# Meeting Compliance Efforts with the Mother of All Control Lists (MOACL)

GIAC (G7799) Gold Certification

Author: Tim Proffitt, tim@timproffitt.com

Advisor:
Becky Thurmond Fowler

Accepted:

## Abstract

*For many security teams, compliance activities can take significant time and resources. Organizations meeting multiple compliance efforts such as ISO 27000, Sarbanes Oxley Act, HIPAA or Gramm-Leach Bliley may find they are performing these activities year round. Technology practitioners should find mechanisms to better manage efforts and consolidate where possible. This paper will provide background on many of the compliance efforts organizations could grapple with and how the creation of a "Mother of All Control Lists" (MOACL) could ease redundant efforts. The goal for the organization will be to have the MOACL map directly to each of the organizations compliance controls to reduce duplicate efforts and over testing.*

## 1. Introduction

With the multitude of different compliance efforts an organization could be subjected to, it is not uncommon to hear confusion on what may or may not apply. What compliance regulations does the organization fall under? What must the organization do to meet a specific compliance effort and not conflict with a separate one? How can the organization know it is meeting required compliance controls? Can anything be done to reduce the amount of work needed to meet these objectives? The answers lay in the details of the many controls of each of these efforts and the ability for technology practitioners to find commonalities that will ease redundant testing. By reviewing each of the compliance frameworks, technologists can define a set of generic controls such that when a control is met for one objective it can meet additional objectives in other compliance frameworks. The creation of the Mother of all Control Lists (MOACL) will be a one-to-many relationship between a general control and varying compliance controls.

## 2.0 Sarbanes Oxley Act of 2002

### 2.1 A description of Sarbanes Oxley:

The Sarbanes Oxley Act of 2002 (SOX), also known as the 'Public Company Accounting Reform and Investor Protection Act' is a US federal law brought about as a reaction to a number of corporate accounting scandals involving Enron, Tyco and World Com. The act, named after U.S. Senator Paul Sarbanes and U.S. Representative Michael G. Oxley, contains 11 sections and requires the Securities and Exchange Commission to implement rulings on requirements to comply with the new law. The act created the Public Company Accounting Oversight Board (PCAOB) charged with overseeing, regulating, inspecting and disciplining accounting organizations in their roles as auditors of public companies. SOX covers issues such as auditor independence, corporate governance, internal control assessment and enhanced financial disclosure (U.S. Securities and Exchange Commission, 2002).

### 2.2 The applicability of Sarbanes Oxley:

Applicability for SOX legislation falls on all U.S. publicly traded companies, company boards, management and public accounting firms.

### 2.3 Enforcement and Penalties under Sarbanes Oxley:

There are two sections on this law that pertain to penalties. Section 802(a) states whoever knowingly alters, destroys, mutilates, conceals, covers up, falsifies, or makes a false entry in any record, document, or tangible object with the intent to impede, obstruct, or influence the investigation or proper administration of any matter within the jurisdiction of any department or agency of the United States or any case filed under title 11, or in relation to or contemplation of any such matter or case, shall be fined under this title, imprisoned not more than 20 years, or both.

Section 1107 states whoever knowingly, with the intent to retaliate, takes any action harmful to any person, including interference with the lawful employment or livelihood of any person, for providing to a law enforcement officer any truthful information relating to the commission or possible commission of any federal offense, shall be fined under this title, imprisoned not more than 10 years, or both (U.S. Securities and Exchange Commission, 2002).

### 2.4: Sarbanes Oxley control details:

Section 404 of SOX is most relevant to technology practitioners. This section requires management and the external auditor to report on the adequacy of the company's internal control over financial reporting. Management is required to produce an internal control report as part of each annual SOX report. To do this, managers are generally adopting an internal control framework such as COSO, COBIT, ISO and ITIL. Both management and an external auditor are responsible for performing their assessment in the context of a top-down risk assessment. The standard requires management to:

- Assess internal controls related to significant material misstatement risks
- Understand the flow of transactions (technology included)
- Evaluate company-level controls
- Perform a fraud risk assessment
- Evaluate controls designed to prevent or detect fraud
- Evaluate controls over the financial reporting process duration
- Scale the assessment based on the size and complexity of the company
- Conclude on the adequacy of internal controls

## 3.0 ISO 27002

### 3.1 A description of ISO27002

ISO/IEC 27002 is part of a growing family of ISO/IEC ISMS standards. The 27000 series is an information security standard published by the International Organization for Standardization. ISO/IEC 27002 provides best practice recommendations on information security management for use by those who are responsible for initiating, implementing or maintaining Information Security Management Systems (ISMS).

### 3.2 The applicability of ISO 27002:

The 27000 series provides best practices in information security management, risks and controls within the context of an overall Information Security Management System (ISMS). Any organization can choose to follow the ISO 27002 framework and ultimately receive certification. There are no requirements at this time that any organization must obtain this status. However, the ability to present the ISO 27002 certification to partners, customers or clients can be an advantage when presenting how sensitive data will be protected.

### 3.3 Enforcement and Penalties under ISO 27002:

Since there are no requirements that make organizations adhere to the ISO 27000 series framework, one will not find any penalties for not implementing the standards.

### 3.4: ISO 27002 control details:

The ISO technology controls are generally configured into 12 high level domains (Hoelzer, 2008):

- Risk Assessment
- Policy
- Organizational Security
- Asset Management
- Human Resources
- Physical and Environmental
- Communications and Operations Management
- Access Control

- System Development and Maintenance
- Security Incident Management
- Business Continuity
- Compliance and Regulations

## 4.0 HIPAA

### 4.1 A description of HIPAA

The Health Insurance Portability and Accountability Act (HIPAA) was enacted in 1996. Title I of HIPAA protects health insurance coverage for workers and their families when they change or lose their jobs. Title II of HIPAA requires the establishment of national standards for electronic health care transactions and national identifiers for providers, health insurance plans, and employers. The intention was to help people keep their medical information private. HIPAA contains two separate sets of rules: the Security Rule and the Privacy Rule. While the Privacy Rule pertains to all Protected Health Information (PHI) including paper and electronic, the Security Rule deals specifically with Electronic Protected Health Information (EPHI) and will be the section an information practitioner will be most interested.

### 4.2 The applicability of HIPAA:

The HIPAA regulates the use and disclosure of certain information held by "covered entities". Covered entities are defined as health care clearinghouses, employer sponsored health plans, health insurers, and medical service providers (Beaver, 2004).

### 4.3 Enforcement and Penalties under HIPAA:

Health and Human Services (HHS) issued a Final Rule regarding HIPAA enforcement on March 16, 2006. The Enforcement Rule sets civil money penalties for violating HIPAA rules and establishes procedures for investigations and hearings for HIPAA violations.

### 4.4: HIPAA control details:

HIPAA defines three types of security safeguards required for compliance: administrative, physical, and technical. For each of these various security standards, it names both required and addressable implementation specifications. Required specifications must be adopted and administered. Addressable specifications are more flexible. Individual organizations can evaluate the best way to implement addressable specifications. The standards and specifications are as follows (Amatayakul, 2004):

Administrative Safeguards

- Create privacy procedures
- Designate a privacy officer
- Policies must reference oversight and buy-in to the security controls
- Procedures should clearly identify employees who will have access to ePHI
- Address authorization, establishment, modification, and termination of access
- Provide ongoing training regarding the handling of ePHI
- Ensure vendors comply with HIPAA requirements
- Have a contingency plan in place for responding to disaster scenarios
- Establish disaster priority, failure analysis, testing, and change control
- Identify potential security violations
- Identify procedures for responding to security breaches

Physical Safeguards

- Controls for installation and destruction of hardware
- Access should be carefully controlled and monitored
- Limit access to properly authorized individuals
- Maintain facility security plans, maintenance records, and visitor sign-in
- Address proper workstation use
- Train contractors on their physical access responsibilities

Technical Safeguards

- Protect systems housing PHI from intrusions
- Utilize encryption when information flows over open networks
- Ensure data within its systems has not been altered by unauthorized means
- Perform data corroboration, including the use of check sum, double-keying, message authentication, and digital signature to ensure data integrity

- Authenticate entities a covered entity communicates with
- Make documentation of HIPAA practices available to HHS
- Document configuration settings on the components of the network
- Document risk analysis and risk management programs

## 5. PCI DSS

### 5.1 A description of PCI DSS

The Payment Card Industry Data Security Standard (PCI DSS) is a security standard assembled by a group of major credit card providers. The objective of the standard was to prevent credit card fraud through better controls around credit card data.

### 5.2 The applicability of PCI DSS:

PCI DSS applies to all organizations which hold, process, or pass cardholder information from any of the credit card brands taking part in the standard (Master Card, Visa, American Express, and Discover). Compliance can be audited either internally or externally, depending on the number of card transactions. Compliance must be assessed annually. Organizations handling large volumes of transactions must have their compliance assessed by an independent assessor known as a Qualified Security Assessor (QSA). Organizations handling smaller volumes have the option of self-certification via a Self-Assessment Questionnaire (Security Standards Council, 2008).

### 5.3 Enforcement and Penalties under PCI DSS:

Compliance is enforced by the PCI DSS member body. In the case of third party suppliers such as hosting companies who have business relationships with in-scope organizations, enforcement of compliance falls to the in-scope company, as neither the acquirers nor the card brands will have appropriate contractual relationships in place to mandate compliance. Non-compliant companies risk losing their ability to process credit card payments and being audited and/or fined.

### 5.4: PCI DSS control details:

The PCI DSS technology controls, at a high level, are configured into 12 domains and often referred to as the "dirty dozen". Each of these controls breaks down into several detailed sub-controls.

- Maintain a firewall configuration to protect cardholder data
- Do not use defaults for passwords and other security
- Protect stored cardholder data parameters
- Encrypt transmission of cardholder data across public networks
- Use and regularly update anti-virus software on all systems
- Develop and maintain secure systems and applications
- Restrict access to cardholder data by business need-to-know
- Assign a unique ID to each user
- Restrict physical access to cardholder data
- Track and monitor all access to network resources and cardholder data
- Regularly test systems and processes
- Maintain a policy that addresses information security

## 6. SAS70 Type II

### 6.1 A description of SAS70

Statement on Auditing Standards No. 70 (SAS70) is an auditing statement issued by the Auditing Standards Board of the American Institute of Certified Public Accountants (AICPA). SAS 70 defines the standards used by an auditor to assess the internal controls of an organization and issue a report. There are two types of SAS70 reports. A Type I report includes opinion on the fairness of the presentation and suitability of the organization's controls in operation (Coolidge, 2009). A Type II report includes the information contained in a Type I report but also includes the auditor's opinion on whether the specific controls were operating effectively during the period under review. Typically organizations interested in providing SAS70 reports will perform biannual or annual reviews.

### 6.2 The applicability of SAS70:

Typically, entities that provide outsourcing services that impact the control environment of their customers warrant the need to perform a SAS70. Examples of these types of organizations are insurance and medical claims processors, trust companies, hosted data centers, application service providers (ASPs), managed security providers, credit processing organizations and clearinghouses.

### 6.3 Enforcement and Penalties under SAS70:

Since SAS70 are voluntarily conducted by the organization, there is no enforcement element. The penalty for failing a SAS70 audit will be a disclosure element and a report detailing failed controls.

### 6.4: SAS70 control details:

Under a SAS 70, organizations are responsible for describing their controls and defining their control objectives. There is no published list of SAS70 controls. Control objectives are specific to the organization and its customers. However, most companies will rely on other sources of published standards, such as CoBit, that can be used to prepare for a SAS70 audit.

## 7.0 GLBA

### 7.1 A description of GLBA

The Gramm–Leach–Bliley Act (GLBA) is an act of the US Congress (1999–2001). GLBA allowed commercial banks, investment banks, securities firms and insurance companies to consolidate. The law was passed to legalize financial mergers on a permanent basis. Under the GLBA, financial institutions must provide their customers a privacy notice that details what data the company gathers about the client, where this data is shared, and how the company safeguards that data.

### 7.2 The applicability of GLBA:

GLBA defines financial institutions as companies that offer financial products or services to individuals, like loans, financial or investment advice, or insurance.
The company must be considered significantly engaged in the financial service or production that defines them as a financial institution (Federal Trade Commission, 2002).

### 7.3 Enforcement and Penalties under GLBA:

GLBA calls for severe civil and criminal penalties for noncompliance, including fines and even imprisonment. The financial institution shall be subject to a civil penalty of not more than $100,000 for each violation and the officers and directors of the financial institution shall be subject to, and personally liable for, a civil penalty of not more than $10,000 for each violation. The Federal Trade Commission (FTC) has jurisdiction over financial institutions and would be the governing body levying any penalties.

### 7.4: GLBA control details:

GLBA requires financial institutions to develop a written information security plan that describes how the company protects clients' nonpublic personal information. This security plan must:

- Designate at least one employee to manage the safeguards
- Develop a risk management methodology for areas handling customer data
- Develop, monitor, and test a program to secure the information
- Change the safeguards as needed with the changes in how information is collected, stored, and used

## 8.0 US State Compliance Regulations

### 8.1 A description of Compliance State Laws

In the US, each state can have a separate set of compliance efforts in addition to the federal level. On the whole, a majority of control overlap exists between the state laws. Since the states standards are generally based on best practices they appear consistent but practitioners need to be aware of the number of controls that are unique. An example of this is the newly implemented Mass 201 CMR 17 state law that implements a control that requires organizations housing sensitive data on mobile devices such as cell phones to provide encryption on the device (201 CMR 17.00 Standards, 2009).

### 8.2 The applicability of State Laws:

The applicability for state regulations can apply to several situations. In many of the cases the law applies if your organization does business in the state, has customers in the state or has employees residing in the state. This can change and the organization should have a clear understanding of what each state requires for its business practices.

### 8.3 Enforcement and Penalties under State laws:

Enforcement and penalties for state laws vary according to the legislation. When an organization fails to comply there are several outcomes: there can be monetary fines based on number of events, the Attorney General can launch investigations and the organization can incur the cost of mailing notification letters to those affected. To provide an example for this paper the Massachusetts Personal Information Law 201 CMR 17.00 will be used. Under this law penalties include:

- Maximum fine of $5,000 per violation of the law
- Up to $50,000 per improper disposal of technology equipment
- The Massachusetts Attorney General can launch an investigation

### 8.4: State Laws control details: Mass 201 CMR 17

The Mass 201 CMR 17 compliance effort requires organizations to report they meet the control details below (201 CMR 17.00 Standards, 2009).

- Designating one or more employees to maintain the security program
- Identifying and assessing reasonably foreseeable internal and external risks
- Developing security policies for employees
- Imposing disciplinary measures for infractions
- Preventing terminated employees from gaining accessing to the systems
- Taking all reasonable steps to verify that any third-party service provider with access to personal information has the capacity to protect such personal information
- Limiting the amount of personal information collected to that necessary to accomplish the purpose for which it is collected
- Limiting the time such information is retained to that reasonably necessary to accomplish such purpose

- Limiting access to those persons who are reasonably required to know such information in order to accomplish such purpose
- Identifying paper, electronic and other records, computing systems, and storage media, including laptops and portable devices used to store personal information so that it can be properly protected
- Provide reasonable restrictions upon physical access to records
- Conduct regular monitoring to ensure that the comprehensive information security program is operating
- Reviewing the scope of the security measures at least annually
- Documenting actions taken with security incidents and review the events and actions taken
- Utilize unique identifier technologies
- Control passwords to ensure that they are kept in a location that does not compromise the security of the data they protect
- Restrict access to active users and active user accounts only
- Block access to users after multiple unsuccessful attempts to gain access
- Restrict access to records and files containing personal information to those who need such information to perform their job duties
- Do not utilize vendor supplied default passwords
- To the extent technically feasible, encryption of all transmitted records and files containing personal information that will travel
- Reasonable monitoring of systems, for unauthorized use of or access to personal information
- Encryption of all personal information stored on laptops or other portable devices
- For files containing personal information on a system that is connected to the Internet, there must be reasonably up-to-date firewall protection and operating system security patches, reasonably designed to maintain the integrity of the personal information
- Reasonably up-to-date versions of system security agent software
- Implement security and awareness training

## 9. Other regulations

The list of compliance efforts can be staggering; especially organizations that have a global reach. There are many other significant compliance efforts that could be included in this type of matrix such as FISMA, HITECH Act, NERC, DCID 6-3, Basel II, Memo22, NISPOM or EU directive 2006/24/EC. For the objective of this paper, the MOACL will use the compliance efforts detailed in the sections above. Regardless of the regulation needed, organizations will find the controls can be integrated into a MOACL or become a new general control.

## 10. The Creation of a General Compliance Control (GCC)

The key ingredient in the creation of the MOACL is the general compliance control. The general compliance control (GCC) list will vary from one organization to another due to the differing applicability of the above compliance standards. A GCC in this paper will be defined as a best practice control for the organization. Since the majority of the compliance frameworks in this paper are based on best practices, it is reasonable to see how these GCC can be easily formulated. To begin the creation of the GCC list, organizations can benefit from initially aligning GCC controls with a known body of work such as ISO 27002 or ITIL. By utilizing the sections of a best practices framework organizations can align, remove or fill in the gaps where required by the organization's existing policies and procedures. At the end of the effort the organization will have a comprehensive list of general controls. When the finalized GCC list has been audited and evidence provided, organizations will see that they have completed the requirements for several compliance efforts with greater efficiency than in previous efforts.

## 11. Mapping compliance controls to GCC

Aligning compliance controls with a GCC list can be tricky and most likely different for each organization. Organizations dealing with electronically protected health information (ePHI) in the United States will have different GCC than an organization in the financial sector. A financial organization would be different than a European manufacturing company.

Take the creation of a GCC that states, "*The organization will implement mandatory security and awareness training for all employees. The training will be administered at least annually and* *will encompass new material as new security threats arise".* The above general control can be mapped to the ISO section 4.4.2, HIPAA 164.308(a)(5), a typical SOX entity control, and 201 CMR 17.03.2a. By auditing the organization's security training and obtaining sufficient evidence the control is being met, the above 4 compliance requirements were all fulfilled.

A second example would be the creation of a GCC that sates, "*The organization will maintain procedures for terminating access to information systems when the employment of a workforce member has ended. Termination of access will be prompt and will include deactivating usernames and passwords".* This general control would meet the efforts outlined in ISO section 4.2.3, HIPAA 164.308(a)(3)(ii)(B), 201 CMR 17.03.4, and most organization's SOX and SAS70 control elements. Conducting an audit to provide evidence of the policies and procedures for terminating access of workforce members for this general control would have fulfilled 5 compliance requirements.

A third example would be a GCC that states, "*The organization will implement security measures to ensure that electronically transmitted information is not improperly modified without detection. Sensitive information will be encrypted during transfer across public systems*". Evidence provided for this GCC will meet compliance efforts in ISO 6.9.1, HIPAA 164.312(e), PCI DSS 4.1, PCI DSS 4.1.1, GLBA 314.4(b)(2), Mass CMR 17.04.3, a general SOX control and a SAS70 control.

There are obvious GCC objectives that map across compliance efforts but organizations are likely to stumble onto objectives that are grey in where they would map in the MOACL. The development of the GCC list should be an iterative review process, by management, during each audit. Audit cycles should improve GCC wording or alter the MOACL matrix to best encompass the concept of the general compliance control. When a GCC becomes too wordy or cannot become specific enough while still meeting other compliance mappings, it may be time to create a new GCC.

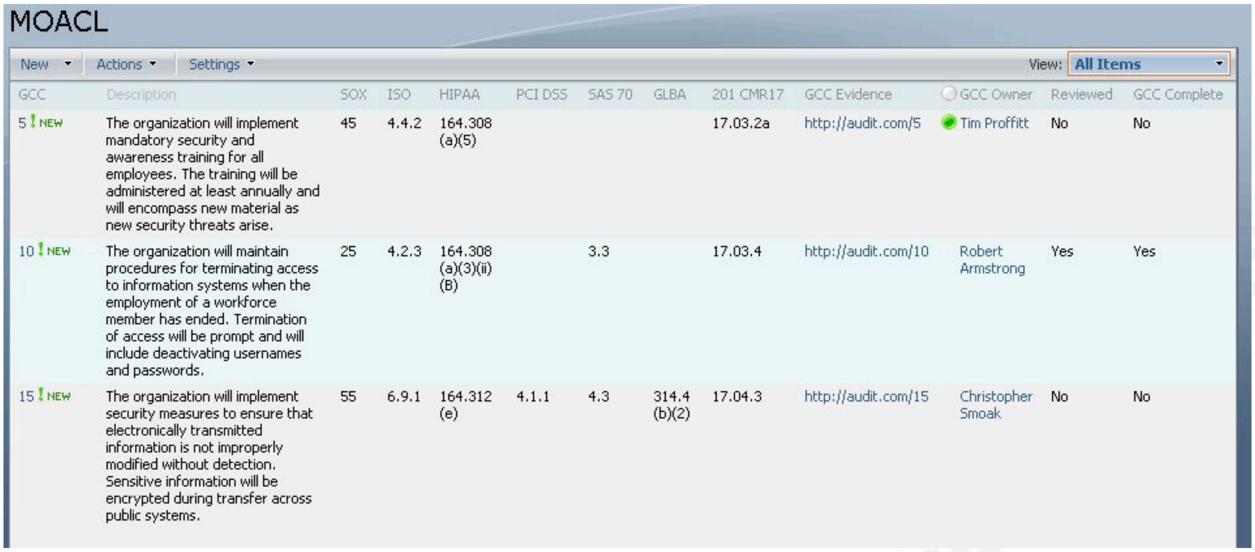
As organizations are building their matrix it will become apparent that some GCC will not map across multiple compliance controls. A good example for this is the ISO 7.3.3 clear desk policy.

Using the compliance efforts outlined in this paper the ISO 27002 is the only body listing this as a control. Although this may seem like a weak GCC, organizations should be aware that regulations and compliance efforts seem to continue to creep into our information systems. A GCC that does not necessarily map across multiple compliance efforts can still be a valuable control to your organization, especially when future legislation may require it. See Appendix A for an example MOACL.

When formulating the GCC and mapping compliance efforts to the MOACL, organizations should benefit from the inclusion of the proper subject matter experts, auditors and management team members to review the effort. Attempting to have just one body, such as the technology security team, complete the entire effort will most likely leave gaps in the matrix.

## 11. Using Microsoft SharePoint and MOACL in audit efforts.

The proper set of individuals or committee has been tasked with the MOACL project and has a completed GCC list for the organization. In many organizations a control list, not unlike the MOACL, begins its life as some form of spreadsheet or document. Although this type of document may provide basic functionality for smaller organizations that avoid change control issues, a larger organization should need a better solution. A superior method for utilizing the MOACL among multiple business units, departments and auditors is to utilize a custom list created on a Microsoft SharePoint Application..



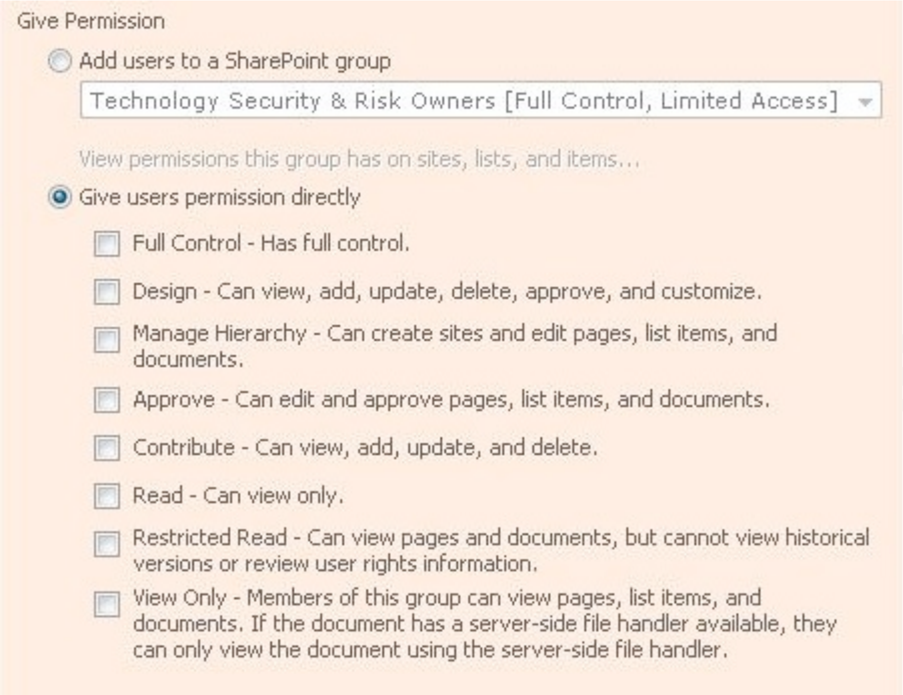
| GCC | Description | SOX | ISO | HIPAA | PCI DSS | SAS 70 | GLBA | 201 CMR17 | GCC Evidence | GCC Owner | Reviewed | GCC Complete |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 5 ! NEW | The organization will implement mandatory security and awareness training for all employees. The training will be administered at least annually and will encompass new material as new security threats arise. | 45 | 4.4.2 | 164.308 (a)(5) | | | | 17.03.2a | http://audit.com/5 | ● Tim Proffitt | No | No |
| 10 ! NEW | The organization will maintain procedures for terminating access to information systems when the employment of a workforce member has ended. Termination of access will be prompt and will include deactivating usernames and passwords. | 25 | 4.2.3 | 164.308 (a)(3)(ii) (B) | | 3.3 | | 17.03.4 | http://audit.com/10 | Robert Armstrong | Yes | Yes |
| 15 ! NEW | The organization will implement security measures to ensure that electronically transmitted information is not improperly modified without detection. Sensitive information will be encrypted during transfer across public systems. | 55 | 6.9.1 | 164.312 (e) | 4.1.1 | 4.3 | 314.4 (b)(2) | 17.04.3 | http://audit.com/15 | Christopher Smoak | No | No |

Figure 1: Custom SharePoint List

The advantage to the Microsoft SharePoint list is due to its wide deployment base, ease of use, and many built in features:

- authentication and authorization
- change control functionality
- versioning
- intuitive form interface
- ability to link to data repositories
- data extraction
- custom views
- workflow engine
- archive

The SharePoint infrastructure can utilize Microsoft active directory or an internal user directory for authentication. This allows the organization to implement the least access principle to the MOACL site. In addition to authentication, SharePoint allows for authorization to specific parts of the MOACL. For example, if an organization requests specific audit teams to see certain document repositories for evidence gathering, it can be configured. If certain auditors only need read only access or contribute only access that can be accomplished (Langfeld, 2004).



Give Permission

○ Add users to a SharePoint group

Technology Security & Risk Owners [Full Control, Limited Access]

View permissions this group has on sites, lists, and items...

● Give users permission directly

☐ Full Control - Has full control.

☐ Design - Can view, add, update, delete, approve, and customize.

☐ Manage Hierarchy - Can create sites and edit pages, list items, and documents.

☐ Approve - Can edit and approve pages, list items, and documents.

☐ Contribute - Can view, add, update, and delete.

☐ Read - Can view only.

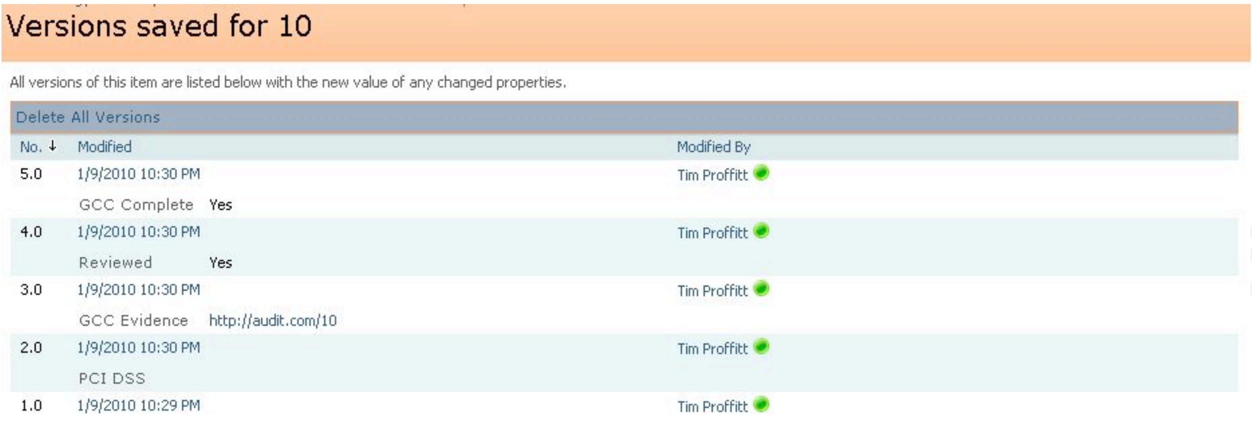
☐ Restricted Read - Can view pages and documents, but cannot view historical versions or review user rights information.

☐ View Only - Members of this group can view pages, list items, and documents. If the document has a server-side file handler available, they can only view the document using the server-side file handler.

**Figure 2: SharePoint Permissions**

The change control functionality inherent in SharePoint allows for multiple contributors to modify the MOACL simultaneously. Compliance efforts are typically group projects and for obvious reasons the GCC list will need to maintain its integrity during access by multiple parties. The backend database of SharePoint technology will allow for integrity to the GCC row level. When a user attempts to access an already open GCC, SharePoint will open a read only view and notify the recipient.

The versioning feature of SharePoint will allow auditors to determine who had created, modified, or removed a GCC. The versioning feature has the ability to rollback to previous versions if questions are raised about the integrity of the GCC data. The versioning is helpful when determining who made changes on what date and in what order.



Versions saved for 10

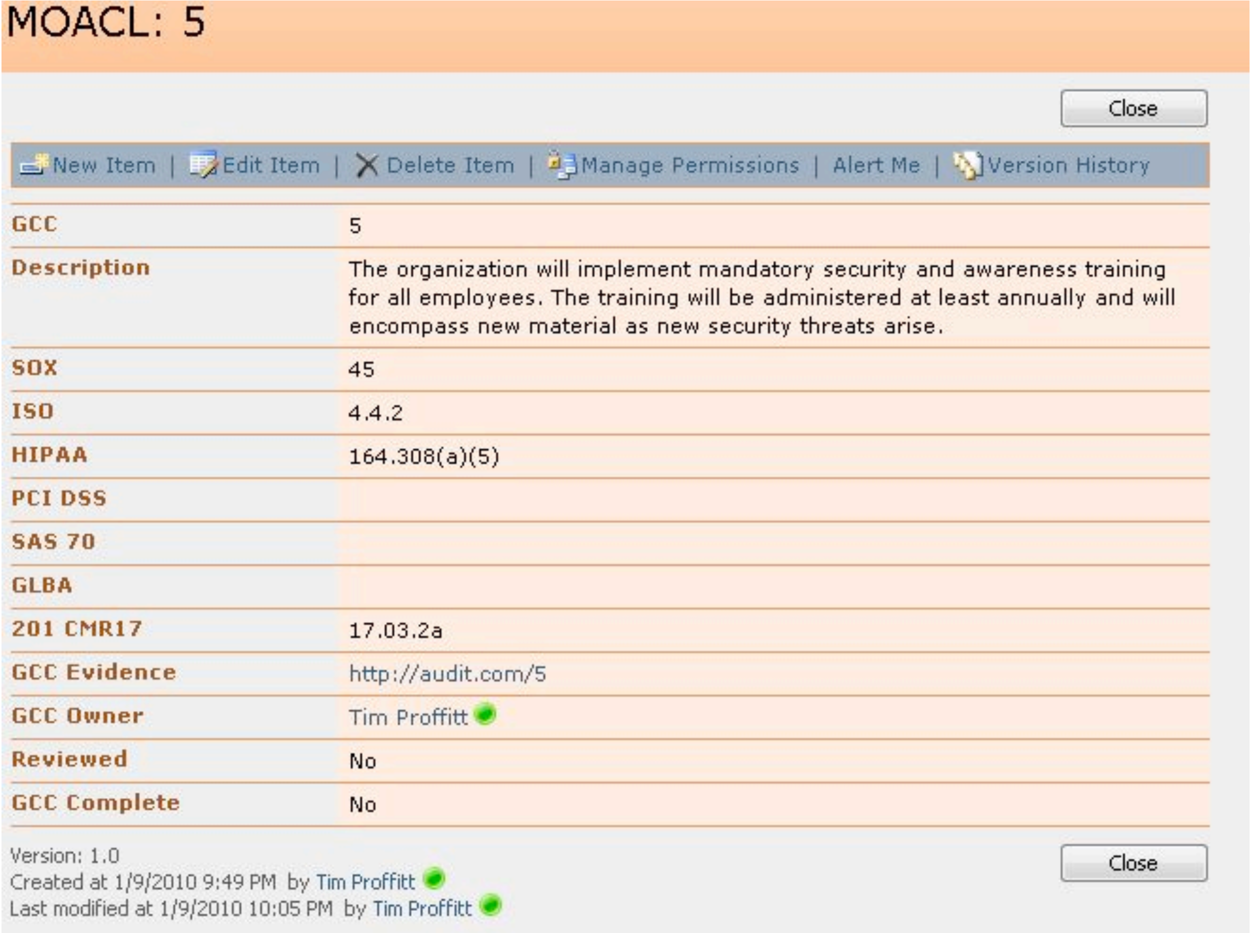
All versions of this item are listed below with the new value of any changed properties.

Delete All Versions

| No. ↓ | Modified | | Modified By |
|---|---|---|---|
| 5.0 | 1/9/2010 10:30 PM | | Tim Proffitt ● |
| | GCC Complete | Yes | |
| 4.0 | 1/9/2010 10:30 PM | | Tim Proffitt ● |
| | Reviewed | Yes | |
| 3.0 | 1/9/2010 10:30 PM | | Tim Proffitt ● |
| | GCC Evidence | http://audit.com/10 | |
| 2.0 | 1/9/2010 10:30 PM | | Tim Proffitt ● |
| | PCI DSS | | |
| 1.0 | 1/9/2010 10:29 PM | | Tim Proffitt ● |

**Figure 3: SharePoint Versioning Information**

By design, SharePoint has an intuitive interface. Each GCC is presented in a form interface that any auditor or non-technical user should be comfortable with. The additions of new compliance frameworks can be added to the MOACL with a few simple steps by a contributor. There is no programming requirement. A simple SharePoint wizard will guide you through the form building process.


MOACL: 5
Close
New Item | Edit Item | Delete Item | Manage Permissions | Alert Me | Version History
Close

| | |
|---|---|
| GCC | 5 |
| Description | The organization will implement mandatory security and awareness training for all employees. The training will be administered at least annually and will encompass new material as new security threats arise. |
| SOX | 45 |
| ISO | 4.4.2 |
| HIPAA | 164.308(a)(5) |
| PCI DSS | |
| SAS 70 | |
| GLBA | |
| 201 CMR17 | 17.03.2a |
| GCC Evidence | http://audit.com/5 |
| GCC Owner | Tim Proffitt |
| Reviewed | No |
| GCC Complete | No |

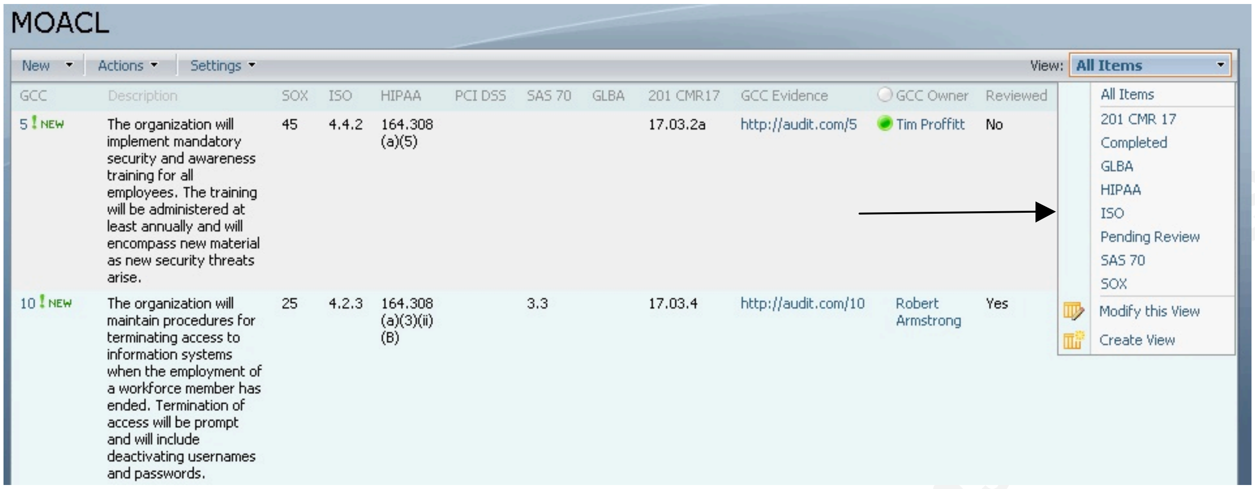
Version: 1.0
Created at 1/9/2010 9:49 PM by Tim Proffitt
Last modified at 1/9/2010 10:05 PM by Tim Proffitt

**Figure 4: SharePoint Simple Form Interface**

Since SharePoint is based on browser technology, linking to evidence repositories is simple. SharePoint can house document libraries in the same site as the MOACL and be referenced easily from the form. Reviewing the evidence for a GCC should be but a click away for anyone looking to review the audit.

The views feature that comes with a custom SharePoint list allows for the flexibility of presenting data. An organization may position itself so that groups interested in HIPAA objectives or GLBA objectives will have filtered views to those controls. Additionally, by utilizing the view features on the MOACL, a custom view can be crafted to show objectives such as completed GCC, controls in review, all GCC assigned to a specific owner, modified by a designated user, or controls not started.

Tim Proffitt, tim@timproffitt.com



| GCC | Description | SOX | ISO | HIPAA | PCI DSS | SAS 70 | GLBA | 201 CMR17 | GCC Evidence | GCC Owner | Reviewed |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 5 ! NEW | The organization will implement mandatory security and awareness training for all employees. The training will be administered at least annually and will encompass new material as new security threats arise. | 45 | 4.4.2 | 164.308 (a)(5) | | | | 17.03.2a | http://audit.com/5 | ● Tim Proffitt | No |
| 10 ! NEW | The organization will maintain procedures for terminating access to information systems when the employment of a workforce member has ended. Termination of access will be prompt and will include deactivating usernames and passwords. | 25 | 4.2.3 | 164.308 (a)(3)(ii) (B) | | 3.3 | | 17.03.4 | http://audit.com/10 | Robert Armstrong | Yes |

**Figure 5: SharePoint Views**

The powerful workflow engine provided by Microsoft SharePoint services can be utilized in the auditing effort. Any item in the MOACL can have a workflow attached. The SharePoint workflows are very similar to Outlook rules and provide basic routing, approval systems and notifications right out of the box. By assigning workflows to a GCC, an overseer can automatically receive emails when a condition is met, require approval to enter data, or the workflow can move data to an alternate destination (Janus, 2007). Leveraging the workflow engine for notification events, i.e. when something has been completed, is a feature that should be popular with management overseeing the project.

The ability to archive an annual audit is typically a requirement by the compliance regulations. Some regulations such as HIPAA require the audit data to be archived for 7 years. The ability to quickly revisit the previous year's results is typically a requirement of the organization. By utilizing SharePoint for the MOACL, the entire site containing the custom list, workflow engine, data repositories and any other library created can be rolled into an archive state. The effort to roll the MOACL into a new year would consist of making a copy of the MOACL repository (a feature of SharePoint), renaming the repository for a new year and setting the old copy to a read only access for the user base. The site administrator would then simply clear the GCC answers for the new audit cycle.

Tim Proffitt, tim@timproffitt.com

## 12. Conclusion

Auditing compliance efforts can take valuable technology resources away from daily tasks. Although these efforts may be seen as a necessary evil by administrators, the duplication of compliance auditing should not be. Duplicating auditing efforts can confuse users, lower morale, and simply waste resources. Mapping commonalities between the organization's compliance efforts into a single general control list can have significant improvement in the audit cycle. By utilizing the MOACL in SharePoint, organizations can streamline their compliance efforts to optimize resources, time and ultimately save money for the organization.

## References

U.S. Securities and Exchange Commission (July 2002). Public Law 107-204. Retrieved from http://www.sec.gov/about/laws/soa2002.pdf

Hoelzer David (2008). *SANS 17799/27001 Security and Audit Framework*. Book 1, Page 45.

Amatayakul Margret, Lazarus Steven (2004). *Complete Guide to HIPAA Security Risk Analysis: A Step By Step Approach.*

Beaver Kevin, Herold Rebecca (2004). *The Practical Guide to HIPAA Privacy and Security Compliance*.

Security Standards Council (2008). PCI DSS New Self-Assessment Questionnaire (SAQ) Summary. Retrieved from https://www.pcisecuritystandards.org/saq/index.shtml

Coolidge Scott (2009). *SAS 70 Overview*. Retrieved from http://www.sas70.com/about.htm#about 100

Federal Trade Commission (May 2002). Final Rule, Federal Register. Retrieved from http://www.ftc.gov/os/2002/05/67fr36585.pdf

201 CMR 17.00 Standards for the Protection of Personal Information of Residents of the Commonwealth. (2009). Retrieved from http://www.mass.gov/Eoca/docs/idtheft/201CMR1700reg.pdf

Langfeld Lynn, Spence Colin, Noel Michael (2004). *Microsoft SharePoint 2003 Unleashed*. Chapter 8.

Philo Janis (2007). *Pro InfoPath 2007*

Tim Proffitt, tim@timproffitt.com

# Appendix A

## Example of the Mother of All Control Lists

| GCC | Control Description | ISO 27002 | SOX | HIPAA | PCI DSS | SAS70 | GLBA | 201 CMR 17 |
|---|---|---|---|---|---|---|---|---|
| **POLICY** | | | | | | | | |
| 1.1 | The organization will maintain a security policy framework. | 1.1 Information Security Policy | 08-SOX - Entity Control | Sanction Policy §164.308(a)(1) | PCI 12.1.1<br>PCI 12.2<br>PCI 12.3 | | | |
| 1.2 | The organization will maintain a high level security policy that displays managements backing. | 1.1.1 High Level Security Policy (HLSP) | | | | | | |
| 1.3 | The security policy framework is reviewed / evaluated on a periodic basis. | 1.1.2 Review and Evaluation | 09-SOX - Entity Control | | PCI 12.1.2<br>PCI 12.1.3 | | | |
| 1.4 | Organization has assigned responsibility for security to an individual or committee. | | 10-SOX - Entity Control | Assigned Security Responsibility §164.308(a)(2) | PCI 12.3.1 | | § 314.4(a) | CMR 17.03.1 |
| **ORGANIZATIONAL SECURITY** | | | | | | | | |
| 2.1 | Organizations will maintain current organizational charts. | 2.1 Internal organization | | | | | | |
| 2.2 | Management will show commitment to the security program and it's efforts. | 2.1.1 Management commitment | | | | | | |
| 2.3 | | 2.1.2 Information security coordination | | | | | | |
| 2.4 | Implement procedures for the authorization and supervision of workforce members who work with sensitive data. Roles should be clearly defined. | 2.1.3 Allocation of responsibilities | | Authorization and/or Supervision §164.308(a)(3) | | | | |
| 2.5 | Procedures will be in place that requires the proper authorization of computing resources before they are allowed in the production environment. | 2.1.4 Authorization for facilities | | | | | | |
| 2.6 | The organization will utilize confidentiality agreements to protect it's information resources. | 2.1.5 Confidentiality Agreements | | | | | | |
| 2.7 | The organization will commit to maintain a relationship with local and federal authorities. | 2.1.6 Contact with Authorities | | | | | | |
| 2.8 | The organization utilizes SME advice for new projects or major program changes. | 2.1.7 Specialist Security Advice | | | | | | |
| 2.9 | Major projects will perform independent review to help reduce risk. | 2.1.8 Independent Review | | | | | | |
| 2.10 | | 2.2 External Parties | 07-SOX - Data | | | | | |

Tim Proffitt, tim@timproffitt.com

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | Recovery | | | | | |
| 2.11 | Organizations will conduct periodic Risk Analysis efforts.<br>Identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks. At a minimum, such a risk assessment should include consideration of risks in each relevant area of your operations, including: | 2.2.1 risk assessment | | Risk Analysis §164.308(a)(1) | | | § 314.4 (b)<br>§ 314.4 (e) | CMR 17.03.2.c<br>CMR 17.03.11 |
| 2.12 | Organizations will remediate risks identified by the RA activities | | | Risk Management §164.308(a)(1) | | | § 314.4 ( c) | |
| 2.13 | Organizations will maintain policies for third party access into the network. | 2.2.2 third party access | | | | | | |
| 2.14 | Organizations will maintain policies for the outsourcing of resources. | 2.2.3 outsourcing | 08-SOX - Data Recovery | | | | | |
| **ASSET MANAGEMENT** | | | | | | | | |
| 3.1 | Organization identifies paper, electronic and other records, computing systems, and storage media, including laptops and portable devices used to store personal information, to determine which records contain personal information, except where the comprehensive information security program provides for the handling of all records as if they all contained personal information | 3 Assets | | | PCI 9.9.1 | | | CMR 17.03.8 |
| 3.2 | Organization has security policies for employees that take into account whether and how employees should be allowed to keep, access and transport records containing personal information outside of business premises.<br>Reasonable restrictions upon physical access to records containing personal information, including a written procedure that sets forth the manner in which physical access to such records is restricted; and storage of such records and data in locked facilities, storage areas or containers | 3.1 Accountability | | | | | | CMR 17.03.3<br>CMR 17.03.9 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 3.3 | Media is labeled so it can be identified as a classification. | 3.2 Classification | | | PCI 9.7.1 | | | |
| 3.4 | Limit the amount of personal information collected to that reasonably necessary to accomplish the legitimate purpose for which it is collected | | | | | | | CMR 17.03.7 |
| **HR DOMAIN** | | | | | | | | |
| 4.1 | Security is clearly defined in Job descriptions | 4.1.1 Security Roles in job descriptions | 01-SOX - Entity Control | | PCI 1.1.4 | SAS 1.2 | | CMR 17.03.2b |
| 4.2 | Organization to determine that the access of a workforce member to specific classifications of electronic information is appropriate. | 4.1.2 Personnel Screening | 02-SOX - Entity Control | Workforce Clearance Procedure 164.308(a)(3) | | | | |
| 4.3 | Organization will clearly review and define terms and conditions. | 4.1.3 Terms and Conditions | | | | | | |
| 4.4 | Organization will monitor traffic leaving the perimeter for violations of policy. | 4.1.4 Egress Monitoring | 03-SOX - Entity Control | | | | | |
| 4.5 | Organizations will review internet activity for appropriate use. | 4.1.5 Appropriate Use Monitoring | 04-SOX - Entity Control | | | | | |
| 4.6 | Management's responsibilities to technology and security are clearly identified. | 4.2.1 Management Responsibilities | 05-SOX - Entity Control | | | | | |
| 4.7 | Implement a security awareness and training program for all members of the organization (including management). | 4.2.2 Security Awareness | 06-SOX - Entity Control | Security Awareness and Training 164.308(a)(5) | | | § 314.4(b)(1) | CMR 17.03.2a<br>CMR 17.04.08 |
| 4.8 | Implement periodic security updates such as quarterly email distribution or poster campaigns. | | | Security Reminders 164.308(a)(5) | | | | |
| | Organization has procedures for terminating access to electronic information when the employment of a workforce member ends<br>Preventing terminated employees from accessing records containing personal information by immediately terminating their physical and electronic access to such records, including deactivating their passwords and user names | 4.2.3 Disciplinary Process | 07-SOX - Entity Control | Termination Procedures 164.308(a)(3)(ii)(B) | | | | CMR 17.03.4<br>CMR 17.03.5 |
| **PHYSICAL AND ENVIRONMENTAL SECURITY** | | | | | | | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 5.1 | Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.<br>Maintain strict control over the internal or external distribution of any kind of media that contains cardholder information: | 5.1.1 Physical Security Perimeter | 01-SOX - Data Center Ops | Facility Security Plan 164.310(a) | PCI 9.1<br>PCI 9.6<br>PCI 9.7<br>PCI 9.9 | | | CMR 17.04.2a |
| 5.2 | Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.<br>Organization will utilize equipment such as cameras and visitor logs. | 5.1.2 Physical Entry Controls | 02-SOX - Data Center Ops | Access Control and Validation Procedures 164.310 (a) | PCI 9.1.1<br>PCI 9.2<br>PCI 9.3<br>PCI 9.4 | SAS 4.2 | | |
| 5.3 | Access to the data center, computer room, and sensitive areas of the operations center is controlled through electronic key cards assigned to appropriate employees. | 5.1.3 Secure offices, rooms and facilities | 03-SOX - Data Center Ops | | | SAS 4.1 | | |
| 5.4 | The data center is equipped to prevent, detect, and suppress environmental factors, such as raised floors, air conditioning, fire and smoke detectors, and fire suppressant systems. | 5.1.4 Protecting Against External and Environ | 04-SOX - Data Center Ops | | | SAS 4.3 | | |
| 5.5 | Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a workstation or class of workstation that can access electronic information. | 5.1.5 Working in Secure Areas | 05-SOX - Data Center Ops | Workstation Use 164.310 (c) | | | | |
| 5.6 | Organization will have procedures for securing loading/delivery areas. | 5.1.6 Isolated delivery and loading areas | 06-SOX - Data Center Ops | | | | | |
| 5.7 | Organization will maintain procedures for the proper placements and physical security of technology equipment. | 5.2.1 Equipment sitting and protection | 09-SOX - Data Recovery | | | | | |
| 5.8 | Redundant/fault tolerant power supplies should be utilized where feasible. | 5.2.2 Power Supplies | 10-SOX - Data Recovery | | | | | |

Tim Proffitt, tim@timproffitt.com

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 5.9 | Restrict physical access to publicly accessible network infrastructure. (Wireless included) | 5.2.3 Cabling Security | 07-SOX - Data Center Ops | | PCI 9.1.2<br>PCI 9.1.3 | | | |
| 5.10 | Implement policies to maintain and document repairs to physical components. | 5.2.4 Equipment maintenance | 08-SOX - Data Center Ops | Maintenance Records 164.310(a) | | | | |
| 5.11 | Management approves all media that is moved from a secured area (especially when media is distributed to individuals). Media back-ups will be stored in a secure off-site facility, which may be either an alternate third-party or a commercial storage facility. | 5.2.5 Security of Equipment Off-Premises | 09-SOX - Data Center Ops | | PCI 9.5<br>PCI 9.8 | | | |
| 5.12 | Policies and procedures to address the final disposition of reuse of electronic hardware or electronic media on which it is stored.<br>Purge, degauss, shred, or otherwise destroy electronic media so that cardholder data cannot be reconstructed. | 5.2.6 Secure Disposal/ Reuse of Equipment | 10-SOX - Data Center Ops | Disposal 164.310(d)<br>Media Re-use 164.310(d) | PCI 9.10<br>PCI 9.10.1<br>PCI 9.10.2 | | | |
| 5.13 | Organization has procedures for removing technology property when it is no longer in a production capacity. | 5.2.7 Removal of Property | 11-SOX - Data Center Ops | | | | | |
| **COMMUNICATIONS AND OPERATIONS MANAGEMENT** | | | | | | | | |
| 6.1 | Organization will have specific procedures that explain exactly how systems are to be configured and operated. For example do not use vendor supplied passwords. | 6.1.1 Documented Operating Procedures | 01-SOX - Network Security | | PCI 1.1.9<br>PCI 2.1<br>PCI 2.2<br>PCI 6.3.6 | | | |
| 6.2 | Change control procedures will be followed for changes in infrastructure. | 6.1.2 Operational Change Controls | 12-SOX - Data Center Ops | | | | | |
| 6.3 | Management's control consciousness and organization structure provides for adequately segregated duties within information systems and between information systems and users. | 6.1.3 Segregation of duties | 06-SOX - Data Recovery | | | SAS 1.1 | | |
| 6.4 | Development, Staging, Testing, Laboratory and Production environments will be separated by logical or physical means. | 6.1.4 Separation of development and operational facilities | 13-SOX - Data Center Ops | | PCI 6.3.2 | | | |
| 6.5 | Organization may permit a business associate to create, receive, maintain, or transmit electronic information on the entity's behalf only if the entity obtains satisfactory assurances that the business associate will appropriately safeguard the information. | 6.2.1 3rd party Service Delivery - Contract | | Business Associate Contracts and Other Arrangement 164.308 (b) | | SAS 7.2 | § 314.4 (d)(1)<br>§ 314.4 (d)(2) | CMR 17.03.6 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 6.6 | Periodic reports regarding services rendered and any records related to that service that pertains to information security of third parties is conducted. | 6.2.2<br>3rd Party Monitoring and Review | | Business Associate Contracts and Other Arrangement<br>164.308 (b) | | | § 314.4 (d)(1)<br>§ 314.4 (d)(1) | |
| 6.7 | Organization has policies and procedures for managing the changes involving 3rd parties. | 6.2.3<br>3rd Party Managing Changes | | Business Associate Contracts and Other Arrangement<br>164.308 (b) | | | | |
| 6.8 | Organization conducts capacity planning on production systems. | 6.3.1<br>Capacity Planning | 07-SOX - Data Recovery | | PCI 1.1.2 | | | |
| 6.9 | A mechanism exists for the acceptance of a system into the environment. Signoff is conducted by the proper management. | 6.3.2<br>System Acceptance | 02-SOX - Network Security | | | | | |
| 6.10 | Procedures and software exist for guarding against, detecting, and reporting malicious software. | 6.4.1<br>Controls Against Malicious Software | 01-SOX - Virus Control | Protection from Malicious Software<br>164.308(a)(5) | PCI 5.1<br>PCI 5.2 | | | CMR 17.04.7 |
| 6.11 | Organization has established clear controls around ACLS and firewall type technologies to protect information assets. | 6.6.1<br>Network Controls | 14-SOX - Data Center Ops | | PCI 1.1<br>PCI 1.1.1<br>PCI 1.1.3<br>PCI 1.1.5<br>PCI 1.1.6<br>PCI 1.1.7<br>PCI 1.2<br>PCI 1.3<br>PCI 1.4<br>PCI 11.4 | | | CMR 17.04.6 |
| 6.12 | Procedures exist for the secure handling of mass media such as tape backups and flash drives. | 6.7<br>Media Handling | 15-SOX - Data Center Ops | | | | | |
| 6.13 | Organization has policies and procedures for the exchanging of data with external parties. | 6.8.1<br>Exchange of Info and Software | 16-SOX - Data Center Ops | | | | | |
| 6.14 | Media will be sent via secured courier or a delivery mechanism that can be accurately tracked. | 6.8.3<br>Physical Media in Transit | 17-SOX - Data Center Ops | | PCI 9.7.2 | | | |
| 6.15 | Sensitive communications conducted over email is secured by a form of encryption. | 6.8.4<br>Security of electronic mail | 18-SOX - Data Center Ops | | PCI 4.2 | | | |
| 6.16 | Implement security measures to ensure that electronically transmitted information is not | 6.9.1<br>Electronic Commerce | 19-SOX - Data Center Ops | Integrity Controls<br>164.312 (e) | PCI 4.1<br>PCI 4.1.1 | | § 314.4(b)(2) | CMR 17.04.3 |

Tim Proffitt, tim@timproffitt.com

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | improperly modified without detection. | Security | | | | | | |
| 6.17 | Publically available systems are protected to ensure sensitive information is protected. | 6.9.3 Publicly Available Systems | 20-SOX - Data Center Ops | | | | | |
| 6.18 | Policies and procedures exist to create and maintain retrievable exact copies of electronic assets. | | 08-SOX - Data Recovery | Data Backup Plan 164.308(a)(7)<br>Data Backup and Storage 164.310 (d) | | | | |
| **ACCESS CONTROL** | | | | | | | | |
| 7.1 | Implement technical policies and procedures for electronic information systems that maintain information to allow access only to those persons or software programs that have been granted access rights as specified .<br>Limit access to those persons who are reasonably required to know such information in order to accomplish such purpose or to comply with state or federal record retention requirements. | 7.1 Access Control Policy | 02-SOX - Network Security | Access Control 164.308(a)(4) | PCI 3.1<br>PCI 3.3 | SAS 5.1 | | CMR 17.03.7 |
| 7.2 | Limit access to computing resources to only those individuals whose job requires such access. | 7.2 User Access Management | 03-SOX - Network Security | | PCI 7.2<br>PCI 7.2<br>PCI 8.1 | | | |
| 7.3 | Organization has policies and procedures for granting access to electronic assets. For example, through access to a workstation, transaction, program, process, or other mechanism. (requests, identify the role, approvals, statement of rights, unique ID) | 7.2.1 User Registration | 04-SOX - Network Security | Access Authorization 164.308(a)(4)<br>Unique User Identification 164.312 (a) | PCI 8.1<br>PCI 10.1 | SAS 5.3 | | CMR 17.04.1.a<br>CMR17.04.1.b<br>CMR 17.04.2b |
| 7.4 | Implement policies and procedures for granting access to electronic assets. for example, through access to a workstation, transaction, program, process, or other mechanism.<br>Ensure proper user authentication and password management for non-consumer users and administrators, on all system components | 7.2.2 Privilege Management | 05-SOX - Network Security | Access Authorization 164.308(a)(4) | PCI 8.5<br>PCI 8.5.16<br>PCI 10.5<br>PCI 10.5.1<br>PCI 10.5.2 | | | |

Tim Proffitt, tim@timproffitt.com

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 7.5 | Organization has procedures for creating, changing, and safeguarding passwords. Access to user identification is blocked after multiple unsuccessful attempts to gain access or the limitation placed on access for the particular system | 7.2.3 Password Management | 06-SOX - Network Security | Password Management 164.308 (a)(5) | PCI 8.2<br>PCI 8.3<br>PCI 8.4 | SAS 5.3<br>SAS 5.4 | | CMR 17.04.1.c<br>CMR 17.04.1.e |
| 7.6 | Organization has policies and procedures that review, and modify a user's right of access to a workstation, transaction, program, or process.<br>restricting access to active users and active user accounts only | 7.2.4 Review of Rights | 07-SOX - Network Security | Access Establishment and Modification 164.308(a)(4) | | SAS 5.2<br>SAS 5.5 | | CMR 17.04.1.d |
| 7.7 | User responsibilities are clearly documented and signed off by the user in an employee agreement. | 7.3 User Responsibilities | 02-SOX - Virus Control | | PCI 3.1 | | | |
| 7.8 | Maintain a record of the movements of hardware and electronic media and any person responsible therefore. | | | Accountability 164.310 (d) | | | | |
| 7.9 | Policies and procedures exist for the correct use and management of passwords. | 7.3.1 Password Use | 08-SOX - Network Security | | PCI 8.5.8<br>PCI 8.5.9<br>PCI 8.5.10<br>PCI 8.5.11<br>PCI 8.5.12<br>PCI 8.5.13<br>PCI 8.5.14<br>PCI 8.5.15 | | | CMR 17.04.1.c |
| 7.10 | Unattended equipment will be secured by timeouts, locking screens, logoffs, etc. | 7.3.2 Unattended Equipment | 09-SOX - Network Security | | | | | |
| 7.11 | Organizations will implement a clean desk policy to protect physical assets such as electronics and paper. | 7.3.3 Clear desk Policy | | | | | | |
| 7.12 | Clear policies exist detailing the use of network services and restrictions. | 7.4.1 Policy on Use of Network Services | 03-SOX - Virus Control | | | | | |
| 7.13 | Authentication will be required for any access across external or public networks. | 7.4.2 User authentication for external connections | 10-SOX - Network Security | | | | | |
| 7.14 | Workstations will be authenticated before they are allowed to access network resources. | 7.4.3 Node authentication | 11-SOX - Network Security | | | | | |
| 7.15 | Organization will implement security for the protection of side band or diagnostic ports in equipment. | 7.4.4 Remote diagnostic port protection | 12-SOX - Network Security | | | | | |
| 7.16 | Networks will be segmented where logically applicable. Segmentation will serve to protect information assets. | 7.4.5 Segregation in networks | 13-SOX - Network Security | | PCI 1.4 | | | |
| 7.17 | Processes are in place to control access to what is | 7.4.6 Network | 14-SOX - Network | | | | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | placed on the internal or external network. | connection control | Security | | | | | |
| 7.18 | Static and dynamic routing protocols will be managed by the appropriate individuals and with security as a priority. | 7.4.7 Network routing control | 15-SOX - Network Security | | | | | |
| 7.19 | Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation | 7.5 Operating system access control | 16-SOX - Network Security | Workstation Use 164.310 (b) | | | | |
| 7.20 | Use windows to restrict access to resources based on user or computer logon procedures, identification, password management, utilities, timeout, and connection time<br>Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed. | 7.5.1 terminal log-on procedures | 17-SOX - Network Security | Person or Entity Authentication 164.312(do) | | | | |
| 7.21 | Users will be authenticated using a industry standard, best practices method to ensure the account being utilized is the correct individual. | 7.5.2 User identification and authentication | 18-SOX - Network Security | | | | | |
| 7.22 | Organization will provide procedures for the management of passwords, recovery, and resets. | 7.5.3 Password Management System | 19-SOX - Network Security | | | | | |
| 7.23 | System utilities will only be used if authorized and are needed for the job. Utilities such as password crackers are forbidden. | 7.5.4 Use of system utilities | 20-SOX - Network Security | | | | | |
| 7.24 | Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity. | 7.5.5 Terminal time-out | 21-SOX - Network Security | Automatic Logoff 164.312 (a) | | | | |
| 7.25 | Implement electronic procedures that terminate an network session after a predetermined time of inactivity. | 7.5.6 Limitation of connection time | 22-SOX - Network Security | | | | | |
| 7.27 | Applications define controls around information accessed inside the application. | 7.5.8 Information access restriction | 24-SOX - Network Security | | | | | |
| 7.29 | Data will be isolated, depending on it's purpose, for sensitivity. De-identification is preferred. | 7.5.9 Sensitive system isolation | 25-SOX - Network Security | | | | | |

Tim Proffitt, tim@timproffitt.com

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 7.30 | Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports. Including: FW, individual user accesses to cardholder data, actions taken by any individual with root or administrative privileges, creation and deletion of system-level objects, date and time, etc.<br>Review logs for all system components at least daily. Log reviews should include those servers that perform security functions like Intrusion Detection System (IDS) and Authentication, Authorization, and Accounting (AAA) servers (for example, RADIUS). | 7.6.1 event logging | 26-SOX - Network Security | Information System Activity Review §164.308(a)(1) | PCI 1.1.8<br>PCI 10.2<br>PCI 10.6 | SAS 5.6 | | CMR 17.03.10<br>CMR 17.04.4 |
| 7.31 | Procedures for monitoring log-in attempts and reporting discrepancies. | | 27-SOX - Network Security | Log-in Monitoring 164.308(a)(5) | | | | |
| 7.32 | Synchronize all critical system clocks and times. | 7.6.1 clock synchronization | 28-SOX - Network Security | | PCI 10.4 | | | |
| 7.33 | Policies and procedures exist for the correct use of mobile computing devices such as laptops and smart phones. The mobile devices will be protected using encryption, authentication, templates, timeouts, etc. | 7.7.1 mobile computing | 29-SOX - Network Security | | | | | |
| 7.34 | Policies and procedures exist for the correct use of tele-working. | 7.7.2 Tele-working | 30-SOX - Network Security | | | | | |
| **SYSTEM DEVELOPMENT** | | | | | | | | |
| 8.1 | Develop applications based on secure coding guidelines and business requirements. | 8.1 Statement of Bus Requirements | 01-SOX - App Development | | PCI 6.3<br>PCI 6.5 | | § 314.4(b)(2) | |
| 8.2 | Implement electronic mechanisms to corroborate that electronic data has not been altered or destroyed in an unauthorized manner. | 8.2 Correct Processing In Applications | 02-SOX - App Development | Mechanism to Authenticate Electronic PHI 164.312(c) | PCI 6.5.1<br>PCI 6.5.2<br>PCI 6.5.3<br>PCI 6.5.4<br>PCI 6.5.5<br>PCI 6.5.6<br>PCI 6.5.7<br>PCI 6.5.8<br>PCI 6.5.9<br>PCI 6.5.10 | | | CMR 17.03.2.c |
| 8.3 | Application will validate data being submitted to the system to check for validity. | 8.2.1 Input data validation | 03-SOX - App Development | | | | | |
| 8.4 | Organization will have policies and procedures to ensure the | 8.2.2 Control of | 04-SOX - App | | | | | |

Tim Proffitt, tim@timproffitt.com

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | internal processing of applications is correct. | Internal Processing | Development | | | | | |
| 8.5 | Applications utilizing data exchange will use message authentication to maintain integrity. | 8.2.3 Message Authentication | 05-SOX - App Development | | | | | |
| 8.6 | Applications will validate the data being presented as output to ensure the data is correct. | 8.2.4 Output Data Validation | 06-SOX - App Development | | | | | |
| 8.7 | Implement a method to encrypt and decrypt sensitive data and manage encryption keys securely. Data on laptops and portable systems will utilize encryption to protect data at rest. | 8.3 Cryptographic Controls | 31-SOX - Network Security | Encryption and Decryption 164.312(a)<br>Encryption 164.312 (e) | PCI 3.4<br>PCI 3.5<br>PCI 3.6 | SAS 7.1 | § 314.4(b)(2) | CMR 17.04.5 |
| 8.8 | Deploy file integrity monitoring to alert personnel to unauthorized modification of critical system or content files | 8.4 Security of System Files | 32-SOX - Network Security | | PCI 11.5 | | | |
| 8.9 | Organization has policies for securing operating systems that applications run on. (Hardening guides, templates, base images, peer review) | 8.4.1 Control of operational software | 07-SOX - App Development | | | | | |
| 8.10 | Separation of duties between development/test and production environments. | 8.4.2 Protection of system test data | 08-SOX - App Development | | PCI 6.3.4<br>PCI 6.3.5 | | | |
| 8.11 | Organization controls access to source code and log files. Provide centralized servers or media that is difficult to alter and requires authorization to manipulate. | 8.4.3 Access control to source code and logs | | | PCI 10.5.3<br>PCI 10.5.4<br>PCI 10.5.5<br>PCI 10.7 | | | |
| 8.12 | Organization has policies and procedures to detect and remedy information leakage from applications. | 8.5.4 Information leakage | 10-SOX - App Development | | | | | |
| 8.13 | Policies and procedures exist for the outsourcing of development efforts. These polices detail how the code will be secured, reviewed, and owned. | 8.5.5 outsourced development management | 11-SOX - App Development | | | | | |
| 8.14 | Organization will perform vulnerability management. Review custom application code to identify coding vulnerabilities. Cover prevention of common coding vulnerabilities in software development processes. Deploy IDS to monitor traffic. | 8.6 Vulnerability Management | 33-SOX - Network Security | | PCI 6.1<br>PCI 6.2<br>PCI 11.1<br>PCI 11.2<br>PCI 11.3<br>PCI 11.4 | | | |
| **Change Control** | | | | | | | | |
| 8.15 | Organization has a comprehensive change management policy and detailed procedures. | 8.5 Security in Development and Support | 01 - SOX - Change Control | | PCI 6.4 | SAS 2.1<br>SAS 2.4<br>SAS 3.1 | | |

Tim Proffitt, tim@timproffitt.com

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 8.16 | Each change request is entered into a CMDB, which is used to coordinate the change process, authorization and track the status of outstanding change requests. | 8.5.1 Change control | 02 - SOX - Change Control | | PCI 6.4.1<br>PCI 6.4.2<br>PCI 6.4.3<br>PCI 6.4.4 | SAS 2.2<br>SAS 3.2 | | |
| 8.17 | Perform testing in response to environmental or operational changes. | 8.5.2 Technical Review following a change | 03-SOX - Change Control | Evaluation 164.308 (a)(8) | PCI 6.3.1<br>PCI 6.3.7 | SAS 2.3<br>SAS 3.3 | | |
| 8.18 | Organization has controls around the ability to modify code or deploy executables into the production environment. | 8.5.3 Restrictions on Change | 04-SOX - Change Control | | | SAS 2.5<br>SAS 3.4 | | |
| **INCIDENT MANAGEMENT** | | | | | | | | |
| 9.1 | Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes. | 9.1 Responding to Incidents | 34-SOX - Network Security | Response and Reporting 164.308 (a)(6) | | | § 314.4(b)(3) | CMR 17.03.2.c |
| 9.2 | Documenting responsive actions taken in connection with any incident involving a breach of security, and mandatory post-incident review of events and actions taken, if any, to make changes in business practices relating to protection of personal information. | 9.1.1 Reporting Security Incidents | 35-SOX - Network Security | | | | | CMR 17.03.12 |
| 9.3 | Response teams have follow up meetings to discuss weaknesses found during incident investigations. | 9.1.2 Reporting weaknesses | | | | | | |
| 9.4 | Incident Response teams report to management when malfunctions are discovered. | 9.2 Reporting Software Malfunctions | 36-SOX - Network Security | | | | | CMR 17.03.2.c |
| 9.5 | Policies and procedure exist for dealing with incidents. | 9.2.1 incident management procedures | 37-SOX - Network Security | | | | | |
| 9.6 | Meetings are scheduled for post incident response. These meetings allow teams to learn from the incident. | 9.2.2 Learning from incidents | | | | | | |
| **BUSINESS CONTINUITY** | | | | | | | | |
| 10.1 | Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.<br>Off-site facilities are mandatory? | 10.1 continuity and management process | 01-SOX - Data Recovery | Contingency Operations 164.310(a) | PCI 9.5 | SAS 6.2 | § 314.4 (c) | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 10.2 | Organizations will conduct a BIA with regard to the importance of assets and what they are worth. | 10.2<br>Business Impact analysis | 02-SOX - Data Recovery | Applications and Data Criticality Analysis 164.308(a)(7) | | | | |
| 10.3 | Establish (and implement as needed) procedures to restore any loss of data. | 10.3<br>writing and implementation plan | 03-SOX - Data Recovery | Disaster Recovery Plan 164.308(a)(7) | | SAS 6.1 | | |
| 10.4 | Establish procedures to enable continuation of critical business processes for protection of the security of electronic assets | 10.4<br>planning framework | 04-SOX - Data Recovery | Emergency Mode Operation Plan 164.308(a)(7) | | | | |
| 10.5 | Procedures for periodic testing and revision of contingency plans. Backup tapes should be restored to ensure they contain valid data. | 10.5<br>testing and maintaining | 05-SOX - Data Recovery | Testing and Revision Procedure 164.308(a)(7)<br>Emergency Access Procedure 164.312 (a) | | SAS 6.3 | | |

Tim Proffitt, tim@timproffitt.com

## Appendix B

## Example General SAS70 Type II Controls

***Organization and Administration***

1.1 Management's control consciousness and organization structure provides for adequately segregated duties within information systems and between information systems and users.
**1.2** Formal job descriptions are used to delineate employee responsibilities.

***Application Development, Maintenance, and Documentation***

**2.1** All program changes must follow a structured program change methodology (including emergency changes).
**2.2** Appropriate user management approves all new or modified program change requests before work is initiated.
**2.3** All program changes are tested before being placed into production.
**2.4** Information systems management approves all test results prior to a program being placed into production.
**2.5** Only appropriate information systems personnel are authorized to move programs from test to production.

***System Software/Hardware Implementation and Maintenance***

**3.1** All system maintenance releases and vendor changes must follow a structured program change methodology (including emergency changes).
**3.2** Appropriate information systems personnel must approve all system changes prior to being placed into production.
**3.3** All system maintenance releases are tested where appropriate and possible, and documented before being placed into production.
**3.4** Only appropriate information systems personnel are authorized to move programs from test to production.

***Access to Computer Facilities and Environmental Controls***

**4.1** Access to the data center, computer room, and sensitive areas of the operations center is controlled through electronic key cards assigned to appropriate employees.
**4.2** All visitors must register upon entering the facilities and must be accompanied by company personnel during their visit.
**4.3** The data center is equipped to prevent, detect, and suppress environmental factors, such as raised floors, air conditioning, fire and smoke detectors, and fire suppressant systems.

***Access to Data Files and Programs***

**5.1** Organization has a process in place to control access to all data and resources.
**5.2** Reviews of user access rights to financial management applications are periodically performed by the appropriate business unit for the information systems. Network accesses for user accounts are periodically reviewed for propriety and reasonableness.
**5.3** Users are required to enter passwords to access the system. Passwords must be changed periodically.
**5.4** After a number of unsuccessful access attempts, a user is locked out of the system.
**5.5** All access must be reviewed and approved by the appropriate user manager.
**5.6** Violations are logged and periodically reviewed.

***Backup of Program and Data Files***

**6.1** An automated backup utility is used to perform all backups.
**6.2** Backups are performed periodically and
rotated off-site, and logs are maintained so that all tapes are accounted for.
**6.3** Periodic restoration of backup tapes are done to confirm that tapes are in good condition.

***Data Transmission***

**7.1** A policy standard requires that proven, industry-accepted encryption algorithms are the basis for encryption techniques used by the organization when data is being transmitted.

Tim Proffitt, tim@timproffitt.com

**7.2** Third-party vendors, where specific sensitive information is to be exchanged, must have a contractual relationship with the organization ensuring compliance with the provisions of the encryption standards and providing for a means to audit compliance with the provisions of that standard. No exchange of sensitive information with a third party may be initiated until the required contractual relationship is in effect.

# Appendix C

## GLBA Technology Controls

**Title 16: Commercial Practices**
PART 314—STANDARDS FOR SAFEGUARDING CUSTOMER INFORMATION

### GLBA § 314.4 Elements.

In order to develop, implement, and maintain your information security program, you shall:

(a) Designate an employee or employees to coordinate your information security program.

(b) Identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks. At a minimum, such a risk assessment should include consideration of risks in each relevant area of your operations, including:

(1) Employee training and management;

(2) Information systems, including network and software design, as well as information processing, storage, transmission and disposal; and

(3) Detecting, preventing and responding to attacks, intrusions, or other systems failures.

(c) Design and implement information safeguards to control the risks you identify through risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures.

(d) Oversee service providers, by:

(1) Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue; and

(2) Requiring your service providers by contract to implement and maintain such safeguards.

(e) Evaluate and adjust your information security program in light of the results of the testing and monitoring required by paragraph (c) of this section; any material changes to your operations or business arrangements; or any other circumstances that you know or have reason to know may have a material impact on your information security program.

# Appendix D

## Mass CMR 17.03 Technology Controls

1. Designating one or more employees to maintain the comprehensive information security program;

2. Identifying and assessing reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, including but not limited to: a. ongoing employee (including temporary and contract employee) training; b. employee compliance with policies and procedures; and c. means for detecting and preventing security system failures.

3. Developing security policies for employees that take into account whether and how employees should be allowed to keep, access and transport records containing personal information outside of business premises.

4. Imposing disciplinary measures for violations of the comprehensive information security program rules.

5. Preventing terminated employees from accessing records containing personal information by immediately terminating their physical and electronic access to such records, including deactivating their passwords and user names.

6. Taking all reasonable steps to verify that any third-party service provider with access to personal information has the capacity to protect such personal information in the manner provided for in 201 CMR 17.00; and taking all reasonable steps to ensure that such third party service provider is applying to such personal information protective security measures at least as stringent as those required to be applied to personal information under 201 CMR 17.00.

7. Limiting the amount of personal information collected to that reasonably necessary to accomplish the legitimate purpose for which it is collected; limiting the time such information is retained to that reasonably necessary to accomplish such purpose; and limiting access to those persons who are reasonably required to know such information in order to accomplish such purpose or to comply with state or federal record retention requirements.

8. Identifying paper, electronic and other records, computing systems, and storage media, including laptops and portable devices used to store personal information, to determine which records contain personal information, except where the comprehensive information security program provides for the handling of all records as if they all contained personal information.

9. Reasonable restrictions upon physical access to records containing personal information, including a written procedure that sets forth the manner in which physical access to such records is restricted; and storage of such records and data in locked facilities, storage areas or containers.

10. Regular monitoring to ensure that the comprehensive information security program is operating in a manner reasonably calculated to prevent unauthorized access to or unauthorized use of personal information; and upgrading information safeguards as necessary to limit risks.

11. Reviewing the scope of the security measures at least annually or whenever there is a material change in business practices that may reasonably implicate the security or integrity of records containing personal information.

12. Documenting responsive actions taken in connection with any incident involving a breach of security, and mandatory post-incident review of events and actions taken, if any, to make changes in business practices relating to protection of personal information.

17.04: **Computer System Security Requirements**

(1) Secure user authentication protocols including: (a) control of user IDs and other identifiers; (b) a reasonably secure method of assigning and selecting passwords, or use of unique identifier technologies, such as biometrics or token devices; (c) control of data security passwords to ensure that such passwords are kept in a location and/or format that does not compromise the security of the data they protect; (d) restricting access to active users and active user accounts only; and (e) blocking access to user identification after multiple unsuccessful attempts to gain access or the limitation placed on access for the particular system;

(2) Secure access control measures that: (a) restrict access to records and files containing personal information to those who need such information to perform their job duties; and (b) assign unique identifications plus passwords, which are not vendor supplied default passwords, to each person with computer access, that are reasonably designed to maintain the integrity of the security of the access controls;

(3) To the extent technically feasible, encryption of all transmitted records and files containing personal information that will travel

(4) Reasonable monitoring of systems, for unauthorized use of or access to personal information;

(5) Encryption of all personal information stored on laptops or other portable devices;

(6) For files containing personal information on a system that is connected to the Internet, there must be reasonably up-to-date firewall protection and operating system security patches, reasonably designed to maintain the integrity of the personal information.

(7) Reasonably up-to-date versions of system security agent software which must include malware protection and reasonably up-to-date patches and virus definitions, or a version of such software that can still be supported with up-to-date patches and virus definitions, and is set to receive the most current security updates on a regular basis.

(8) Education and training of employees on the proper use of the computer security system and the importance of personal information security.

# Appendix E

## PCI Standard Risk Assessment

1.1 Establish firewall configuration standards that include:
1.1.1 A formal process for approving and testing all external network connections and changes to the firewall configuration.
1.1.2 A current network diagram with all connections to cardholder data, including any wireless networks.
1.1.3 Requirements for a firewall at each Internet connection and between any DeMilitarized Zone (DMZ) and the Intranet.
1.1.4 Description of groups, roles, and responsibilities for logical management of network components.
1.1.5 Documented list of services/ports necessary for business.
1.1.6 Justification and documentation for any available protocols besides HTTP, SSL,SSH, VPN.
1.1.7 Justification and documentation for any risky protocols allowed (for example, File Transfer Protocol [FTP]), which includes reason for use of protocol and security features implemented.
1.1.8 Periodic review of firewall/router rule sets.
1.1.9 Configuration standards for routers.
1.2 Build a firewall configuration that denies all traffic from "untrusted" networks/hosts, except for:
1.2.1 Web protocols—HTTP (port 80) and SSL (typically port 443).
1.2.2 System administration protocols (for example, SSH, or VPN).
1.2.3 Other protocols required by the business (for example, for ISO 8583).
1.3 Build a firewall configuration that restricts connections between publicly accessible servers and any system component storing cardholder data, including any connections from wireless networks. This firewall configuration should include:
1.3.1 Restricting inbound Internet traffic to IP addresses within the DMZ (ingress filters).
1.3.2 Restricting inbound and outbound Internet traffic to ports 80 and 443.
1.3.3 Not allowing internal addresses to pass from the Internet into the DMZ (egress filters).
1.3.4 Stateful inspection, also known as dynamic packet filtering (only "established" connections are allowed into the network).
1.3.5 Placing the database in an internal network zone, segregated from the DMZ.
1.3.6 Restricting outbound traffic to that which is necessary for the payment card environment.
1.3.7 Securing and synchronizing router configuration files (for example, running configuration files—used for normal running of the routers, and start-up configuration files—used when machines are re-booted, should have the same, secure configuration).
1.3.8 Denying all other inbound and outbound traffic not specifically allowed.
1.3.9 Installation of perimeter firewalls between any wireless networks and the payment card environment, and configuration of these firewalls to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment.
1.3.10 Installation of personal firewall software on any mobile and/or employee-owned computers with direct connectivity to the Internet (for example, laptops used by employees), which are used to access the organization's network.
1.4 Prohibit direct public access between external networks and any system component that stores cardholder information (for example, databases).
1.4.1 Implement a DMZ to filter and screen all traffic, to prohibit direct routes for inbound and outbound Internet traffic.
1.4.2 Restrict outbound traffic from payment card applications to Internet Protocol (IP) addresses within the DMZ.
1.5 Implement IP masquerading to prevent internal addresses from being translated and revealed on the Internet. Use technologies that implement RFC 1918 address space, such as Port Address Translation (PAT) or Network Address Translation (NAT).
2. Do not use vendor-supplied defaults for system passwords and other security parameters
2.1 Always change the vendor-supplied defaults before you install a system on the network (for example, passwords, Simple Network Management Protocol [SNMP] community strings, and

elimination of unnecessary accounts).

2.1.1 For wireless environments, change wireless vendor defaults, including but not limited to, Wireless Equivalent Privacy (WEP) keys, default Service Set Identifier (SSID), passwords, and SNMP community strings, and disabling of SSID broadcasts. Enable Wi-Fi Protected Access (WPA) technology for encryption and authentication when WPA-capable.
2.2 Develop configuration standards for all system components. Make sure these standards address all known security vulnerabilities and industry best practices.
2.2.1 Implement only one primary function per server (for example, Web servers, database servers, and DNS should be implemented on separate servers).
2.2.2 Disable all unnecessary and insecure services and protocols (services and protocols not directly needed to perform the devices' specified function).
2.2.3 Configure system security parameters to prevent misuse.
2.2.4 Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems (for example, unnecessary Web servers).
2.3 Encrypt all non-console administrative access. Use technologies such as SSH, VPN, or SSL/Transport Layer Security (TLS) for Web-based management and other non-console administrative access.
3. Protect Stored Data
3.1 Keep cardholder information storage to a minimum. Develop a data retention and disposal policy. Limit your storage amount and retention time to that which is required for business, legal, and/or regulatory purposes, as documented in the data retention policy.
3.2 Do not store sensitive authentication data subsequent to authorization (not even if encrypted):
3.2 Do not store sensitive authentication data subsequent to authorization (not even if encrypted):
3.2.1 Do not store the full contents of any track from the magnetic stripe (on the back of a card, in a chip, etc.).
3.2.2 Do not store the card-validation code (CVC) (Three-digit or four-digit value printed on the front or back of a payment card (for example, CVV2, and CVC2 data).
3.2.3 Do not store the PIN Verification Value (PVV).
3.3 Mask account numbers when displayed (the first six and last four digits are the maximum number of digits to be displayed).
3.4 Render sensitive cardholder data unreadable anywhere it is stored (including data on portable media, backup media, in logs, and data received from or stored by wireless networks) by using any of the following approaches:
• One-way hashes (hashed indexes), such as SHA-1
• Truncation
• Index tokens and PADs, with the PADs being securely stored
• Strong cryptography, such as Triple-DES (Data Encryption Standard) 128-bit or AES 256-bit with associated key management processes and procedures
3.5 Protect encryption keys against both disclosure and misuse.
3.5.1 Restrict access to keys to the fewest number of custodians necessary.
3.5.2 Store keys securely in the fewest possible locations and forms.
3.6 Fully document and implement all key management processes and procedures, including:
3.6.1 Generation of strong keys.
3.6.2 Secure key distribution.
3.6.3 Secure key storage.
3.6.4 Periodic key changes.
3.6.5 Destruction of old keys.
3.6.6 Split knowledge and dual control of keys (so that it requires two or three people, each knowing only their part of the key, to reconstruct the whole key).
3.6.7 Prevention of unauthorized substitution of keys.
3.6.8. Replacement of known or suspected compromised keys.
3.6.9. Revocation of old or invalid keys (mainly for RSA keys).
3.6.10 Requirement for key custodians to sign a form specifying that they understand and accept their key-custodian responsibilities.
4. Encrypt transmission of cardholder and sensitive information across public networks

4.1 Use strong cryptography and encryption techniques (at least 128 bit) such as SSL, Point-to-Point Tunneling Protocol (PPTP), Internet Protocol Security (IPSEC) to safeguard sensitive cardholder data during transmission over public networks.
4.1.1 For wireless networks transmitting cardholder data, encrypt the transmissions by using Wi-Fi Protected Access (WPA) technology if WPA capable, or VPN or SSL at 128-bit. Never rely exclusively on WEP to protect confidentiality and access to a wireless Local Area Network (LAN). Use one of the above methodologies in conjunction with WEP at 128 bit, and rotate shared WEP keys quarterly and whenever there are personnel changes.
4.2 Never send cardholder information via unencrypted e-mail.
5. Use and regularly update anti-virus software or programs
5.1 Deploy anti-virus mechanisms on all systems commonly affected by viruses (for example PC's and servers).
5.2 Ensure that all anti-virus mechanisms are current, actively running, and capable of generating audit logs.
6. Develop and maintain secure systems and applications
6.1 Ensure that all system components and software have the latest vendor-supplied security patches.
6.1.1 Install relevant security patches within one month of release.
6.2 Establish a process to identify newly discovered security vulnerabilities (for example, subscribe to alert services freely available on the Internet). Update your standards to address new vulnerability issues.
6.3 Develop software applications based on industry best practices and include information security throughout the software development life cycle. Include the following:
6.3.1 Testing of all security patches and system and software configuration changes before deployment.
6.3.2 Separate development/test and production environments.
6.3.3 Separation of duties between development/test and production environments.
6.3.4 Production data (real credit card numbers) are not used for testing or development.
6.3.5 Removal of test data and accounts before production systems become active.
6.3.6 Removal of custom application accounts, usernames, and passwords before applications become active or are released to customers.
6.3.7 Review of custom code prior to release to production or customers, to identify any potential coding vulnerability.
6.4 Follow change control procedures for all system and software configuration changes. The procedures should include:
6.4.1 Documentation of impact.
6.4.2 Management sign-off by appropriate parties.
6.4.3 Testing that verifies operational functionality.
6.4.4 Back-out procedures.
6.5 Develop Web software and applications based on secure coding guidelines such as the Open Web Application Security Project guidelines. Review custom application code to identify coding vulnerabilities. Cover prevention of common coding vulnerabilities in software development processes, to include:
6.5.1 Invalidated input.
6.5.2 Broken access control (for example, malicious use of user IDs).
6.5.3 Broken authentication/session management (use of account credentials and session cookies).
6.5.4 Cross-site scripting (XSS) attacks.
6.5.5 Buffer overflows.
6.5.6 Injection flaws (for example, SQL injection).
6.5.7 Improper error handling.
6.5.8 Insecure storage.
6.5.9 Denial of service.
6.5.10 Insecure configuration management.
7. Restrict access to data by business need-to-know
7.1 Limit access to computing resources and cardholder information to only those individuals whose job requires such access.
7.2 Establish a mechanism for systems with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.
8. Assign a unique ID to each person with computer access

8.1 Identify all users with a unique username before allowing them to access system components or cardholder data.
8.2 Employ at least one of the methods below, in addition to unique identification, to authenticate all users:
- Password
- Token devices (for example, SecureID®, certificates, or public key)
- Biometrics

8.3 Implement two-factor authentication for remote access to the network by employees, administrators, and third parties. Use technologies such as Remote Authentication Dial-In User Service (RADIUS) or Terminal Access Controller Access Control System (TACACS) with tokens, or VPN with individual certificates.
8.4 Encrypt all passwords during transmission and storage, on all system components.
8.5 Ensure proper user authentication and password management for non-consumer users and administrators, on all system components:
8.5.1 Control the addition, deletion, and modification of user IDs, credentials, and other identifier objects.
8.5.2 Verify user identity before performing password resets.
8.5.3 Set first-time passwords to a unique value per user and change immediately after first use.
8.5.4 Immediately revoke accesses of terminated users.
8.5.5 Remove inactive user accounts at least every 90 days.
8.5.6 Enable accounts used by vendors for remote maintenance only during the time needed.
8.5.7 Distribute password procedures and policies to all users who have access to cardholder information.
8.5.8 Do not use group, shared, or generic accounts/passwords.
8.5.9 Change user passwords at least every 90 days.
8.5.10 Require a minimum password length of at least seven characters.
8.5.11 Use passwords containing both numeric and alphabetic characters.
8.5.12 Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.
8.5.13 Limit repeated access attempts by locking out the user ID after not more than six attempts.
8.5.14 Set the lockout duration to thirty minutes or until administrator enables the user ID.
8.5.15 If a session has been idle for more than 15 minutes, require the user to re-enter the password to re-activate the terminal.
8.5.16 Authenticate all access to any database containing cardholder information. This includes access by applications, administrators, and all other users.
9. Restrict physical access to cardholder data
9.1 Use appropriate facility entry controls to limit and monitor physical access to systems that store, process, or transmit cardholder data.
9.1.1 Use cameras to monitor sensitive areas. Audit this data and correlate with other entries. Store for at least three months, unless otherwise restricted by law.
9.1.2 Restrict physical access to publicly accessible network jacks.
9.1.3 Restrict physical access to wireless access points, gateways, and handheld devices.
9.2 Develop procedures to help all personnel easily distinguish between employees and visitors, especially in areas where cardholder information is accessible.
9.3 Make sure all visitors are:
9.3.1 Authorized before entering areas where cardholder data is processed or maintained.
9.3.2 Given a physical token (for example, badge, or access device) that expires, and that identifies them as non-employees.
9.3.3 Asked to surrender the physical token before leaving the facility or at the date of expiration.
9.4 Use a visitor log to retain a physical audit trail of visitor activity. Retain this log for a minimum of three months, unless otherwise restricted by law.
9.5 Store media back-ups in a secure off-site facility, which may be either an alternate third-party or a commercial storage facility.
9.6 Physically secure all paper and electronic media (for example, computers, electronic media, networking and communications hardware, telecommunication lines, paper receipts, paper reports, and faxes) that contain cardholder information.

9.7 Maintain strict control over the internal or external distribution of any kind of media that contains cardholder information:
9.7.1 Label the media so it can be identified as confidential.
9.7.2 Send the media via secured courier or a delivery mechanism that can be accurately tracked.
9.8 Ensure management approves all media that is moved from a secured area (especially when media is distributed to individuals).
9.9 Maintain strict control over the storage and accessibility of media that contains cardholder information:
9.9.1 Properly inventory all media and make sure it is securely stored.
9.10 Destroy media containing cardholder information when it is no longer needed for business or legal reasons:
9.10.1 Cross-cut shred, incinerate, or pulp hardcopy materials.
9.10.2 Purge, degauss, shred, or otherwise destroy electronic media so that cardholder data cannot be reconstructed.
10. Track and monitor all access to network resources and cardholder data
10.1 Establish a process for linking all access to system components (especially those done with administrative privileges such as root) to an individual user.
10.2 Implement automated audit trails to reconstruct the following events, for all system components:
10.2.1 All individual user accesses to cardholder data.
10.2.2 All actions taken by any individual with root or administrative privileges.
10.2.3 Access to all audit trails.
10.2.4 Invalid logical access attempts.
10.2.5 Use of identification and authentication mechanisms.
10.2.6 Initialization of the audit logs.
10.2.7 Creation and deletion of system-level objects.
10.3 Record at least the following audit trail entries for each event, for all system components:
10.3.1 User identification.
10.3.2 Type of event.
10.3.3 Date and time.
10.3.4 Success or failure indication.
10.3.5 Origination of event.
10.3.6 Identity or name of affected data, system component, or resource.
10.4 Synchronize all critical system clocks and times.
10.5 Secure audit trails so they cannot be altered, including the following:
10.5.1 Limit viewing of audit trails to those with a job-related need.
10.5.2 Protect audit trail files from unauthorized modifications.
10.5.3 Promptly back-up audit trail files to a centralized log server or media that is difficult to alter.
10.5.4 Copy logs for wireless networks onto a log server on the internal LAN.
10.5.5 Use file integrity monitoring/change detection software (such as Tripwire) on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).
10.6 Review logs for all system components at least daily. Log reviews should include those servers that perform security functions like Intrusion Detection System (IDS) and Authentication, Authorization, and Accounting (AAA) servers (for example, RADIUS).
10.7 Retain your audit trail history for a period that is consistent with its effective use, as well as legal regulations.
11. Regularly test security systems and processes
11.1 Test security controls, limitations, network connections, and restrictions routinely to make sure they can adequately identify or stop any unauthorized access attempts. Where wireless technology is deployed, use a wireless analyzer periodically to identify all wireless devices in use.
11.2 Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (for example, new system component installations, changes in network topology, firewall
rule modifications, product upgrades).
11.3 Perform penetration testing on network infrastructure and applications at least once a year and after any significant infrastructure or application upgrade or modification (for example, operating system

upgrade, sub-network added to environment, Web server added to
environment).
11.4 Use network intrusion detection systems, host-based intrusion detection systems, and/or intrusion prevention systems to monitor all network traffic and alert personnel to suspected compromises. Keep all intrusion detection and prevention engines up to date.
11.5 Deploy file integrity monitoring to alert personnel to unauthorized modification of critical system or content files, and perform critical file comparisons at least daily (or more frequently if the process can be automated).
12. Maintain a policy that addresses information security for employees and contractors
12.1 Establish, publish, maintain, and disseminate a security policy that:
12.1.1 Addresses all requirements in this specification.
12.1.2 Includes an annual process that identifies threats, and vulnerabilities, and results in a formal risk assessment.
12.1.3 Includes a review at least once a year and updates when the environment changes.
12.2 Develop daily operational security procedures that are consistent with requirements in this specification (for example, user account maintenance procedures, and log review procedures).
12.3 Develop usage policies for critical employee-facing technologies, such as modems and wireless, to define proper use of these technologies for all employees and contractors. Ensure these usage policies require:
12.3.1 Explicit management approval.
12.3.2 Authentication for use of the technology.
12.3.3 A list of all such devices and personnel with access.
12.3.4 Labeling of devices with owner, contact information, and purpose.
12.3.5 Acceptable uses of the technology.
12.3.6 Acceptable network locations for these technologies.
12.3.7 A list of company-approved products.
12.3.8 Automatic disconnect of modem sessions after a specific period of inactivity.
12.3.9 Activation of modems for vendors only when needed by vendors, with immediate deactivation after use.
12.3.10 When accessing cardholder data remotely via modem, disable storage of cardholder data onto local hard drives, floppy disks or other external media. Also, disable cut and paste, and print functions during remote access.
12.4 Ensure the security policy and procedures clearly define information security responsibilities for all employees and contractors.
12.5 Assign to an individual or team the following information security management responsibilities:
12.5.1 Establish, document, and distribute security policies and procedures
12.5.2 Monitor and analyze security alerts and information, and distribute to appropriate personnel.
12.5.3 Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations.
12.5.4 Administer user accounts, including additions, deletions, and modifications.
12.5.4 Monitor and control all access to data.
12.6 Make all employees aware of the importance of cardholder information security:
12.6.1 Educate employees (for example, through posters, letters, memos, meetings, and promotions).
12.6.2 Require employees to acknowledge in writing that they have read and understood the company's security policy and procedures.
12.7 Screen potential employees to minimize the risk of attacks from internal sources.
12.8 Contractually require all third parties with access to cardholder data to adhere to payment card industry security requirements. At a minimum, the agreement should address:
12.8.1 Acknowledgement that the 3rd party is responsible for security of cardholder data in their possession.
12.8.2 Ownership by each Payment Card brand, Acquirer, and Merchants of cardholder data and acknowledgement that such data can ONLY be used for assisting these parties in completing a transaction, supporting a loyalty program, providing fraud control services, or for others uses specifically required by law.
12.8.3 Business continuity in the event of a major disruption, disaster, or failure.
12.8.4 Audit provisions that ensure that Payment Card Industry representative, or a Payment Card

Industry approved third party, will be provided with full cooperation and access to conduct a thorough security review after a security intrusion. The review will validate compliance with Payment Card Industry Security Standards for protecting cardholder data.
12.8.5 Termination provision that ensures that 3rd party will continue to treat cardholder data as confidential.
12.9 Implement an incident response plan. Be prepared to respond immediately to a system breach.
12.9.1 Create an incident response plan to be used in the event of system compromise. Ensure the plan addresses, at a minimum, specific incident response procedures, business recovery and continuity procedures, data backup processes, roles and responsibilities, and communication and contact strategies (for example, informing Acquirers and credit card associations).
12.9.2 Test the plan at least annually.
12.9.3 Designate specific personnel to be available on a 24/7 basis to respond to alerts.
12.9.4 Provide appropriate training to staff with security breach response responsibilities.
12.9.5 Include alerts from intrusion detection, intrusion prevention, and file integrity monitoring systems.
12.9.6 Have a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments.

## Appendix F

## Example of Sarbanes Oxley Technology Controls

| | |
|---|---|
| 01 - General Control - Change Control | Each change request is entered into the CMDB, which is used to coordinate the change process and track the status of outstanding change requests. |
| 01 - General Control - Change Control | All application development changes are tested in the Test environment prior to being migrated to the Staging environment. The status in CMDB is changed from Development to Build. |
| 01 - General Control - Change Control | All application development CMDB tickets require QA Team signoff prior to being considered for promotion to production. |
| 01 - General Control - Change Control | The QA team documents results of testing of major change controls as pass or fail. |
| 01 - General Control - Change Control | Deployment dates are scheduled for each change request. |
| 01 - General Control - Change Control | Technology Solutions QA Group is dedicated to the testing efforts for all development changes. Depending on the severity of the change, user acceptance testing will occur. |
| 01 - General Control - Change Control | QA performs regression testing in the stage environment. When necessary, rollback testing is performed by the QA group in the stage environment. |
| 01 - General Control - Change Control | A test plan, when applicable, is documented by the Business Analyst and is attached to each CMDB ticket. |
| 01 - General Control - Change Control | Periodically, end users are involved in testing for major releases. When involved, the UA check-box is checked and the BA name is recorded in CMDB. |
| 01 - General Control - Change Control | Formal change management procedures are documented for standard, infrastructure, and emergency changes in the form of policy documents and process flows. |
| 01 - General Control - Change Control | Developers do not have the ability to modify code or deploy executables into the production environment . |
| 01 - General Control - Change Control | hen production data is modified by the DBA team, the activity is formally tracked in Heat or documented in the project plan requiring the changes. |
| 01 - General Control - Change Control | All users, with the exception of authorized personnel based on job function, have read only access to production data in Informix databases using ODBC or other direct connection |

| | |
|---|---|
| | methods. |
| 01 - General Control - Change Control | Users, with the exception of authorized personnel based on job function, do not have access to production data |
| 01 - General Control - Change Control | When production data is modified by Production Support Team the activity and resolution are formally tracked. |
| 01 - General Control - Change Control | The Change Control Committee (CCC) meets weekly to give the final approval for Business Application Changes to be released into production. The committee is composed of appropriate personnel. |
| 01 - General Control - Change Control | A source code versioning system is used to store production code. Once checked in to the secured source code repository, all changes are tracked. Multiple code repository systems are used depending on the code being developed. |
| 01 - General Control - Change Control | A rollback plan is in place for all deployment activities to ensure that previous system settings can be restored in the event that an implementation needs to be reversed. |
| 01 - General Control - Change Control | The Test Environment is refreshed periodically to support ongoing deployment activities. |
| 01 - General Control - Change Control | The Staging Environment is refreshed periodically to support ongoing deployment activities. |
| 01 - General Control - Change Control | The Development Environment is refreshed periodically to support ongoing deployment activities. |
| 01 - General Control - Change Control | Upgrades and patches to critical network servers and the operating systems are documented in a change control form. |
| 01 - General Control - Change Control | Upgrades and patches to critical operating systems are tested (when possible) in a separate test environment and applied according to change control procedures. |
| 01 - General Control - Change Control | Access to migrate operating system patches into the production environment is restricted to the infrastructure team. |
| 01 - General Control - Change Control | Emergency changes are documented in a change control form, deployed by the appropriate personnel, and must be approved by one director. |
| 02 - General Control - Data Recovery | Changes made to the database are replicated to the disaster recovery site in near real time. |
| 02 - General Control - Data Recovery | Backup tapes are stored in turtle boxes and sealed with a tie, and are sent offsite each afternoon. Backup tapes for Monday-Thursday are retained for 2 weeks, and Friday's backups are retained for 6 months. A bar code system is used |

Tim Proffitt, tim@timproffitt.com

| | |
|---|---|
| | to track the distribution of backup tapes. |
| 02 - General Control - Data Recovery | Backup processes are scheduled to automatically occur on a nightly basis using the backup infrastructure. |
| 02 - General Control - Data Recovery | Backup responsibilities are separated between two teams. Separation of duties exists between the backup scheduling and the monitoring and troubleshooting of backups. |
| 02 - General Control - Data Recovery | The backup report shows the schedule type, source, etc., and is used to indicate a successful completion of backup activities. |
| 02 - General Control - Data Recovery | Tape backups are restored in the pre-production environment as needed and are tested to ensure reliability of the tapes and the supporting process. |
| 02 - General Control - Data Recovery | Only authorized personnel can obtain the backup tapes. |
| 02 - General Control - Data Recovery | There is a company-wide Disaster Recovery Plan (DRP) that is documented, and resides on a company website. |
| 02 - General Control - Data Recovery | A disaster recovery test of the technology systems is conducted at least once a year. |
| 02 - General Control - Data Recovery | One Uninterrupted Power Supply (UPS) system is located in the Data Center which provides power to the data center in the event of a disruption. The UPS will maintain power for approximately 20 minutes. |
| 02 - General Control - Data Recovery | Two diesel generators are in place with enough fuel to operate the Data Center components for approximately 3 days. The two megawatt generator is the initial generator that will power the Data Center and the five hundred kilowatt generator is available as a backup. Both generators are maintained on a quarterly basis by a third party vendor with respective documentation maintained by the Facilities Group. Testing of the generators is performed on a weekly basis by the Facilities Group and documentation is kept on file. |
| 02 - General Control - Data Recovery | A redundant WAN infrastructure exists between data centers to ensure a continuous data flow in the event of an single point of failure. |
| 03 - General Control - Data Center Operations | Access to the data center is controlled thru the privileges assigned to the employee's identification badges. Access to the data center is limited to only authorized personnel. |
| 03 - General Control - Data Center Operations | A security policy addressing data center access requirements and data center procedures is formally documented. |

| | |
|---|---|
| 03 - General Control - Data Center Operations | All requests for new user access to the Data Center must be submitted and formally approved by the Director. |
| 03 - General Control - Data Center Operations | Employee terminations are formally communicated via email from HR to the Security Supervisor for timely removal of unauthorized access to the Data Center. Upon receipt of HR notification, access to the Data Center is disabled. |
| 03 - General Control - Data Center Operations | Only authorized employees will escort visitors into the Data Center. |
| 03 - General Control - Data Center Operations | The entrances to the data center remain locked at all times, and are only accessible via an authorized identification badge. |
| 03 - General Control - Data Center Operations | Numerous failed attempts by one individual is followed up by security with individual's manager. |
| 03 - General Control - Data Center Operations | All visitors and vendors, unless explicitly authorized, are escorted during their time in the data center. |
| 03 - General Control - Data Center Operations | Management periodically reviews the listing of personnel who have access to the data center. |
| 03 - General Control - Data Center Operations | Data Center is protected from fires by FM200 fire suppression and smoke detectors located both under the floor and on the ceiling. Pre-actual dry pipe sprinkler systems are activated as soon as FM200 sends alert. |
| 03 - General Control - Data Center Operations | The data center is protected by water detection devices underneath the floor paneling. A secondary metal roof that is below the physical roof also protects the Data Center from moisture. The water detection device detects and sends an alert to the Facilities group at the first sign of moisture. |
| 03 - General Control - Data Center Operations | An 18 inch raised floor exists throughout the primary data center. |
| 03 - General Control - Data Center Operations | The following systems exist to monitor environmental for the primary data center: 1) UPS, 2) Generator, 3) dedicated HVAC, and 4) emergency electricity shutoff switches. |
| 03 - General Control - Data Center Operations | The information infrastructure is monitored by several software technologies that send alerts to the system administrators for events of interest. |
| 04 - General Control - Virus Control | Anti-Virus exists on Windows client server devices and desktops. |
| 04 - General Control - Virus Control | The AV server obtains the latest virus definition files on a daily basis and automatically distributes them to connected network computers. |
| 04 - General Control - Virus Control | Upon detection of a virus, the anti-virus software will attempt to clean the infected file. If unsuccessful the anti-virus software will delete the infected file. If the anti-virus software is unable to delete the file, the action will be logged in the |

| | |
|---|---|
| | management console. |
| 04 - General Control - Virus Control | 3rd party email filtering vendor is used filter incoming email from viruses, spam, and phishing attacks. |
| 04 - General Control - Virus Control | Corporate imaged laptops have the ability to obtain virus definition updates over the internet when they cannot connect to the internal AV server. |
| 04 - General Control - Virus Control | IPS maintains virus definitions inside the IPS signature updates. These updates are "pushed" to the IPS infrastructure when issued. |
| 04 - General Control - Virus Control | The Acceptable Use Policy documents user responsibilities for virus controls. |
| 05 - General Control - Network Security | Request for initial access for the corporate user comes from the Business Unit's Executive Assistant or an appropriate authorized individual in the form of a ticket |
| 05 - General Control - Network Security | Request for initial access for a contract employee comes from the contract employee's direct report. The corporate manager, supervisor, or executive assistant submits a ticket with provisioning information. |
| 05 - General Control - Network Security | IT assigns new users to respective groups, based on the information provided in the employee setup request, to provide access to file shares (NTFS permissions). |
| 05 - General Control - Network Security | Employee terminations are formally communicated from HR to IT for timely removal of unauthorized access to the network (Active Directory). |
| 05 - General Control - Network Security | Password parameter settings are enforced. The minimum password length is set to 8 characters. Passwords must have 3 of the following 4 provisions: 1) upper case character, 2) lower case character, 3) numeric, and 4) special character. |
| 05 - General Control - Network Security | Access requires a unique username and password, authenticated to the Microsoft Active Directory, to gain access to network resources. |
| 05 - General Control - Network Security | The account lockout threshold is set to 5 invalid password attempts, with an auto reset after 30 minutes. |
| 05 - General Control - Network Security | Passwords are set to expire after a period of 90 days. |
| 05 - General Control - Network Security | Initial passwords are randomly created and are set to immediately expire after the user setup and hardware processes have been provisioned. |
| 05 - General Control - Network Security | NT has a password history of 24, which does not allow users to reuse one of their most previously used 24 passwords. |
| 05 - General Control - Network Security | A procedure is executed on a periodic basis to check for accounts that have been inactive for over 90 days. |

Tim Proffitt, tim@timproffitt.com

| | |
|---|---|
| 05 - General Control - Network Security | The default account "administrator" has been renamed on the server and workstation platforms. |
| 05 - General Control - Network Security | The "Guest" account is disabled on the corporate image and servers to minimize misuse of the account. |
| 05 - General Control - Network Security | The system administrator capabilities are restricted to only appropriate personnel. |
| 05 - General Control - Network Security | A warning message is displayed to all users who attempt to log into critical network servers. |
| 05 - General Control - Network Security | User logon failures are logged for critical servers. File level auditing is initiated upon request. All audit logs are backed up as part of the normal backup process. Logon failures are captured in a daily report that is reviewed by the Technology Security team. |
| 05 - General Control - Network Security | When vulnerabilities are found, Technology Security submits requests to remediate the issue in a timely manner. |
| 05 - General Control - Network Security | A warning message is displayed to all users who attempt to log into critical network servers via VPN. |
| 05 - General Control - Network Security | Enterprise level firewall protects internal and DMZ networks. |
| 05 - General Control - Network Security | A distribution tool is used to maintain platform baselines, and push updates to MS servers. Hardware upgrades must be performed in conjunction with the normal change management process. |
| 05 - General Control - Network Security | Server updates are received from MS and applied according to priority and need. Updates that are assigned a critical priority by the security group, are applied within two weeks of receiving. |
| 05 - General Control - Network Security | MS updates for desktop images are reviewed when received and scheduled for installation according to need. Updates are bundled and scheduled for install. |
| 05 - General Control - Network Security | Policies and procedures related to installation of patches and updates are defined and approved by management. |
| 05 - General Control - Network Security | IT Policies and Standards are reviewed, approved, and published. |
| 05 - General Control - Network Security | The wireless network is secured and encrypted using WPA-TKIP and RADIUS technologies. Domain authentication is required before connection to the wireless network is allowed. |
| 05 - General Control - Network Security | Visitors, vendors and contractors can access a segmented wireless network for Internet access only. |

Tim Proffitt, tim@timproffitt.com

| | |
|---|---|
| 10 - Entity Level Controls | Technology department focuses on alignment of technology with business goals. |
| 10 - Entity Level Controls | staff performance reviews and incentive goals are aligned with the company using the same system and metrics as the other business units. |
| 10 - Entity Level Controls | Project prioritization meetings occur periodically to determine critical projects and align resources appropriately |
| 10 - Entity Level Controls | Annual budget process occurs to define budget needs for following year based on research and input from business units and internal organization. |
| 10 - Entity Level Controls | "Periodic meetings with key personnel across the company to discuss technology initiatives and understand new corporate direction. |
| 10 - Entity Level Controls | PMO defines and maintain a project methodology. |
| 10 - Entity Level Controls | The PMO office has the responsibility to review projects to ensure compliance to the methodology and standards defined. |
| 10 - Entity Level Controls | Managers and teams align directly to the divisions within the company to work more closely with them on their needs. |
| 10 - Entity Level Controls | Business Units participate in Application Development through providing detailed requirements and participate in design efforts as well as POC and User Acceptance Testing of all systems. |
| 10 - Entity Level Controls | "PMO Risk Management Responsibilities provide for proper management of risk and checkpoints during major projects to review project viability and risk. |
| 10 - Entity Level Controls | Bi-Weekly Project Review meetings take place at manager level in the organization to review changes in project status such as scope, budget or accomplishment of major milestones. |
| 10 - Entity Level Controls | Project Office Dashboard is regularly updated by project managers for all enterprise level projects and made available for review by all Directors and Managers. |
| 10 - Entity Level Controls | All security and access control policies are documented in the Technology Policy. |
| 10 - Entity Level Controls | Upon the occurrence of a security issue, the IT Security Committee will meet to mitigate the issue and discuss post mortem. |
| 10 - Entity Level Controls | Security Awareness Training is administered to all personnel. |

Tim Proffitt, tim@timproffitt.com