi-Fi Protected Access
* SSID Problems and Issues

**Phase III – Penetration or Exploitation of Internal and External Network Vulnerabilities**

**Background**

Once Control Solutions has identified network/system vulnerabilities in Phase II, we will attempt to exploit the vulnerabilities.

*If we find a high number of major vulnerabilities or network weaknesses, we will meet with you before proceeding, to determine if GBSB can address the weaknesses identified. Once these weaknesses have been corrected, then we would proceed with the Penetration test.*

Our consultants will attempt to gain privileged access to a target by exploiting the identified vulnerabilities. This may take the form of launching a password guessing attack using user names collected during Phase I or the exploitation of a known vulnerability – i.e. buffer overflow.

Control Solutions’ penetration tests will be designed to simulate an inside (internal) and an outside (external) attack. With external penetration testing, firewalls usually limit the amount and types of traffic that are allowed into the internal network from external sources. Depending on what protocols are allowed through, initial attacks are generally focused on commonly used and allowed application protocols such as FTP, HTTP, or SMTP and POP. The following describes both an external and internal penetration attack.

**External Penetration Test**

To simulate an actual external attack, the testers are not usually provided with any real information about the target environment other than targeted IP address/ranges and they must covertly collect information before the attack. Information about the target organization is usually obtained from public web pages, newsgroups, Google, Yahoo and similar sites. Support sites where systems administrators sometimes post problems or assist with solutions can yield valuable foot printing information. Port scanners and vulnerability scanners are then used to identify target hosts. Since they are, most likely, going through a firewall, the amount of information is far less than they would get if operating internally. After identifying hosts on the network that can be reached from the outside, the tester tries to compromise one of the hosts using a vulnerability that is known about such host.

*NOTE: Once a single vulnerability is exploited and access to the internal network has been achieved, the test penetration test will usually stop. However, GBSB may wish to test/exploit additional vulnerabilities.*

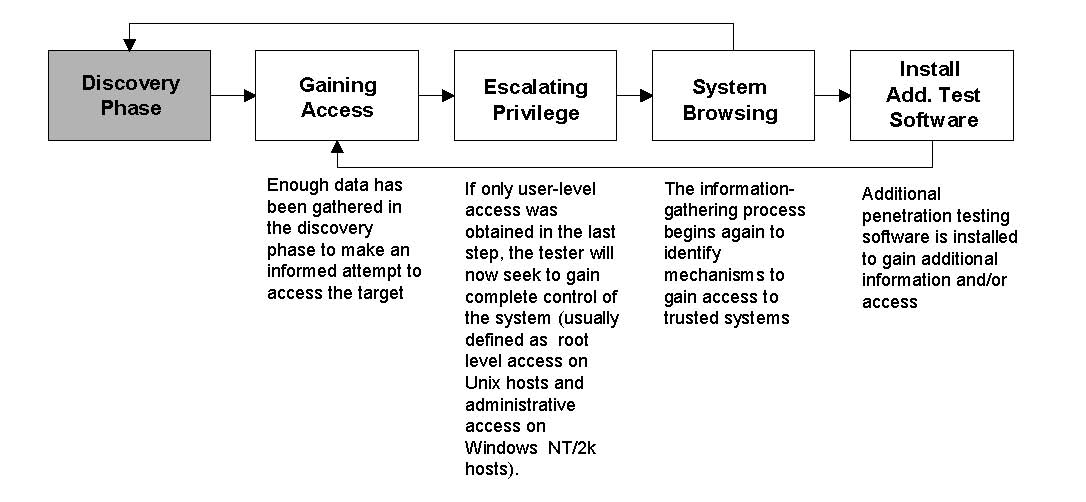
**Internal Penetration Test**

An internal penetration test is similar to an external except that the testers are now on the internal network behind the firewall. The security consultant is granted some level of access to the network, generally as a user but sometimes at a higher level. This penetration tester will then try to gain a greater level of access to the network through privilege escalation. The tester is provided with the information about the network that somebody with their provided privileges would normally have or know.

**Controls Solution Penetration Methodology**

Executing an attack is at the heart of any penetration test. This is where previously identified potential vulnerabilities as identified in Phases I to IV are verified by attempting to exploit them.

If an attack is successful, the vulnerability is verified and safeguards are identified to mitigate the associated security exposure. Frequently, exploitsthat are executed during attack execution do not grant the maximum level of access that can be gained by an attacker. Instead they may result in the testing team learning more about the targeted network and its potential vulnerabilities, or they may induce a change in the state of the security of the targeted network. In either case, additional analysis or testing is sometimes required to determine the true level of risk for the network. This is represented in the feedback loop between the Attack and Discovery phase of a penetration test as represented below.



**Attack Phase Steps with Loopback to Discovery Phase**

**Penetration Test – Rules of Engagement**

Since penetration testing is designed to simulate an attack and uses tools and techniques that may be restricted by law, federal regulations, and organizational policy, Control Solutions will work with GBSB to understand and document the rules of engagement which will include the following:

* Specific IP addresses/ranges to be tested;
* Any restricted hosts (i.e., hosts, systems, subnets, not to be tested);
* A list of acceptable testing techniques (e.g. social engineering, DoS, etc.) and tools (password crackers, network snuffers, etc.);
* Times when testing is to be conducted (e.g., during business hours, after business hours, etc.);
* Identification of a finite period for testing;
* IP addresses of the machines from which penetration testing will be conducted so that administrators can differentiate the legitimate penetration testing attacks from actual malicious attacks. Network providers may also need to be notified so that such traffic is not blocked;
* Points of contact for the penetration testing team, the targeted systems, and the networks;
* Measures to prevent law enforcement being called with false alarms (created by the testing); and
* Handling of information collected by penetration testing team.

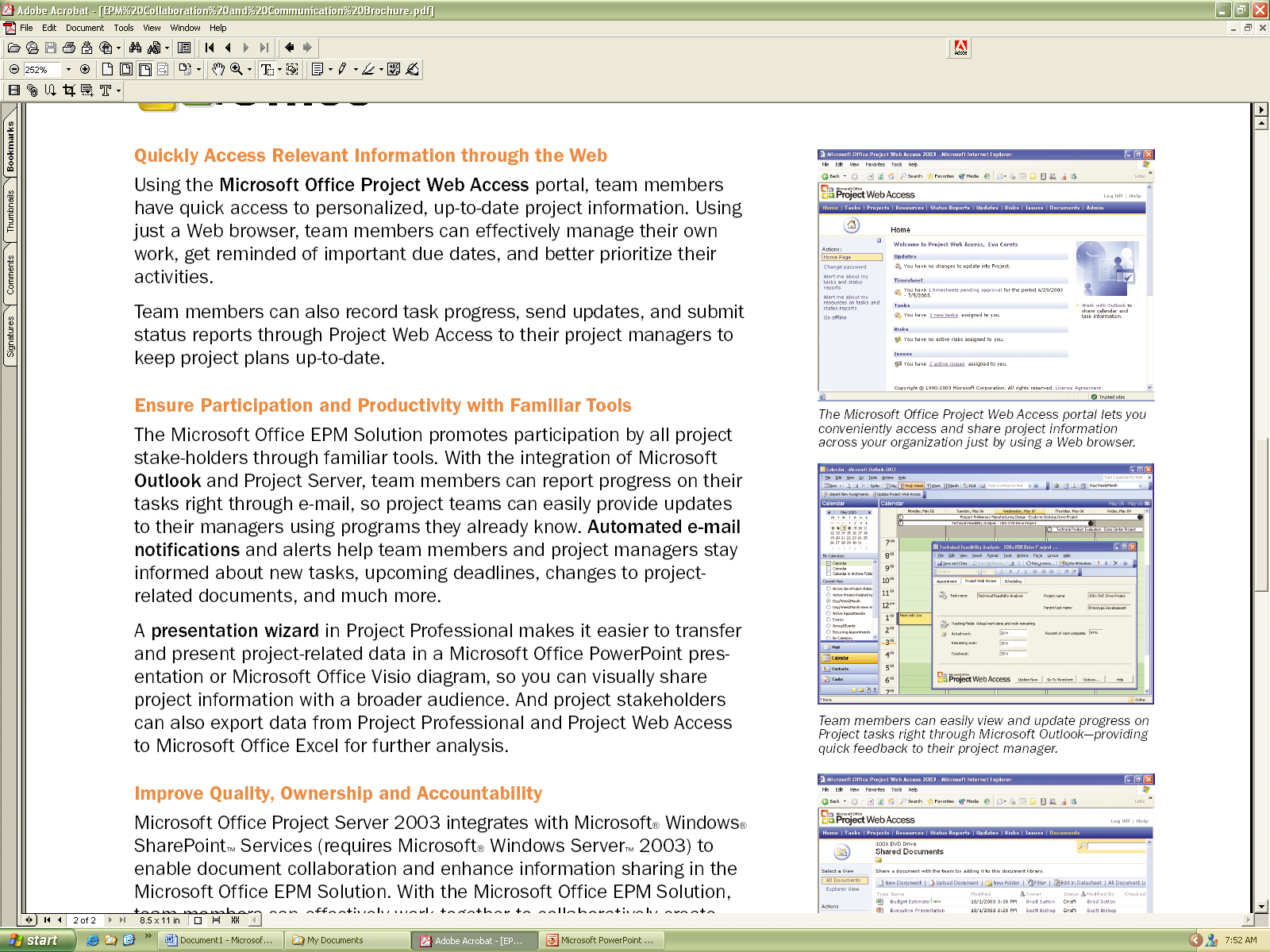
5 – Project Management Approach

**Project Management**

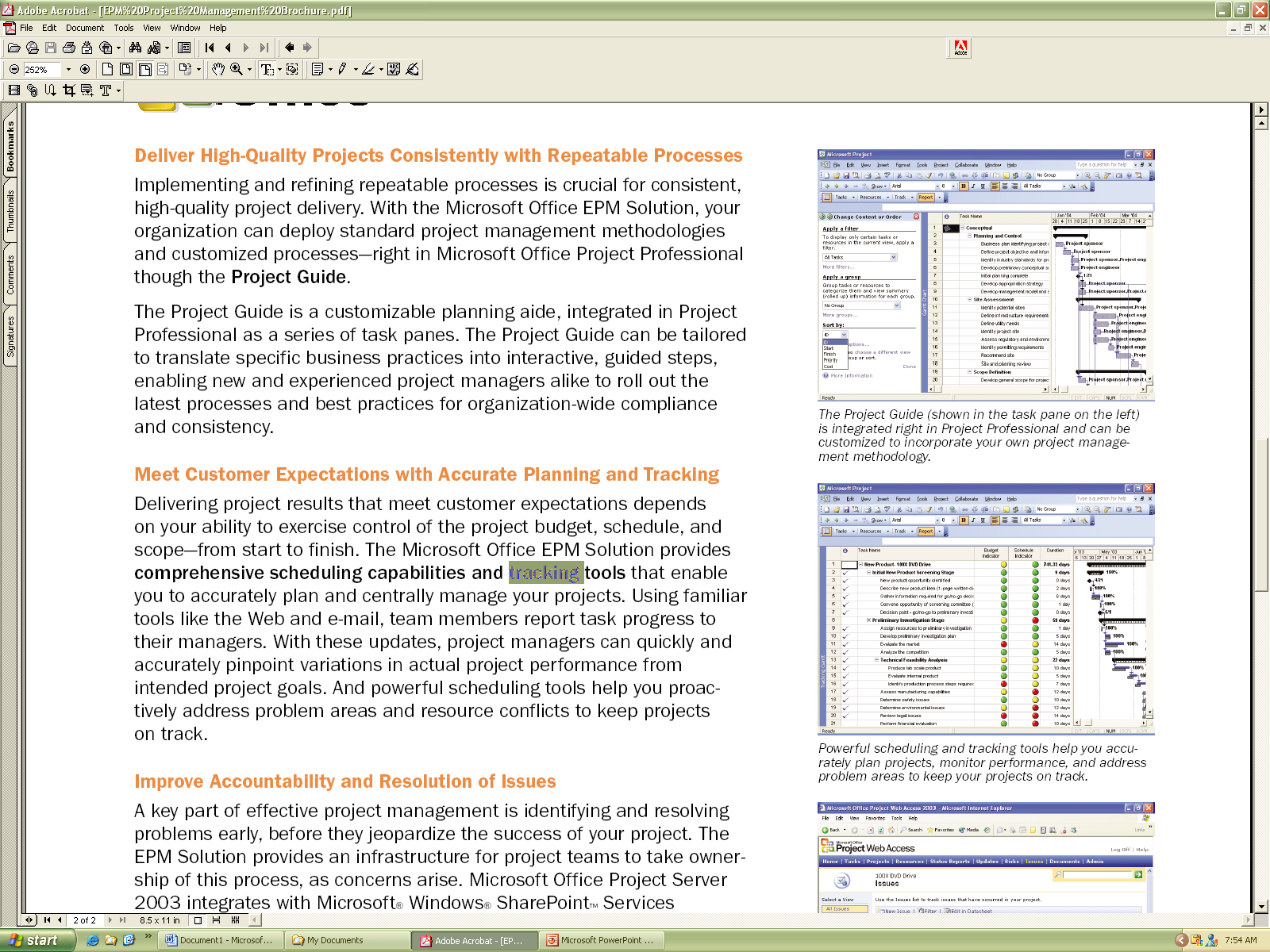
Allen Lum will be assigned as the project manager. He will use MS project to assist in managing the Network Security Assessment and Penetration Study. Resources, tasks, hours and milestones will be placed with MS project.

**Project Planning & Tracking**

**D**uring the early phases of the engagement, our team uses Microsoft Project Professional to develop a master project plan. The master project plan will be utilized in order to manage and monitor the progress. Once the project is initiated, our consultants utilize Microsoft Outlook to submit weekly status reports by area/phase/section. Updates will be loaded to Microsoft Project Web Access and are applied to the master project plan to track and report budget status. With the information consolidated and applied to the master project plan, Project Managers can quickly and accurately pinpoint variations in actual project performance versus intended goals.



ControlNET utilizes Microsoft Office Project Server 2003 which integrates with Microsoft SharePoint to enable project leaders to centrally track, assign and escalate issues for greater accountability. As issues (both from a project as well as compliance standpoint) are identified, our consultants create a new issue item. For each issue, the potential impact, the area assigned and the person responsible. We can further assign and escalate the issue and create reminders to follow-up in real-time by area, by project, or for the entire worldwide engagement. Through this central issue tracking system, we can better manage issues affecting your project and better prioritize efforts to resolve them quickly.



**Reporting**

Control Solutions will provide GBSB’s Internal Audit Department weekly briefings on project status, issues noted, and issues resolved. In addition, we will also provide real-time reporting of any significant project issues that would require immediate mitigating actions in the form of interim deliverables.

6 – Deliverables

**Deliverables**

The final product for GBSB Internal Vulnerability and Assessment and Internet Penetration Assessment will consist of two Deliverables as detailed below:

### *Deliverable 1: Oral Presentation*

Prior to submission of the final document, Control Solutions will deliver an oral presentation to highlight the work accomplished, including: Project Plan, detailed steps performed, limited work papers, and a documented corrective action log with weakness, associated vulnerability, risk, and recommended corrective action. We will obtain management feedback and reach an agreed upon action plan which will be documented and included in the final report discussed below.

### *Deliverable 2: Final Turnover Document*

At the end of the engagement, Control Solutions will submit a final report. This report will include:

* An executive summary including an overall assessment of security measures currently in place, the business implications of the key findings from the project, and a management level summary of any outstanding recommended actions;
* A summary chart showing findings and associated risks;
* An introduction stating the purpose of the report and a brief overview of the project including the scope, objectives, and approach used; and
* Project details including findings, analyses, key vulnerabilities, diagrams describing recommended changes to the architecture, and recommendations (both tactical and strategic).

In addition we have included the following Sample Deliverables that the Controls Solutions teams will deliver as part of this engagement:

* Summary Finding Chart – Exhibit I
* Internal and External Penetration Time Line – Exhibit II
* Table of Key Vulnerabilities – Exhibit III

**Exhibit I – Sample Deliverables – Summary Finding Chart**



The above chart represents a Summary of how key findings will be ranked and positioned in the table according to the relative risk or likelihood of exploit (on the vertical axis), effort required to remediate (horizontal), and overall business impact on the Customer. [(Color Code) Red – High Risk, Yellow – Medium Risk, Green – Low Risk.]

**Internal and External Penetration Time Line**

As part of our attack and penetration testing, Control Solutions will provide GBSB a timeline with milestones and associated comments. (Note the following is only a sample and may not represent actual work that may be performed on your network).

**Exhibit II**

| Penetration Timeline | | |
| --- | --- | --- |
| Date | Milestone | Comments |
| 1 April | **External Penetration Begins**. |  |
| 1 April | **Network Discovery**. The public-facing network was probed for access points. | CSI determined that the Class B network allocated to Customer is used as a private address block. Publicly routable addresses were limited to (IP Addresses). |
| 1 April | **Cisco Brute Forcing**. CSI began brute force login attempts. | Telnet administration was enabled on the Cisco router at (IP Addresses). CSI began a dictionary and brute force login attack against this router in an attempt to gain access. While no access was achieved, this interface should be closed to the outside world, as a brute force attack would eventually succeed. |
| 1 April | **SMTP Relaying**. SMTP relaying allows an attacker to send mail destined for another server via a third-party server. | The SMTP server at (IP Address) allows unrestricted SMTP relaying. This allows the server to be used as a relay in email attacks on other servers and companies. |
| 2 April | **Web Publisher Interface**. Enterprise Server includes an interface that facilitates the maintenance of web pages. | This web publisher interface was found to be enabled and is not restricted from public access. Also, it is not protected by SSL. While CSI was unable to modify files with this interface, it may still be possible. At the very least, the interface should be restricted to Customer intranet hosts. |
| 5 April | **Enterprise Server Administration Vulnerability**. The Enterprise Server has a remotely exploitable vulnerability in its administration server. | CSI was unable to access this server as it was protected by the firewall. However, the version of Netscape Enterprise Server that Customer uses is vulnerable to the attack. This vulnerability could be used to elevate access once an attacker has penetrated the firewall. |
| 5 April | **Overflow in Document Direct for the Internet Found**. | CSI found what looked like a remotely exploitable buffer overflow in Document Direct for the Internet. This third-party product is used by Customer on reports. While this vulnerability is not public, CSI is working with Customer and Vendor to ensure that it is resolved, as vulnerabilities of this sort may be found at any time by malicious attackers. |
| 6 April | **Exploit Attempt on Web base reporting.**  XYZ is running an old version Windows ISS Server that is susceptible to a remote buffer overflow. | CSI attempt at exploiting this vulnerability resulted in crashing the web server. A successful attempt would have gained access to the server, while unsuccessful attempts cause a denial of service. |
| 6 April | **XYZ Bypass Vulnerability Found**. It is possible to bypass the protection provided by XYZ product. | CSI discovered a flaw in XYZ product that allows bypassing the username/password authorization on protected web pages. This allowed CSI to access normally protected pages on xxx.com. |

Table of Key Vulnerabilities

Control Solutions will provide a table of Key Vulnerabilities describing the difficulty of exploit, risk of business impact, and associated recommendations for remediation.

**Exhibit III**

| Key Vulnerabilities | | | | |
| --- | --- | --- | --- | --- |
| Vulnerability Description | Difficulty of Exploit | Risk / Business Impact | Recommendation | IP Addresses AFFECTED |
| **IIS Showcode**.**asp Enabled**.  Showcode is a sample Active Server Page (ASP) that displays arbitrary files on a web server. | **Trivial**.This attack requires a web browser. | **High**.Attackers could view files on several IIS servers. | Remove showcode.asp from the filesystem.  Additionally, Marex.com should consider removing the /msadc directory. |  |
| **Webhits**.**dll and the** .**htw file extension enabled**.  Webhits.dll will reveal source code to asp and asa files. | **Moderate/Sophisticated**.An attacker requires some form of access to view these files. | **High**.The viewing of asp and asa files allows an attacker to understand the business logic of a web site. This might also allow for the compromise of database or other credentials. | Using the Internet Service Manager (ISM) unmap the extensions .htw from webhits.dll. |  |
| **Htimage Buffer Overflow**.  There is a remotely exploitable buffer overflow in htimage.exe. | **Sophisticated**.There are no publicly available exploits for this vulnerability. | **High**.Attackers could gain interactive access to the host, allowing them to view files and attack services on the same subnet without the protection of a firewall. | Remove htimage.exe and consider removing the /cgi-bin virtual directory via ISM. |  |

7 – Technical Tools and Utilities

Currently Controls Solution uses a number of commercially proven open-source and internally developed software tools to assist in performing Information Technology Audits, IT Risk Assessments Security Reviews, and Vulnerability and Penetration Attacks.

In addition we have developed tools in house that can perform host assessments on Windows and UNIX based systems. These host based tools examine operating system security such as networking parameters/services and user access controls.

We have included a table of tools that can be used as part of our engagement with CTC.

**Port Scanners**

|  |  |
| --- | --- |
| Amap | Analyzes services that are running on a system that may be running on non-default ports |
| Nmap | Linux based port scanner, used for OS finger printing and port scanning |
| Solar Winds | Used to analyze SNMP information |
| SuperScan | Windows based port scanner for and OS finger printer |
| RPCScan | RPC enumerator and scanner |
| Netcat | Unix tool for TCP connection establishment |

**Vulnerability Scanners**

|  |  |
| --- | --- |
| Nessus | Open source vulnerability scanner |
| Nikto | Web server scanner which performs comprehensive tests against web servers for multiple items, including over 2200 potentially dangerous files/CGIs, versions on over 140 servers, and problems on over 210 servers |
| Nilo | IIS security scanner |
| Retina | Windows based vulnerability scanner (commercial) |
| Scanner.sql | An Oracle database security scanner that find possible vulnerabilities in Oracletable layouts. |
| Triton | Utilizes pre configured lists of known http application paths to find flaws in application configuration |

**Tools Used to Exploit Hosts**

|  |  |
| --- | --- |
| Core-Impact | A network vulnerability assessment and exploitation tool utilized by our consultants to identify and test the security of your information technology infrastructure. |
| Holodeck | Program used to find vulnerabilities in software |
| Kaht.exe | Utilized as a Trojan horse when exploiting webdav |
| Minibrowser | Used when performing CSS attacks, allows reading of cookie data |
| Ncx99 | Modified version of netcat that extend the service and port binding capabilities |
| Tsearch | A memory editor used to read and modify memory values |
| WebDavin | Main tool used when exploiting Webdav vulnerabilities |

**Brute Forcing Tools**

|  |  |
| --- | --- |
| Access Driver | A Windows based password brute forcer that is good for web forms |
| John The Ripper | The hash brute forcing utility |
| Raptor | A wordlist manager and generator that takes a website and will create a password mailing list from the website |
| SAMInside | Brute forces Windows SAM files as well as syskey passwords |
| THC-Hydra | A complete brute forcing tool that utilizes nmap and can brute force SMB, Telnet, HTTP and other forms of passwords |
| Tscrack.exe | A Windows Terminal Services brute force utility |

8 – Detailed and Itemized Pricing

Our approach to fees is summarized as follows:

* We have provided you with a competitive fee structure, recognizing that this is an important opportunity for us to build a strategic relationship with GBSB.
* We will work to ensure you receive a consistent quality of service and we will not surprise you with “special charges” or additional costs.
* Consultants dedicated to GBSB will have an average of eight years of business, technology and internal auditing experience. Your projects will not be used as a training ground as we do not employ inexperienced staff.
* Our professional fees for this engagement will be based on the actual time spent on the engagement at the proposed hourly rates for our professionals. Our proposed hourly rates are based on the skill and experience level of the individuals assigned.

|  |
| --- |
| **Professional Fees – Hourly Rates** |
| |  |  |  |  |  | | --- | --- | --- | --- | --- | | **IT Resource Level** |  | **Standard Rates** |  | **Proposed Rates** | | Information Technology Consultants |  | **$XXXX** |  | **XXXXXX** | |

We would like to partner with GBSB on this important engagement and we are willing to make an investment in that partnership. We propose to perform the work at an hourly rate of $125 for all levels of staff.

In addition to our professional fees, we are reimbursed for travel, lodging and other expenses that we incur such as telephone charges, fax transmissions, postage and photo reproduction. We will seek pre-approval should significant travel be required for any reason. Please be assured that every effort will be made to keep both our professional fees and our expenses to the minimum necessary to satisfactorily accomplish each engagement.

We have developed a detailed task list below showing the estimated hours to complete each Phase I. In Phase II – we broke down the hours for each task. This will give GBSB the opportunity to select tasks based on their internal Audit requirements.

|  |  |
| --- | --- |
| **Project Tasks** | **Estimated Hours** |
| Planning | 8 |
| Phase I – Identification of Critical Information Technology Assets | 16 |
| Phase II – Internal and External Network Vulnerability Analysis |  |
| - Footprint Analysis and Information Gathering | 32 |
| - Verification of Footprint Analysis | 16 |
| - Network Vulnerability Scan And Assessment  Internal and External | 40 |
| - Host Base Assessment - includes 4 hosts | 32 |
| - Firewall Review and Testing | 40 |
| Phase IV – Penetration Testing |  |
| - Internal Penetration test | 40 |
| - External Penetration Test | 60 |
| Report Generation | 40 |
| Total | 324 |
| - Host Based Assessment per additional host  At this time the total number of hosts to be assessed is not known. The hours represent the additional cost per host above 4 hosts which are listed in the above table | 8 |
| - Wireless Scans and Assessments - optional | 32 |

***Please Note:***

*The table above depicts the estimated effort required to perform the external and internal Network Security Assessment Review. If, during the course of our work we find that events beyond our control may impact our estimate, we will notify you and seek your approval to proceed or to modify the scope of work. Any work performed in excess of our original estimate will be discussed and agreed with you in writing.* *No additional work or costs will be incurred without your written approval. Our ability to meet the timetable presented herein takes into account a certain level of preparation and assistance from GBSB personnel. We will advise management on a timely basis if GBSB or any related third parties are not providing the required information or resources, or should any other circumstances arise, which may cause actual time or resources to exceed our estimate.*

9 – Legal Terms and Conditions

**Terms & Conditions**

These Terms and Conditions and the engagement letter (and any attachments) (the “Engagement Letter”), and any subsequent amendments or addenda thereto, to which these Terms and Conditions are attached (collectively, the “Agreement”) constitute the entire agreement between the client to which such engagement letter is addressed (“Client”) and Control Solutions International, a corporation organized under the laws of the State of Florida (“Control Solutions”), regarding the project described in the Engagement Letter. Capitalized terms not otherwise defined herein, shall have the meaning ascribed to them in the Engagement Letter. Headings are only used for informational purposes and have no legal significance.

***Changes to Services.***Control Solutions will not undertake work that is beyond the Scope of Services set forth in this Agreement. Either party may request changes to the Services. To be effective, a change in scope must be in writing and signed by both parties.

***Confidentiality****.* Control Solutions’ proprietary software tools, methodologies, techniques, ideas, discoveries, inventions, trade secrets, intellectual property, and any other oral or written information identified as confidential by Control Solutions, are confidential information of Control Solutions. Such confidential information of Control Solutions includes information owned prior to the beginning of the engagement to which this letter relates as well as information developed by Control Solutions during the course of this engagement. Any data relating specifically to the Client’s business, and other information identified as confidential by the Client, are confidential information of Client. Client confidential information and Control Solutions’ confidential information are collectively referred to as “Confidential Information.” Each party shall use Confidential Information of the other party only in furtherance of the purposes of this Agreement and shall not disclose such Confidential Information to any third party without the other party’s prior written consent. Each party agrees to take reasonable measures to protect the confidentiality of the other party’s Confidential Information and to advise their employees of the confidential nature of the Confidential Information and of the prohibitions herein.

Notwithstanding anything to the contrary contained in this Agreement, neither party shall be obligated to treat as confidential any information disclosed by the other party (the “Disclosing party”) which: (1) is rightfully known to the recipient prior to its disclosure by the Disclosing Party; (2) is released by the Disclosing Party to any other person or entity (including governmental agencies) without restriction; (3) is independently developed by the recipient without any reliance on Confidential Information; or (4) is or later becomes publicly available without violation of this Agreement or may be lawfully obtained by a party from any nonparty. Notwithstanding the foregoing, either party will be entitled to disclose Confidential Information of the other to a third party as may be required by law, statue, rule or regulation, including any subpoena or other similar form of process, provided that (and without breaching any legal or regulatory requirement) the party to which the request is made provides the other party with prompt written notice and allows the other party to seek a restraining order or other appropriate relief.

Subject to Control Solutions’ confidentiality obligations in this Agreement, nothing herein shall preclude or limit Control Solutions from providing similar services for other clients.

***Deliverables.***The passage of ten working days from the date when a project deliverable or output (each a “Deliverable”) is provided to Client without receipt by Control Solutions of notice of non-acceptance by Client, or use by Client of a Deliverable will constitute final acceptance by Client. Client will own all written material originally prepared for Client and delivered under this Agreement. Control Solutions’ working papers and Control Solutions’ confidential information belong exclusively to Control Solutions (except to the extent they contain Client Confidential Information). Client will have a non-exclusive, non-transferable license to use Control Solutions Confidential Information for Client’s own internal use and only for the purposes for which they are delivered to the extent that they form part of the deliverables.

***Electronic Mail (“e-mail”) Communications.***During the provision of the Services the parties may wish to communicate electronically with each other at a business e-mail address. However, the electronic transmission of information cannot be guaranteed to be secure or error free and such information could be intercepted, corrupted, lost, destroyed, arrive late or incomplete or otherwise be adversely affected or unsafe to use. Accordingly, each party agrees to use commercially reasonable procedures to check for the then most commonly known viruses and to check the integrity of data before sending information to the other electronically, but each party recognizes that such procedures cannot be a guarantee that transmissions will be virus free. It remains the responsibility of the party receiving an electronic communication from the other to carry out a virus check on any attachments before launching any documents whether received on disk or otherwise.

***Client Responsibilities.***Client agrees to perform the tasks and provide the assistance agreed to by the parties. Client also agrees to provide additional support necessary for Control Solutions to perform the Services, and to ensure that it has appropriate back up, security and virus ­checking procedures in place for any computer facilities, information or materials it provides. Any timing or fee estimate we have provided for this engagement takes into account the agreed-upon level of assistance from Client and commitment of Client resources. Control Solutions shall not be responsible for any delay or other consequences resulting from Client’s failure to perform any of its obligations under this Agreement. Client’s failure to satisfy its responsibilities under this letter may lead to an increase in Control Solutions fees, depending on the extent to which Control Solutions has to perform more services or reschedule its commitments to deliver the Services, or Control Solutions’ inability to provide the Services.

***Fees and Payment.***Client shall pay Control Solutions the fees set forth in the Engagement Letter and all invoices submitted to Client. Client shall be responsible for paying any taxes (such as applicable sales taxes, duties or goods and services taxes) for which it is legally liable arising from this Agreement at the rate in force at the date the liability arises. All invoices will be due fifteen (15) days after the date of the invoice. Control Solutions reserves the right to charge a commercial rate of interest, within the confines of applicable law, on accounts that are overdue by more than one month.

***Warranties and Liabilities.***Control Solutions will perform the Services in accordance with the consulting standards established by the AICPA and in accordance with the terms of this Agreement. Notwithstanding anything to the contrary contained in this Agreement. CONTROL SOLUTIONS MAKES NO OTHER WARRANTIES, EXPRESS OR IMPLIED, OR WHETHER ARISING BY OPERATION OF LAW OR OTHERWISE, INCLUDING WITHOUT LIMITATION IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. IN PARTICULAR, CONTROL SOLUTIONS DOES NOT WARRANT THAT THE SERVICES OR THE CLIENT’S IMPLEMENTATION OF ANY DELIVERABLE OR RECOMMENDATION WILL SATISFY CLIENT’S REQUIREMENTS. CLIENT ACKNOWLEDGES, UNDERSTANDS AND AGREES THAT CONTROL SOLUTIONS DOES NOT GUARANTEE OR WARRANTY THAT IN PERFORMANCE OF THIS AGREEMENT IT SHALL FIND, LOCATE OR DISCOVER ALL OF THE CLIENT’S SYSTEM VULNERABILITIES AND WILL NOT HOLD CONTROL SOLUTIONS RESPONSIBLE TO DO SO.

Control Solutions agrees to indemnify, defend and hold harmless Client from and against any and all amounts payable under any judgment, verdict, court order or settlement for (i) death or bodily injury or the damage to or loss or destruction of any real or tangible personal property to the extent arising out of the Control Solutions’ negligence or willful acts in the performance of this Agreement, and (ii) claims of infringement of any trade secrets, copyrights, trademarks or trade names alleged to have occurred and arising from deliverables provided by Control Solutions to Client in connection with this engagement. Should the Client’s use of the deliverable prepared by Control Solutions be determined to have infringed, or if, in Control Solutions’ judgment, such use is likely to be infringing, Control Solutions may, at its option: (1) procure for the Client the right to continue to use the deliverable; or (2) replace or modify the deliverable to make its use non-infringing while yielding substantially equivalent results. If neither of such options are or would be available on a basis that Control Solutions finds commercially reasonable, Control Solutions may terminate this Agreement, the Client shall return the deliverable and Control Solutions shall refund the fees paid for the associated services, less a reasonable allowance for use. This indemnity does not cover alleged infringements caused by modifications to the deliverable that are not made by Control Solutions or that result from the Client provided designs, specifications or other information or from combination of such work with products or services not provided by Control Solutions.

In no event will Control Solutions be liable for any loss, damage, cost or expense attributable to any act, omission or misrepresentations by Client, its directors, employees or agents. In no event shall Control Solutions be liable to Client, whether a claim be in tort, contract or otherwise: (a) for any amount in excess of the total professional fees paid by Client to Control Solutions pursuant to this Agreement; or (b) for any consequential, indirect, lost profit or similar damages relating to or arising from the Services provided under this Agreement, except (i) to the extent finally determined to have resulted from the gross negligence, willful misconduct or fraudulent acts of Control Solutions relating to such Services, and (ii) in connection with the indemnity for intellectual property infringement. In addition, Control Solutions shall have no liability to Client arising from or relating to any third party hardware, software, information or materials selected or supplied by Client.

***Testing Services.***If the Services include testing, penetration, intrusion or analysis of Client’s information systems or enterprise, whether by using intrusive or passive techniques and software tools (“Testing Services”), the provisions of this section shall apply. Client hereby consents to Control Solutions performing the Testing Services to Client’s systems identified as well as any other ancillary systems that may be connected to the Client’s networking infrastructure, including Internet, Intranet and Extranet connections and Client shall be solely responsible to obtain all necessary consents of all such persons or entities to allow Control Solutions to perform such Testing Services.

Client understands that Testing Services may result in disruptions of and/or damage to Client’s or third party’s information systems and the information and data contained therein, including but not limited to denial of access to a legitimate system user, automatic shut-down of information systems caused by intrusion detection software or hardware, or failure of the information system. Client is solely responsible for understanding the testing steps that will be performed as part of the Testing Services and for arranging alternative means of operation should such disruptions or failures occur and for all damage caused by the Testing Services. Control Solutions and its members, officers, directors, employees, representatives, agents, subsidiaries, affiliates, subcontractors and consultants shall have no responsibility or liability for, and Client shall have no recourse against any of them for any damages or losses whatsoever as a result of such Testing Services.

***Terms and Termination.***If Control Solutions commenced the performance of Services prior to the execution of this Agreement, this Agreement shall nonetheless cover the performance of such Services. Either party may terminate this Agreement upon written notice to the other party. In the event of termination Client will be responsible for fees and expenses incurred through the date termination notice is received.

***Other Matters.*** For the duration of this Assignment, and for 12 months after its termination or completion, Client agrees not to hire (as an employee, independent contractor, or consultant) or otherwise utilize in any other capacity the services of any Control Solutions employee who has performed services for the Client as part of this Assignment, unless Client first obtains the written consent of Control Solutions. If the Client violates this portion of the Engagement Letter, it agrees to pay to Control Solutions the equivalent of 40% of the employee’s total post-termination compensation he or she earns from Client. That payment to Control Solutions is to be made on a monthly basis for the duration of the employee’s services to client, for a maximum of eighteen months.

Neither party shall be liable to the other for any delay or failure to perform any of the Services or obligations set forth in this Agreement due to causes beyond its reasonable control. If any provision of this Agreement is determined to be invalid under any applicable law, it is to that extent to be deemed omitted, and the balance of the Agreement shall remain enforceable. In performing the Services, Control Solutions is an independent contractor. No delay or omission by either party in exercising any right or power shall impair such right or power or be construed to be a waiver. No waiver or discharge shall be valid unless in writing and signed by an authorized representative of the party against whom such waiver or discharge is sought to be enforced. A waiver by either party of any of the covenants to be performed by the other or any breach thereof shall not be construed to be a waiver of any succeeding breach or of any other covenant. Client accepts and acknowledges that any legal proceedings arising from or in connection with the Services must be commenced within one year from the date Client became aware or ought reasonably to have become aware of the facts which give rise to our alleged liability and in any event no later than two years after any such cause of action accrued. Neither party may assign this Agreement without the prior written consent of the other party, which consent will not be unreasonably withheld. The provisions of this letter, which expressly or by implication are intended to survive its termination or expiration, will survive and continue to bind both parties. This Agreement constitutes the entire Agreement between the parties with respect to the Services and the rights and responsibilities of the parties with respect to this engagement. This Agreement supersedes any prior understandings, proposals or agreements with respect to the Services. Any claims or disputes arising from this Agreement shall be brought in the courts of the State of New Hampshire and any questions with respect to the construction of this agreement, and the rights and liabilities of the parties hereto, shall be governed by the laws of the State of New Hampshire. If Client breaches any term of this Agreement, Control Solutions may engage the services of an attorney or attorneys to protect its rights hereunder, and in the event of such engagement following any breach by Client, Client shall pay Control Solutions its reasonable attorneys’ fees (together with reasonable appellate counsel fees, if any) and expenses incurred by Control Solutions, whether or not an action is actually commenced against Client by reason of such breach. All references to “attorneys” shall include without limitation any attorney or law firm engaged by Control Solutions, and all references to “fees and expenses” in this paragraph and elsewhere in this Agreement shall include without limitation any fees of such attorney or law firm and any allocation charges. In the event that any provision or clause of this Agreement conflicts with applicable law, such conflict shall not affect other provisions of this Agreement which can be given effect without the conflicting provision, and to this end, the provisions of this Agreement are declared to be severable.

Rev. 3/21/06

Appendices

References

Upon your request, we can provide you with detailed professional services that were performed by Controls Solutions for the following references:

**Canadian Pacific Railway**

Garry Richards

Assistant Director of Internal Audit

(416) 595-3224

IT Security Network Review – Internal and External

**Manulife Corp.**

Mike Laman

VP Financial Disclosure and Internal Control Compliance

(416) 852-8481

IT SOX Engagement

**Blue Cross Blue Shield of Vermont**

Ms. Dawn A. Schneiderman

Director – Audit & Business Consulting

(802) 371-3222

IT Security Network Review – Internal and External

The GBSB Engagement Team

Our people are the most important aspect of the services we offer and the most critical element of a successful relationship. The quality of service you receive from the firm selected will only be as good as the people engaged on this important project. Beyond their professional credentials, as presented in the summary of their biographies, our professionals embody the personal chemistry, motivation, and enthusiasm necessary to ensure smooth and efficient working relationships with GBSB . In addition to auditing and consulting skills, our professionals have been selected for their adaptability, experiences, communication skills, interpersonal skills and business acumen. We are confident that this team, under the leadership of Allen Lum, will meet or exceed your expectations in every respect.

We are confident that all of our consultants will demonstrate the skills, professionalism and commitment needed to ensure that the goals and objectives of the engagement are met. Below are the key individuals who will support this effort and who will report directly to you.

The consultants that have been assigned to the engagement have not been convicted of a felony to our knowledge.

Allen Lum – IT Director

|  |  |
| --- | --- |
| Education & Certification   * MS, Computer Science – Pace University * MBA, Finance– New York Institute of Technology * BA, Accounting – University of Louisiana at Monroe * Certified Public Accountant * Certified Information Systems Auditor * Certified Information Security Manager   Areas of Expertise   * Sarbanes-Oxley Section 404 * Internal audit * Business continuity and disaster recovery planning * Risk assessments * IT controls * Security planning * System implementation * Project management   Recent Engagements   * Sarbanes-Oxley Section 404 * Internal audit * System implementation | An executive information technology professional with 25 years of experience, Allen Lum is the IT Director for Control Solutions International. A recognized and published information systems security and assurance professional, he is currently specializing in design and assessment of information security and in Sarbanes-Oxley (SOX) Section 404 engagements.  In recent Section 404 projects, Allen has been responsible for documenting and testing general computer controls and application controls. Management responsibilities have included project planning and scoping, which encompasses understanding the financial reporting processes and the systems supporting these processes.  Prior to joining Control Solutions, Allen formed ACS Solutions Inc. / eDelta Consulting, which provided a wide range of technology and information technology consulting services to Fortune 500 firms and other private and public companies. Engagement responsibilities included performing SOX 404 testing and controls documentation, security reviews, operating system audits (UNIX, Windows NT/2000), and network audits, among other things. He developed and implemented IT disaster recovery plans including equipment and storage requirements, development of vendor RFPs, networking solutions at recovery site, and media backup and recovery requirements. Additionally, he developed and implemented network security standards covering firewall and networking architecture, intrusion detection, evaluation of incident response plans and the use of various security, forensic and network scanning tools.  For ten years, Allen was a Principal at Ernst & Young LLP in New York, where he managed a staff of ten professionals in Retail Distribution and Financial Services Sectors. He built strong client relationships, developed his credibility as a project manager and expanded his interpersonal skills. Management responsibilities included developing and maintaining a book of business exceeding $4 million. During internal audit outsourcing projects, Allen managed the IT Internal Audit Department for several financial services clients. Performing business risk assessments, he used results as a basis for the implementation of audit plan and strategy. For management infrastructure and security consulting engagements, he developed and implemented overall data integrity programs as a prelude to the implementation of major ERP and demand planning software packages. Allen led teams to create and implement enterprise-wide data integrity, network security architecture and security solutions. As a business continuity and disaster recovery plan project manager, he developed and implemented plans for major retailing and financial institutions. In addition, he led a team that designed and implemented a technology disaster recovery plan for a major retailer’s data center.  Previously, Allen held prestigious positions at several corporations, including Security Pacific Corporation, EF Hutton and Avon Products. His responsibilities ranged from review and evaluation of general and application controls in various business areas, to development and use of audit software in data analysis and review of security implementations on systems (from stand-alone systems to multiple-node networks). |

RossBoulton– Manager

|  |  |
| --- | --- |
| Education & Certification   * Certified Information Systems Auditor * Certified Information Systems Security Professional * Microsoft Certified Systems Engineer * Microsoft Certified Solution Developer C#.net 2003 * Novell Certified Administrator * Cisco Certified * Citrix Certified   Areas of Expertise  Industry:   * IT security/auditing * Network infrastructure * Sarbanes-Oxley compliance   Functional:   * IT security assurance * Enterprise networking architecture * Penetration testing * LAN management   Technical:   * IT security audits * Platforms – UNIX, Windows (all), NetWare * Penetration testing * Database (MS-SQL)   Recent Engagements   * Sarbanes-Oxley 404 IT testing * State government IT audits * IT security * Healthcare/HIPAA compliance | Ross Boulton has over 20 years of experience in the field of IT security consulting and MIS management. His diverse knowledge of IT contributes to the secure and effective management of large government, institutional and corporate networks.  Ross’s Sarbanes-Oxley Section 404 engagements have included Georgia Gulf Corporation, Artesyn, ACP, Florida Distillers Company, Dycom and Helen of Troy. For general IT and application controls, he wrote the narratives, identified the IT controls, developed test plans, tested the controls, provided guidance to remediate problems and then retested the remediated controls.  As the senior IT auditor for the Louisiana Legislative Auditor, Ross provided IT audits for state agencies that were as large as 10,000+ nodes in hundreds of locations throughout the State of Louisiana. The COBIT standard was used for these audits.  Ross also consulted with the chief information security officer to create security policies and procedures that encompassed Internet access, remote access, network architecture and acceptable use. The most recent guideline he developed was for the secure disposal of surplus hard disks. Ross demonstrated the need for this guideline by using Encase, a forensics tool, to prove that sensitive data was recoverable even after reformatting the disks and deleting the partitions. Ross has also developed security policies for almost every company with which he has been associated.  As a consultant, Ross provided network penetration tests and IT audit services for three banks in the New Orleans area. He uncovered vulnerabilities and then documented the actions needed to remediate these vulnerabilities.  Ross’s previous assignment was as an IT security consultant with ERCOT, the electrical management company for the state of Texas. His role at ERCOT was to protect the network from intruders, viruses and other security risks by enforcing compliance with the ISO 17799 standard. Ross created a security operations center to monitor two intrusion detection systems (Cisco IDS and Real Secure) plus a collection of other security tools. The successful protection of this network prevented electrical outages such as those experienced in the northeastern states during the summer of 2003.  Ross obtained experience with HIPAA regulations while he was the LAN administrator for a major hospital network (1999 to 2001). Preparation for HIPAA compliance included securing servers and network communications.  Ross continues to build a portfolio of credentials by obtaining one major certification every year. He is close to completing an online degree in MIS and has half the credit hours for a master’s degree in IT security. Ross recently completed the requirements for Certified Information Systems Auditor (CISA). |

Brian Goss – IT Manager

|  |  |
| --- | --- |
| Education & Certification   * Center for Advanced Technology Training – Bray, Ireland * AnCo Computer Ecuation Center – Dundalk, Ireland * De La Salle College – Dundalk, Ireland   Areas of Expertise   * IT auditing * Sarbanes-Oxley Section 404 * Cisco Catalyst switches * IT processes * Systems, network and application vulnerability assessments * Application, network infrastructure, database and data center audits * IT governance, risk management and assessment * Information security program development and evaluation   Recent Engagements   * Sarbanes-Oxley Section 404 compliance * IT controls   Technologies   * Cisco PIX and Checkpoint firewalls * Cisco core switches and routers * Network Intrusion Detection Systems * Open Source Nessus and commercial vulnerability scanners such as Core Impact and Eeye Digital Retina | Brian Goss has over twenty years of experience in the computer industry and is currently a Senior IT Manager with Control Solutions International with wide-ranging experience in the area of Information Security.  Brian has an in-depth understanding of COBIT, ISO 17799, ITIL, COSO and the Federal IT Security Framework. He has worked in a variety of security roles over the years including Director of Security, consultant performing penetration and vulnerability scanning, developing tailored Internet and Internal Security audit programs as well as auditing network, system and database security configurations. He has been a consultant to US, Canadian and European large cap companies in the financial services, high tech, manufacturing and pharmaceutical sectors as well as working with the Irish and Swedish Department of Defense. His intricate knowledge and hands on expertise in administrating wide area networks, network operating systems, storage area networks, desktop computing, anti-virus operations, firewalls, virtual private networks, routers and Web ASP development has enabled him to assist corporations design layered security defenses, analyze vulnerability assessments and develop risk assessment methodologies to evaluate technology based and IT GCC mitigating controls.  Brian has developed risk management programs and risk assessment methodologies that not only identify compensating controls but also calculate the residual risk posed by threats after evaluating mitigating controls. His business experience and IT skills have allowed him to work closely with client senior management and technical staff in developing audit strategies, disaster recovery and business continuity plans  Prior to joining Control Solutions, Brian was a senior security consultant with Limbic Networks LLC where he designed security solutions for high tech, non-profit and financial sector companies. He developed a risk assessment application where management could assign IT General Computer and technology controls to systems and vulnerabilities identified with Eeye Digital Retina security scanning products which allowed them to calculate residual risk.  As Director of Systems Architecture and Security Group at Engage Technologies, Brian’s group was responsible for the design, implementation and management of a global network consisting of four data centers spread across three continents providing solutions to 30 autonomous business units with over 3,000 users. Engage’s parent company adopted his network design as the blue print for all of their holding companies.  Holding various system and network administration positions after beginning his career at Siemens-Nixdorf Information Systems in Dublin, Ireland, Brian specialized in PC networking and Unix client server systems where he was a member of a team responsible for government, military, banking and insurance contracts.  Brian is an active member of the Information Systems Audit and Control Association and performs pro-bono security services to high target non-profit organizations. |

Mark Edmead – IT Director

|  |  |
| --- | --- |
| Education & Certification   * PhD Candidate, DM (University of Phoenix) * MBA, University of Phoenix * BS, Information Technology, University of Phoenix * BSEE, Northeastern University * Certified Information Systems Security Professional (CISSP) * Certified Information Systems Auditor (CISA) * Systems Security Certified Practitioner (SSCP) * Active Department of Defense Top Security Clearance   Areas of Expertise   * IT audits * Compliance audits * SAS 70 * Security policy and development * Sarbanes-Oxley * Operating system security * Network Architecture * Network security * ISO 17799 * COBIT/COSO   **Recent Engagements**   * Audit consultant * Project management * Security consultant * Senior Systems Security Architect * Information Security consultant   **Technical Experience**   * Windows NT/2000 * IIS * Unix * SQL * Oracle | As an IT Director at Control Solutions International, Mark Edmead has over 28 years of experience in computer systems architecture, information security, and project management. Mark has extensive knowledge in IT and Application audits, IT Governance, and Sarbanes-Oxley compliance auditing. He specializes in all aspects of information security and protection including access controls, cryptography, security management practices, network and Internet security, computer security law and investigations, and physical security. Mark has consulted with Fortune 500 and Fortune 1000 companies in the areas of information systems and Internet security. He is an instructor for the Internal Institute of Internal Auditors and Learning Tree International, as well as an adjunct faculty profession for Keller Graduate School of Management, where he teaches graduate information security courses.  Prior to joining Control Solutions, Mark was an independent information security and regulatory compliance consultant where he performed IT General Infrastructure and Application audits in line with COBiT and COSO standards and methodologies. He conducted internal IT audits in the areas of critical infrastructure/systems and applications, assessed and tested internal controls of critical infrastructure platform systems – Windows, Unix, IIS, SQL, Oracle – and assessed and tested internal controls of various critical financial applications. He prepared risk assessments and determined risks to critical financial data systems and infrastructure components. He conducted reviews of existing systems and applications – ensuring appropriate security, management, and data integrity via control processes. He prepared written reports to all levels of management, where he also participated in audit review panel sessions to address results, conclusions, and follow-up actions required.  Mark helped establish the IT Risk Management department for various large corporations. He managed the implementation of all controls and governance initiatives and developed business process narratives, flowcharts and defined, developed and implemented control processes as needed. He performed business process and IT Risk/Control services including Application Security and Controls Assessment, Information Technology Controls, Infrastructure Security, System Project Control Assurance and Security Management.  Mark worked as a consultant for Sarbanes-Oxley IT General and Application Control Audits for various companies where he performed SOX IT and Application control audits. He evaluated existing controls and was responsible for presenting complete analysis of internal control issues to the SOX Compliance and Tax Officer, Disclosure Committee and Audit Committees. His work included reviews of security policies and standards to ensure the consistency of security products and their configurations. He also reviewed the security controls to determine if they effectively enforced the governing policy and standards and addressed threats from both within and outside the enterprise network.  Mark’s previous clients include Toyota Motors, Ingram Micro, New Century Mortgage, PeoplesBank, Capital One Credit, Bridgemark/BDO Siedman, Maxwell Technologies, Wells Fargo Bank, Sempra Energy, IBM Corporation, World Health Organization, Booz-Allen Hamilton, Wells Fargo, Washington Mutual, and Affinity Networks. |

Company Overview

* Official registered name: Controls Solutions International, Inc

Dun & Bradstreet Number: 92779842

Primary SIC number: 8721

Secondary SIC number: 8748

Address: Control Solutions

400 Amherst Street, Suite 201

Nashua, NH 03063

Phone number: 603-598-0700 or 800-627-0028

Fax number: 603-598-8345

* Key contact name and title: Robert Carucci, Partner, Cell number -SSSSSSS
* Person authorized to contractually bind the organization for any proposal against RFP: Robert Carucci
* Brief Background:

Year established: 1991

Number of years your company has been offering Information Security Testing: 15 years