

# CSF Assurance Program Assessment Report

---

Business Associate ABC

October 10, 2010

SAMPLE

# Contents

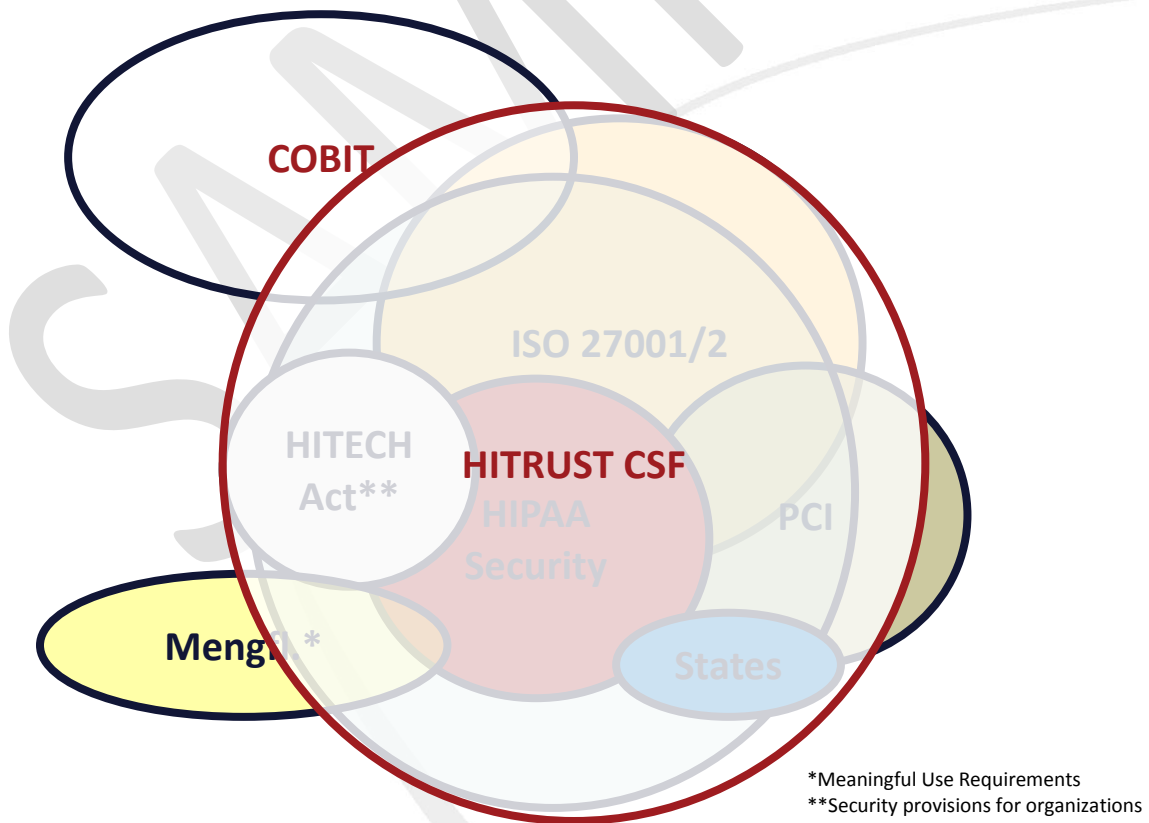
1. HITRUST Background .....	3
2. Letter of Certification.....	5
3. Representation Letter from Management .....	6
4. Assessment Context.....	7
5. Scope of systems in the assessment.....	8
6. Security Program Analysis.....	10
7. Assessment Results.....	11
8. Overall Security Program Summary.....	14
9. Breakdown by CSF Control Areas Required for Certification.....	16
10. Compliance Scorecards.....	22
HIPAA Security Rule.....	23
COBIT DS5.....	27
Appendix A – Detailed Control Summary of Business Associate ABC .....	28
Appendix B – Testing Summary .....	29
Appendix C – Corrective Action Plan .....	30
Appendix D – Questionnaire Results .....	31
Appendix E – System Profile .....	32

## 1. HITRUST Background

The Health Information Trust Alliance (HITRUST) was born out of the belief that information security should be a core pillar of, rather than an obstacle to, the broad adoption of health information systems and exchanges. HITRUST, in collaboration with healthcare, business, technology and information security leaders, has established the Common Security Framework (CSF), a certifiable framework that can be used by any and all organizations that create, access, store or exchange personal health and financial information. Beyond the establishment of the CSF, HITRUST is also driving the adoption of and widespread confidence in the framework and sound risk management practices through awareness, education, advocacy and other outreach activities. For more information about HITRUST, the HITRUST CSF and other HITRUST offerings and programs, visit [www.HITRUSTalliance.net](http://www.HITRUSTalliance.net).

An integral component to achieving HITRUST's goal to advance the healthcare industry's protection of health information is the establishment of a practical mechanism for validating an organization's compliance with the CSF.

The CSF is an overarching security framework that incorporates and leverages the existing security requirements placed upon healthcare organizations, including federal (e.g., HIPAA and HITECH), state, third party (e.g., PCI and COBIT), and other government agencies (e.g., NIST, FTC, and CMS). The CSF is already being widely adopted by leading healthcare payers, providers, and state exchanges as their security framework.



HITRUST has developed the CSF Assurance program, which encompasses the common requirements, methodology and tools that enable both healthcare organizations and their business partners to take a consistent and incremental approach to managing compliance.

This program is the mechanism that allows healthcare organizations and their business partners to assess and report against multiple sets of requirements. Unlike other programs in healthcare and in other industries, the oversight, vetting and governance provided by HITRUST and the CSF Assurance Committee affords greater assurances and security across the industry.



## 2. Letter of Certification

October 10, 2010

Business Associate ABC  
2 Business Associate St.  
Anchorage, AK 93127

Based upon representation from management as to the accuracy and completeness of information provided, the procedures performed by an approved CSF Assessor to validate such information, and HITRUST's independent confirmation that the work was performed in accordance with the CSF Assurance Program, the following business units of the organization meet the 2010 CSF Certification Criteria:

Business Associate ABC

The certification is valid for a period of two years assuming the following occurs:

- Annual progress is being made on areas identified in the CAP
- A continuous monitoring program is in place to determine if the controls continue to operate effectively over time
- No data security breach has occurred
- No significant changes in the business or security policies, practices, controls and processes have occurred that might impact its ability to meet the CSF certification criteria

The Health Information Trust Alliance (HITRUST) has developed the Common Security Framework (CSF), a certifiable framework that provides organizations with the needed structure, detail and clarity relating to information security tailored to the healthcare industry. HITRUST, with input from leading organizations within the industry, identified a subset of the CSF control requirements that an organization must meet to be CSF Certified. For those CSF control requirements that are not required for certification and are currently not being met, the organization must have a Corrective Action Plan (CAP) that outlines its plans for meeting such requirements.

Additional information on the CSF Certification program can be found at the HITRUST website:  
[www.hitrustalliance.net](http://www.hitrustalliance.net).

HITRUST

### 3. Representation Letter from Management

October 10, 2010

HITRUST LLC  
6136 Frisco Square Blvd.  
Suite 327  
Frisco, TX 75034

In connection with our engagement to perform an assessment of Business Associate ABC's security controls compared with the HITRUST Common Security Framework (CSF) controls required for certification, we recognize that obtaining representations from us concerning the information contained in this report and the information regarding our security controls is a significant procedure in enabling you to complete your work. Accordingly, we make the following representations to you and the recipients of your report regarding our security controls which are true to the best of our knowledge and belief:

- We acknowledge that, as members of management, we are responsible for the controls implemented to secure protected health information (PHI) as required by HIPAA and HITRUST's CSF certification program.
- We have responded fully to all inquiries made to us by you during the engagement.
- We have made available to you all records and necessary documentation related to the controls used to protect PHI processed by the systems included in the scope of your engagement.
- We have disclosed to you all design and operating deficiencies in our controls over PHI of which we are aware, including those for which we believe the cost of corrective action may exceed the benefits.
- No events or transactions have occurred or are pending that would have an effect on the assessment that you performed and used as a basis for issuing your certification report.

We understand that the engagement was conducted in accordance with the security requirements contained in the CSF. We also understand that the sufficiency of this report and the procedures performed is solely the responsibility of report recipients.

Very truly yours,

Authorized Signature

#### 4. Assessment Context

<b>Prepared For</b>	Business Associate ABC 2 Business Associate St. Anchorage, AK 93127
<b>Contact</b>	Alan Park Director, Information Security Alan.park@baabc.com
<b>Assessed Entity</b>	Business Associate ABC
<b>Date of Report</b>	October 10, 2010
<b>Period of Assessment</b>	September 2010
<b>Date of Quality Assurance by HITRUST</b>	October 2010
<b>Type of Assessment</b>	On-site 3 <sup>rd</sup> party testing conducted: <ul style="list-style-type: none"> <li>• Interviews</li> <li>• Review of documents</li> <li>• Review of technical settings</li> </ul>
<b>Company Background</b>	Business Associate ABC is Alaska's premier full service pharmacy benefit management (PBM) company.
<b>Number of covered lives</b>	7 Million
<b>Geographic scope of operations considered for the assessment</b>	Multi-state
<b>Number of employees</b>	1000
<b>Requirements in scope of review</b>	<ul style="list-style-type: none"> <li>• HIPAA Security Rule</li> <li>• COBIT DS5</li> </ul>

## 5. Scope of systems in the assessment

Business Associate ABC is Alaska's premier full service Pharmacy Benefit Management (PBM) company, also with operations extending to Washington, Oregon and Wyoming. Business Associate ABC provides healthcare management and administration services on behalf of clients that include health maintenance organizations, health insurers, third-party administrators, employers, union-sponsored benefit plans and government health programs. Business Associate ABC's integrated PBM services include network claims processing, home delivery pharmacy services, specialty prescription fulfillment, benefit design consultation, drug utilization review, and drug data analysis services. Business Associate ABC delivers its PBM services through networks of approximately 2,000 retail pharmacies (representing more than 95% of retail pharmacies in the Pacific Northwest) and one home delivery pharmacies.

A PBM is a link between the entities involved in the delivery of prescription drugs to health plan members' Health plans, employers, and third-party administrators that hire a PBM to design, implement and manage their overall drug benefits. Business Associate ABC offers services such as developing the drug formulary (the list of drugs covered as the plan), establishing a pharmacy network, and processing prescription claims.

Business Associate ABC provides PBM services for clients by processing (adjudicating) pharmacy claims primarily through its proprietary Hardline system and by processing rebates through the Quad and Customer CoOp systems. The Hardline system is a mainframe application supported by an IBM front-end processor. Organizational Benefit System (OBS), Benefit Administration (BenAdmin), Drug Administration (DrugAdmin), Formulary Administration (FormAdmin), and Quad are multiuser applications, supported by midrange front-end processors (HP and IBM) paired with a mainframe back-end processor. These applications support the following business activities:

- Client setup and member enrollment
- Claims processing/adjudication
- Claims billing and reimbursement
- Manufacturer rebate processing

The Customer CoOp system is a UNIX application supported by a Hewlett Packard (HP) operating system in the midrange environment. Customer CoOp supports the allocation of manufacturer rebates to Business Associate ABC's clients.

Claims data transmitted into the Hardline system either directly or via a pharmacy switch to the mainframe located at EDS in San Francisco, CA. Based on previously loaded and established client setup and member enrollment data, the Hardline system validates member, group, and provider information, as well as coverage information for each pharmacy claim based on client-specified parameters. Once this validation is completed, the Hardline system calculates the drug coverage amounts based on the benefit plan and client specifications.

Claims that have been successfully adjudicated for Business Associate ABC's clients are summarized by the pharmacy within the Hardline system. The Hardline system produces a check file to generate payments to pharmacies for adjudicated claims. Business Associate ABC summarizes all the adjudicated pharmacy claims data and bills the client organization on a contractually determined basis.

Based on actual drug usage, pharmaceutical manufacturers provide rebates to Business Associate ABC. Business Associate ABC accumulates the actual drug usage information based on processed pharmacy claims within the Quad system and invoices the manufacturers. Manufacturer invoices are created using the Sol Systems (SOL) financial system or the automated invoicing process and, in turn, are paid by manufacturers to Business Associate ABC via electronic transmission (ACH or Fedwire) or directly to the bank lockbox on a contractually determined basis. Received and reconciled manufacturer rebate payments are allocated to clients based on each client's actual usage of the rebate-eligible products.

The scope of this report includes only those Business Associate ABC's commercial and Medicare Part D clients on the Hardline, Quad and Customer CoOp systems. It does not include mail-order fulfillment processes that Business Associate ABC provides through its proprietary mail-order systems and does not include specialty services for its Canadian customers (including specialty pharmacy and distribution) that Business Associate ABC provides through its subsidiary.

Business Associate ABC has contracted with EDS to provide various services, including computer operations support, data center management, and telecommunications network management. The data center managed by EDS, which hosts all of Business Associate ABC's in-scope midrange and mainframe systems, is located in San Francisco, CA. Business Associate ABC receives Type II Statement on Auditing Standards (SAS) 70 reports from EDS on at least an annual basis, which report on the design and operating effectiveness of the controls that EDS is solely responsible for performing.

## 6. Security Program Analysis

The following sections include tables and charts of Business Associate ABC's information security practices.

### Overview of the security organization:

Business Associate ABC takes its responsibility as a healthcare and health benefits provider very seriously. Business Associate ABC serves its clients and members as a trusted custodian of the vital information entrusted to them every day on behalf of the hundreds of thousands of Americans it serves. Business Associate ABC has the policies, procedures, hardware, software and training in place to support its philosophy that data protection is a top priority.

Business Associate ABC is committed to protecting the confidentiality, integrity and availability of client and member data through vigilant focus on prevention, detection and response. For protection of sensitive information, including personal health information and personally identifiable information of members, Business Associate ABC has implemented multiple safeguards.

In addition to the safeguards and controls that have been implemented across its infrastructure, Business Associate ABC relies on regular audits of its security processes and procedures as a key component of continually identifying and reducing risk in its environment.

### Additional information regarding Business Associate ABC's security program:

<b>Types of security tools deployed</b>	<ol style="list-style-type: none"><li>1. Laptop Encryption</li><li>2. Wireless Network Scanning</li><li>3. Anti-Malware</li><li>4. Anti-Spam and Web Filtering</li><li>5. Windows Server and Workstation Configuration Standard</li><li>6. Vulnerability Scanning</li><li>7. Web Application Vulnerability Scanning</li><li>8. Network Security Scanning</li><li>9. Database Security and Compliance Scanning</li><li>10. Intrusion Detection</li><li>11. B2B File Transfer Encryption</li><li>12. Email Encryption</li><li>13. Remote Authentication Hard Token</li><li>14. Secure VPN</li></ol>
<b>3<sup>rd</sup> party assessments</b>	<ol style="list-style-type: none"><li>1. EDS Data Center SAS 70</li><li>2. PCI Assessment</li><li>3. Quarterly internal and external scans</li><li>4. Security strategy assessment</li><li>5. Active Internal Auditors</li></ol>

An additional description of controls is included in [Appendix A](#).

## 7. Assessment Results

To assist organizations with prioritizing and focusing efforts, HITRUST established a list of priority controls based on an analysis of breach data for the industry and input obtained from over 100 security professionals in healthcare. By implementing these controls, organizations mitigate threats and exposures that are most likely to result in a breach. An organization must implement these controls to qualify for CSF Certification.

### **High-risk exposure areas for Healthcare Organizations:**

- Insecure and/or unauthorized removable transportable media and laptops (internal and external movements)
- Insecure and/or unauthorized external electronic transmissions of covered information
- Insecure and/or unauthorized remote access by internal and third party personnel
- Insider snooping and data theft
- Malicious code and inconsistent implementation and update of prevention software
- Inadequate and irregular information security awareness for the entire workforce
- Lack of consistent network isolation between internal and external domains
- Insecure and/or unauthorized implementation of wireless technology
- Lack of consistent service provider, third party and product support for information security
- Insecure web development and applications
- Ineffective password management and protection
- Ineffective disposal of system assets

The following table is a summary of the results for Business Associate ABC of the testing of required controls:

Required for HITRUST Certification 2010	Overall Compliance	Comments	Corrective Action Plan Ref
<b>01.a Access Control Policy</b>	Yes	None	N/A
<b>01.b User Registration</b>	Yes	None	N/A
<b>01.d User Password Management</b>	Yes	None	N/A
<b>01.f Password Use</b>	Yes	None	N/A
<b>01.h Clear Desk and Clear Screen Policy</b>	Yes	None	N/A
<b>01.i Policy on Use of Network Services</b>	Yes	None	N/A
<b>01.j User Authentication for External Connections</b>	Yes	None	N/A
<b>01.m Segregation in Networks</b>	Yes	None	N/A
<b>01.n Network Connection Control</b>	Yes	None	N/A
<b>01.o Network Routing Control</b>	Yes	None	N/A
<b>01.q User Identification and Authentication</b>	Yes	None	N/A
<b>01.r Password Management System</b>	Yes	None	N/A
<b>01.v Information Access Restriction</b>	Yes	None	N/A
<b>01.w Sensitive System Isolation</b>	Yes	None	N/A
<b>01.x Mobile Computing and Communications</b>	Yes	None	N/A
<b>01.y Teleworking</b>	Yes	None	N/A
<b>02.a Roles and Responsibilities</b>	Yes	None	N/A
<b>02.d Management Responsibilities</b>	Yes	None	N/A
<b>02.e Information Security Awareness, Education, and Training</b>	Yes	None	N/A
<b>04.a Information Security Policy Document</b>	Yes	None	N/A
<b>04.b Review of the Information Security Policy</b>	Yes	None	N/A
<b>05.a Management Commitment to Information Security</b>	Yes	None	N/A
<b>05.b Information Security Coordination</b>	Yes	None	N/A
<b>05.i Identification of Risks Related to External Parties</b>	Yes	None	N/A
<b>05.k Addressing Security in Third Party Agreements</b>	Yes	None	N/A

Required for HITRUST Certification 2010	Overall Compliance	Comments	Corrective Action Plan Ref
06.e Prevention of Misuse of Information Assets	Yes	None	N/A
06.g Compliance with Security Policies and Standards	Yes	None	N/A
07.c Acceptable Use of Assets	Yes	None	N/A
08.l Secure Disposal or Re-Use of Equipment	Yes	None	N/A
09.aa Audit Logging	Yes	None	N/A
09.ab Monitoring System Use	Yes	None	N/A
09.ac Protection of Log Information	Yes	None	N/A
09.ae Fault Logging	Yes	None	N/A
09.af Clock Synchronization	Yes	None	N/A
09.c Segregation of Duties	Yes	None	N/A
09.e Service Delivery	Yes	None	N/A
09.f Monitoring and Review of Third Party Services	Yes	None	N/A
09.g Managing Changes to Third Party Services	Yes	None	N/A
09.j Controls Against Malicious Code	Yes	None	N/A
09.m Network Controls	Yes	None	N/A
09.o Management of Removable Media	Yes	None	N/A
09.p Disposal of Media	Yes	None	N/A
09.q Information Handling Procedures	Yes	None	N/A
09.s Information Exchange Policies and Procedures	Yes	None	N/A
10.b Input Data Validation	Yes	None	N/A
10.f Policy on the Use of Cryptographic Controls	Yes	None	N/A
10.l Outsourced Software Development	Yes	None	N/A
10.m Control of Technical Vulnerabilities	Yes	None	N/A
11.a Reporting Information Security Events	Yes	None	N/A
11.c Responsibilities and Procedures	Yes	None	N/A

## 8. Overall Security Program Summary

HITRUST evaluates Business Associate ABC’s security program overall at a **Level 3+** rating.

HITRUST leverages the concepts and rating scheme of the NISTIR 7358 standard - Program Review for Information Security Management Assistance (PRISMA) to assess an organizations security management program. The methodology is a proven and successful scalable process and approach to evaluating an organization’s information security program. The structure of a PRISMA Review is based upon the Software Engineering Institute’s (SEI) former Capability Maturity Model (CMM), where an organization’s developmental advancement is measured by one of five maturity levels. The rating is an indicator of an organization’s ability to protect information in a sustainable manner.

Maturity Level	Evidence is in place to demonstrate that the organization:
Level 1-	Has an informal security program
Level 1	<b>Relies on policies to enforce the majority</b> of the HITRUST critical control areas and the individual controls apply to the majority of the systems within the assessment scope
Level 1+	<b>Relies on policies to enforce all</b> of the HITRUST critical control areas and the individual controls apply to the all of the systems within the assessment scope
Level 2-	<b>Has policies and supporting procedures and technologies that can be used to enforce some</b> of the HITRUST critical control areas and the individual controls apply to some of the systems within the assessment scope
Level 2	<b>Has policies and supporting procedures and technologies that can be used to enforce the majority</b> of the HITRUST critical control areas and the individual controls apply to the majority of the systems within the assessment scope
Level 2+	<b>Has policies and supporting procedures and technologies that can be used to enforce all</b> of the HITRUST critical control areas and the individual controls apply to all of the systems within the assessment scope
Level 3-	<b>Has policies and supporting procedures and technologies that are consistently used to enforce some</b> of the HITRUST critical control areas and the individual controls apply to some of the systems within the assessment scope
Level 3	<b>Has policies and supporting procedures and technologies that are consistently used to enforce the majority</b> of the HITRUST critical control areas and the individual controls apply to the majority of the systems within the assessment scope
Level 3+	<b>Has policies and supporting procedures and technologies that are consistently used to enforce all</b> of the HITRUST critical control areas and the individual controls apply to all of the systems within the assessment scope
Level 4-	<b>Routinely conducts tests</b> to evaluate the adequacy and effectiveness of implemented controls for <b>some</b> of the HITRUST critical

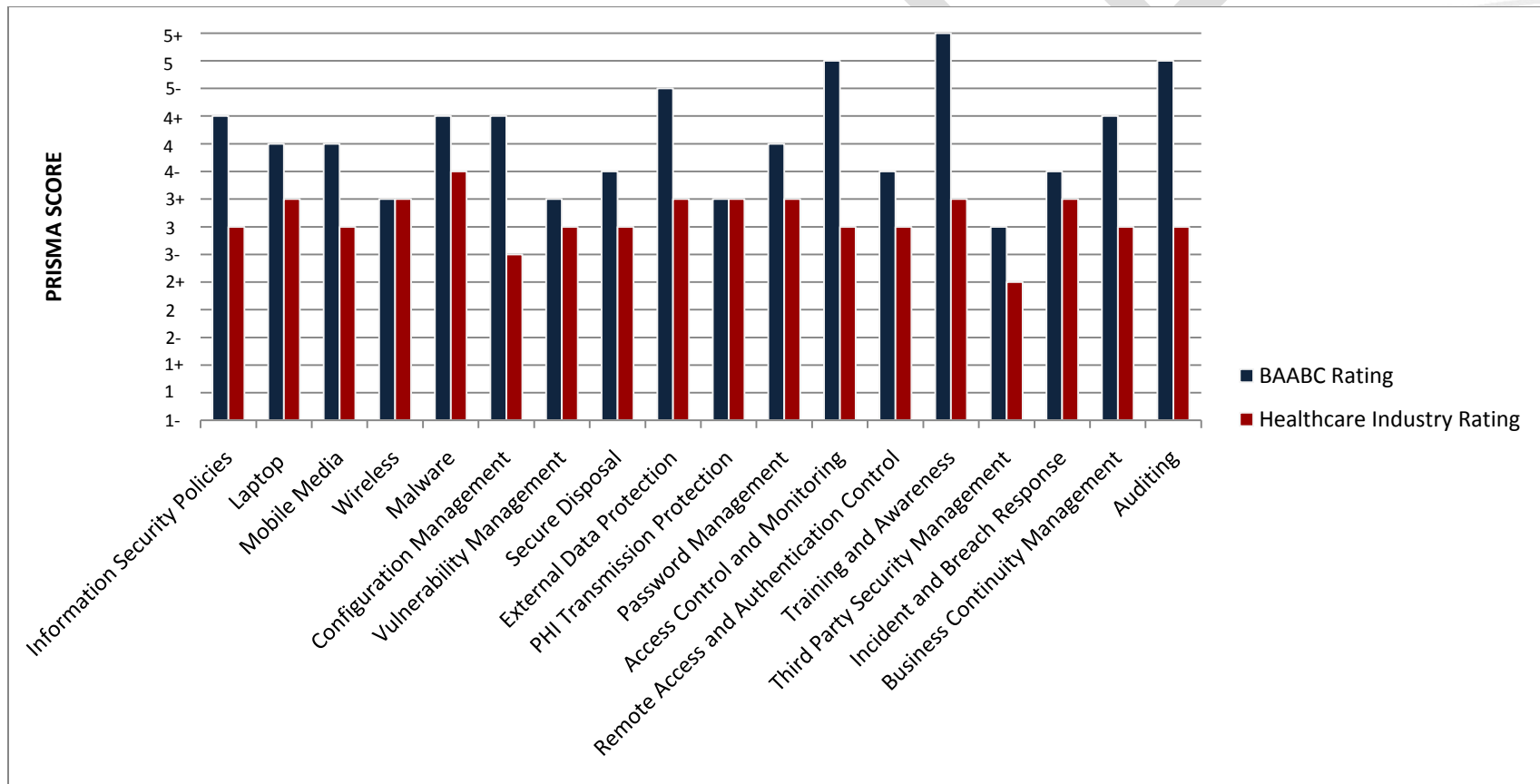
Maturity Level	Evidence is in place to demonstrate that the organization:
	control areas and the individual controls apply to some of the systems within the assessment scope
Level 4	<b>Routinely conducts tests</b> to evaluate the adequacy and effectiveness of implemented controls for the <b>majority</b> of the HITRUST critical control areas and the individual controls apply to the majority of the systems within the assessment scope
Level 4+	<b>Routinely conducts tests</b> to evaluate the adequacy and effectiveness of implemented controls <b>for all</b> of the HITRUST critical control areas and the individual controls apply to all of the systems within the assessment scope
Level 5-	<b>Consistently produces and actively monitors status metrics</b> for the information security program as well as <b>some</b> of the individual HITRUST critical control areas and the individual controls apply to some of the systems within the assessment scope
Level 5	<b>Consistently produces and actively monitors status metrics</b> for the information security program as well as the <b>majority</b> of the individual HITRUST critical control areas and the individual controls apply to the majority of the systems within the assessment scope
Level 5+	<b>Consistently produces and actively monitors status metrics</b> for the information security program as well as <b>all</b> of the individual HITRUST critical control areas and the individual controls apply to all of the systems within the assessment scope

The HITRUST CSF Assurance program is intended to gather and report information in an efficient and effective manner. An organization should use this assessment report as a component of its overall risk management program. Each organization’s risk management program should define the potential exposure for its business partners and the corresponding assurance required of those controls. The program should also leverage the results of this assessment to evaluate the risks associated with a business relationship and the corresponding risk mitigation strategy. The assessment is not a substitute for a comprehensive risk management program, but is a critical data point in the analysis of risk. The assessment should also not be a substitute for management oversight and decision making, but again, leveraged as key input.

The results summarized in this document are based upon a collection of methodologies and tests interacting at a single point in time with technology that is continually changing and becoming ever more complex. Any projection to the future of the findings contained in this document is subject to the risk that, because of change, they may no longer portray the system or environment in existence at that time. The information gathered is subject to inherent limitations and, accordingly, control failures may occur and not be detected.

## 9. Breakdown by CSF Control Areas Required for Certification

The required controls for certification identified in the CSF reflect the controls needed to mitigate the most common sources of breaches for the industry. An organization must achieve a level 3 for each control area to qualify for certification. In some circumstances, a level 3- is acceptable if the organization has existing projects underway to further deploy a control to the rest of their environment. The industry rating is based on the survey results of organizations within HITRUST’s leadership group. These organizations reflect larger institutions with generally robust security programs.



CSF Control Areas	Rating	Comments
<b>Laptop Security</b>	<b>4+</b>	<p>HIPAA/HITECH Committee is established and comprises of multiple departments. It is chartered with defining an information security program with supporting policies and procedures for safeguarding PHI. An overarching information security policy document was developed covering security principles, physical security, access control, destruction, network security, auditing, security breaches, and security with customers.</p> <p>Higher ratings can be achieved by:</p> <ul style="list-style-type: none"> <li>• Reviewing and updating the information security policy and supporting procedures when material changes are made to the organization or environment, or to account for new regulatory requirements and best practices.</li> <li>• Ensuring senior leadership has overall accountability for the information security policy and signs off on an annual basis.</li> </ul>
<b>Laptop Security</b>	<b>4-</b>	<p>CREDANT data encryption solution is deployed and operating for all laptops in the environment.</p> <p>Higher ratings can be achieved by:</p> <ul style="list-style-type: none"> <li>• Periodically evaluating the laptop security measures including encryption and firewall to ensure they are installed and operating correctly on all devices. Many tools have centralized management consoles which can monitor and alert security personnel if the tool is not working correctly.</li> <li>• Defining metrics for laptop security including encryption and firewall to monitor and track deployment and operating effectiveness. The HITRUST CHIP-Questionnaire outlines a number of metrics that should be considered.</li> </ul>
<b>Mobile Media Security</b>	<b>4-</b>	<p>CREDANT data encryption solution, which has the capability to protect mobile media, is deployed and operating on all laptops and desktops in the environment.</p> <p>Higher ratings can be achieved by:</p> <ul style="list-style-type: none"> <li>• Provide authorized users with approved USB devices with encryption enabled.</li> <li>• Periodically evaluating the mobile media security measures, including encryption and use, to ensure they are installed and operating correctly on all devices.</li> <li>• Defining metrics for mobile media security, including encryption and use, to monitor</li> </ul>

		and track deployment and operating effectiveness. The HITRUST CHIP-Questionnaire outlines a number of metrics that should be considered.
<b>Wireless Security</b>	<b>3+</b>	<p>All wireless network access points are protected with WPA/2 security protocols. Guest access is segmented from internal access. Both network and guest access require authentication prior to joining the network.</p> <p>Higher ratings can be achieved by:</p> <ul style="list-style-type: none"> <li>• Regularly scanning for rogue wireless access points in the organization’s environment and disabling any devices found.</li> <li>• Defining metrics for wireless security including implementation of security protocols, vulnerabilities found, and rogue access points found, and monitor and track deployment and operating effectiveness. The HITRUST CHIP-Questionnaire outlines a number of metrics that should be considered.</li> </ul>
<b>Malware Protection</b>	<b>4+</b>	<p>Anti-malware is deployed to all of the workstations and servers in the environment. The tool is configured to automatically receive updates from a centrally managed server on a daily basis. A centralized dashboard capability is enabled and utilized to monitor the anti-malware solution to ensure the definitions are up-to-date.</p> <p>Higher ratings can be achieved by:</p> <ul style="list-style-type: none"> <li>• Defining metrics for malware security for both workstations and servers, and monitor and track deployment and operating effectiveness. The HITRUST CHIP-Questionnaire outlines a number of metrics that should be considered.</li> </ul>
<b>Configuration Management</b>	<b>4+</b>	<p>All of the systems’ clocks are synchronized to support logging. A server security policy is developed for Windows, Linux, and UNIX systems. Policy and procedural documentation is defined for the secure build and configuration of all types of servers and databases implemented. All workstations, servers, and databases are scanned regularly to verify compliance with the configuration standard.</p> <p>Higher ratings can be achieved by:</p> <ul style="list-style-type: none"> <li>• Defining metrics for configuration management for workstations, servers, databases, and monitoring and tracking deployment and operating effectiveness. The HITRUST CHIP-Questionnaire outlines a number of metrics that should be considered.</li> </ul>

<b>Vulnerability Management</b>	<b>3+</b>	<p>A policy requires the IT Team keep a full inventory of all computer equipment and software in use throughout the organization. An inventory is regularly taken and managed. Third party vulnerability scans are performed on an annual basis for both the internal and external environment. Web application vulnerability assessments are performed on an annual basis and after any significant changes to the environment.</p> <p>Higher ratings can be achieved by:</p> <ul style="list-style-type: none"> <li>• Developing formal procedures and timelines for remediating any critical or high vulnerabilities discovered as a result of the scans and/or assessments.</li> <li>• Defining metrics for vulnerability management and monitoring and tracking deployment and operating effectiveness. The HITRUST CHIP-Questionnaire outlines a number of metrics that should be considered.</li> </ul>
<b>Secure Disposal</b>	<b>4-</b>	<p>Data destruction procedure flow is defined for destroying hardcopy and electronic media. Third party bins are placed throughout the facility for securing documents to be destroyed.</p> <p>Higher ratings can be achieved by:</p> <ul style="list-style-type: none"> <li>• Regularly testing the effectiveness of the data destruction process by confirming information is inaccessible on a random sample of destroyed media and confirming logs are retained.</li> <li>• Defining metrics for media disposal and monitoring and tracking operating effectiveness. The HITRUST CHIP-Questionnaire outlines a number of metrics that should be considered.</li> </ul>
<b>PHI Transmission Protection</b>	<b>3+</b>	<p>Communications are maintained via SSL/TLS for web portals, secure VPN for terminal services, or site-to-site VPN. The organization’s entire web infrastructure is standardized on SSL/TLS. Email is automatically scanned to detect and encrypt email messages containing PHI and other sensitive information. Web application vulnerability assessments are performed on an annual basis and after any significant changes to the environment.</p> <p>Higher ratings can be achieved by:</p> <ul style="list-style-type: none"> <li>• Regularly reviewing third party connections to confirm security, and that they are still required for business purposes.</li> <li>• Defining metrics for PHI transmission protection and monitoring and tracking deployment and operating effectiveness. The HITRUST CHIP-Questionnaire outlines a number of metrics that should be considered.</li> </ul>

<b>Password Management</b>	<b>4</b>	<p>A policy requires databases and database servers have default passwords changed or accounts removed. Active directory policy is configured to require strong passwords in accordance with the CSF requirements. Default vendor accounts are removed or disabled and default passwords are changed during the build and QA process for all workstations, servers, databases, and applications. All workstations, servers, databases, and applications are regularly scanned for default accounts and potentially weak passwords.</p> <p>Higher ratings can be achieved by:</p> <ul style="list-style-type: none"> <li>Defining metrics for password protection and monitoring and tracking deployment and operating effectiveness. The HITRUST CHIP-Questionnaire outlines a number of metrics that should be considered.</li> </ul>
<b>Remote Access and Authentication Control</b>	<b>4-</b>	<p>Remote access for employees is granted through terminal services via a secure VPN. Customers are given remote access via a site-to-site VPN using an SSL client. Two-factor authentication is required for all remote VPN access. IP restrictions are setup for each customer. Remote access points are documented as part of the organization’s network diagram, and updated at least annually.</p> <p>Higher ratings can be achieved by:</p> <ul style="list-style-type: none"> <li>Maintaining audit logs and developing procedures to regularly review the logs for suspicious activity.</li> <li>Defining metrics for remote access control and monitoring, and monitoring and tracking deployment and operating effectiveness. The HITRUST CHIP-Questionnaire outlines a number of metrics that should be considered.</li> </ul>
<b>Third Party Security Management</b>	<b>3</b>	<p>The security practices of third parties are reviewed where the organization’s information is shared. Standard information security contract language is defined that addresses the business associate agreement requirements of HIPAA and HITECH.</p> <p>Higher ratings can be achieved by:</p> <ul style="list-style-type: none"> <li>Regularly reviewing the information security contract language and business associate agreements at least on an annual basis or when any significant changes are made affecting the information sharing arrangement.</li> <li>Requesting business associates provide reports initially and on a recurring basis of information security assessments performed internally or by a qualified third party. CSF Validated or Certified reports under the CSF Assurance Program provide a</li> </ul>

		<p>practical solution.</p> <ul style="list-style-type: none"> <li>Defining metrics for third party security management, and monitoring and tracking deployment and operating effectiveness. The HITRUST CHIP-Questionnaire outlines a number of metrics that should be considered.</li> </ul>
<b>Incident and Breach Response</b>	<b>4-</b>	<p>HIPAA/HITECH committee is formed and tasked with the development of an information security breach response program. An incident / breach form is available for users to submit discovered or potential breaches to information security personnel.</p> <p>Higher ratings can be achieved by:</p> <ul style="list-style-type: none"> <li>Regularly testing the breach response program and procedures through tabletop exercises and controlled scenarios and updating the program based on any resulting issues.</li> <li>Defining metrics for information security incident and breach response, and monitoring and tracking deployment and operating effectiveness. The HITRUST CHIP-Questionnaire outlines a number of metrics that should be considered.</li> </ul>
<b>Business Continuity Management</b>	<b>4+</b>	<p>The organization's environment is setup in a mesh topology to replicate data and processing across multiple locations. SAN and host-based replication is implemented. Policies supported by detailed procedures are defined for business continuity management and disaster recovery for each system and facility in the organization's environment. The business continuity and disaster recovery program and procedures are regularly tested through tabletop exercises and controlled scenarios, and the program is updated based on any resulting issues.</p> <p>Higher ratings can be achieved by:</p> <ul style="list-style-type: none"> <li>Defining metrics for business continuity and disaster recovery, and monitoring and tracking deployment and operating effectiveness. The HITRUST CHIP-Questionnaire outlines a number of metrics that should be considered.</li> </ul>

## 10. Compliance Scorecards

The CSF is an overarching security framework that incorporates and leverages the existing security requirements placed upon healthcare organizations, including federal (e.g., HIPAA and HITECH), state, third party (e.g., PCI and COBIT), and other government agencies (e.g., NIST, FTC, and CMS). The framework enables organizations to assess once and report against multiple sets of requirements, which is aligned with HITRUST’s objectives of simplifying and reducing the cost of compliance for the industry.

This report includes the following scorecards:

- HIPAA Security Rule
- COBIT DS5

Each scorecard includes color coded ratings that relate to the definitions in the table below. Based on the assessment, Business Associate ABC’s state of compliance with each of the requirements is denoted by a black line on the relevant color coded rating. It is important to denote that the scorecards do not represent a formal certification against the particular requirements, as the requirements either do not have a formal certification (e.g., HIPAA) or the assessment did not follow the unique certification processes prescribed by the certification authority (e.g., ISO).

Rating Definition – The rating is intended as a data point regarding security compliance against a particular requirement. Your organization should consider this information within your overall risk management framework, and your response and mitigation strategy should align with your risk analysis.	
<b>G</b>	The assessment identified controls that are implemented and aligned with the requirements
<b>Y</b>	The assessment identified controls that are partially implemented and aligned with the requirements
<b>R</b>	The assessment identified no controls that are implemented and aligned with the requirements

Testing Definition – Certain controls listed for each scorecard are tested as part of the overall CSF Assurance assessment. The testing performed is indicated as follows:	
<input type="radio"/>	The control was not tested.
<input checked="" type="radio"/>	The control was partially tested.
<input checked="" type="radio"/>	The control was fully tested.

## HIPAA Security Rule

A. General Rules	1. Security Rule and Privacy Rule Distinctions		N/A
	2. Level of Detail		N/A
	3. Implementation Specifications		N/A
	4. Examples		N/A
B. Applicability (164.302)			N/A
C. Transition to the Final Rule (164.304)			N/A
D. General Rules (164.306)	1. Scope of Health Information Covered by the Rule (164.306(a))		N/A
	2. Technology-Neutral Standards		N/A
	3. Miscellaneous Comments		N/A
E. Administrative Safeguard (164.308)	Assigned Security Responsibility	(a)(2) Authority and Responsibility for the Information Security Program	
	Business Associate Contracts and Other Arrangements	(b)(1) Business associate contracts and other arrangements	
		(b)(2)(i) Business associate contracts and other arrangements - Covered Entity Exception	
		(b)(2)(ii) Business associate contracts and other arrangements - Group Health Plan or HMO Exception	
		(b)(2)(iii) Business associate contracts and other arrangements - Service Agency Exception	
		(b)(3) Business associate contracts and other arrangements	
		(b)(4) Written contract or other arrangement (Required)	
		(b)(4) Written contract or other arrangement (Required)	
	Contingency Plan	(a)(7)(i) Emergency Response Policies and Procedures	
		(a)(7)(ii)(A) Data backup plan (Required)	
		(a)(7)(ii)(B) Disaster recovery plan (Required)	
		(a)(7)(ii)(C) Emergency mode operation plan (Required)	
		(a)(7)(ii)(D) Testing and revision procedures (Addressable)	
		(a)(7)(ii)(E) Applications and data criticality analysis (Addressable)	
Evaluation	(a)(8) Security Audits		
Information Access	(a)(4)(i) Access Control Policies and		

	Management	Procedures	
		(a)(4)(ii)(A) Isolating health care clearinghouse functions (Required)	●
		(a)(4)(ii)(B) Access authorization (Addressable)	○
	Security Awareness and Training	(a)(4)(ii)(C) Access establishment and modification (Addressable)	○
		(a)(5)(i) Security Awareness Program	●
		(a)(5)(ii)(A) Security reminders (Addressable)	●
		(a)(5)(ii)(B) Protection from malicious software (Addressable)	●
		(a)(5)(ii)(C) Log-in monitoring (Addressable)	●
	Security Incident Procedures	(a)(5)(ii)(D) Password management (Addressable)	●
		(a)(6)(i) Incident Response Policies and Procedures	●
		(a)(6)(ii) Response and Reporting (Required)	○
	Security Management process	(a)(1)(i) Security Policy Implementation	○
		(a)(1)(ii)(A) Risk analysis (Required)	○
		(a)(1)(ii)(B) Risk management (Required)	○
		(a)(1)(ii)(C) Sanction policy (Required)	○
		(a)(1)(ii)(D) Information system activity review (Required)	○
	Workforce Security	(a)(3)(i) Access Control Policies and Procedures	●
		(a)(3)(ii)(A) Authorization and/or supervision (Addressable)	○
		(a)(3)(ii)(B) Workforce clearance procedure (Addressable)	○
		(a)(3)(ii)(C) Termination procedures (Addressable)	○
F. Physical Safeguard (164.310)	Device and Media Controls	(d)(1) Receipt and Removal	○
		(d)(2)(i) Disposal (Required)	●
		(d)(2)(ii) Media re-use (Required)	●
		(d)(2)(iii) Accountability (Addressable)	○
		(d)(2)(iv) Data backup and storage (Addressable)	○

	Facility Access Controls	(a)(1) Physical Access Policy and Procedures	●
		(a)(2)(i) Contingency operations (Addressable)	●
		(a)(2)(ii) Facility security plan (Addressable)	●
		(a)(2)(iii) Access control and validation procedures (Addressable)	●
		(a)(2)(iv) Maintenance records (Addressable)	●
		Workstation Security	(c) Physical Workstation Safeguards
	Workstation Use	(b) Acceptable Use Policy	●
G. Technical Safeguard (164.312)	Access Control	(a)(1) Access Control Policies and Procedures	●
		(a)(2)(i) Unique user identification (Required)	●
		(a)(2)(ii) Emergency access procedure (Required)	●
		(a)(2)(iii) Automatic logoff (Addressable)	●
		(a)(2)(iv) Encryption and decryption (Addressable)	●
	Audit controls	(b) Logging	●
	Integrity	(c)(1) Integrity	●
		(c)(2) Mechanism to authenticate electronic protected health information (Addressable)	○
	Person or Entity Authentication	(d) Non-Repudiation	●
	Transmission Security	(e)(1) Transmission Security	○
(e)(2)(i) Integrity controls (Addressable)		○	
(e)(2)(ii) Encryption (Addressable)		●	
H. Organizational Safeguard (164.314)	Business Associate Contracts or Other Arrangements	(a)(1)(i) Business associate contracts or other arrangements	●
		(a)(1)(ii) Business associate contracts or other arrangements	N/A
		(a)(1)(ii)(A) Business associate contracts or other arrangements	●
		(a)(1)(ii)(B) Business associate contracts or other arrangements	N/A
		(a)(2)(i) Business associate contracts or other arrangements	●

		(a)(2)(i)(A) Business associate contracts (Required)	
		(a)(2)(i)(B) Business associate contracts (Required)	
		(a)(2)(i)(C) Business associate contracts (Required)	
		(a)(2)(i)(D) Business associate contracts (Required)	
		(a)(2)(ii)(A) Business associate contracts or other arrangements	
		(a)(2)(ii)(A)(1) Other arrangements (Required)	
		(a)(2)(ii)(A)(2) Other arrangements (Required)	
		(a)(2)(ii)(B) Other arrangements (Required)	
		(a)(2)(ii)(C) Other arrangements (Required)	
	Requirements for Group Health Plans	(b)(1) Requirements for group health plans	
		(b)(2) Requirements for group health plans	
		(b)(2)(i) Implement Safeguards (Required)	
		(b)(2)(ii) Separation (Required)	
		(b)(2)(iii) Acknowledge Responsibility (Required)	
		(b)(2)(iv) Incident Reporting (Required)	
I. Policies, Procedures and Documentation Safeguards (164.316)	Documentation	(b)(1)(i) Documentation	
		(b)(1)(ii) Documentation	
		(b)(2)(i) Time limit (Required)	
		(b)(2)(ii) Availability (Required)	
		(b)(2)(iii) Updates (Required)	
	Policies and Procedures	(a) Policies and procedures	

## COBIT DS5

05 Ensure Systems Security	05.01 Management of IT Security	
	05.02 IT Security Plan	
	05.03 Identity Management	
	05.04 User Account Management	
	05.05 Security Testing, Surveillance and Monitoring	
	05.06 Security Incident Definition	
	05.07 Protection of Security Technology	
	05.08 Cryptographic Key Management	
	05.09 Malicious Software Prevention, Detection and Correction	
	05.10 Network Security	
	05.11 Exchange of Sensitive Data	

## Appendix A – Detailed Control Summary of Business Associate ABC

Below is a summary of information security controls implemented by Business Associate ABC<sup>1</sup>:

- Controls access points to its network through the use of commercial firewalls, router ACLs, IP masking, network IDS for inbound and outbound traffic, and regular vulnerability scans.
- Isolates internet accessible systems in a DMZ segmented from the internal network via commercial firewalls, and employs host-based IDS tools.
- Controls system and application access based on the principle of least privilege, issuing access through automated and manual processes that are documented, tracked and require approval; access reviews are conducted on a quarterly basis.
- Protects sensitive information in transit through public web portals using digital certificates and SSL 128-bit encryption.
- Protects sensitive information exchanged with third parties using FTP with PGP file encryption, client web portals using digital certificates and SSL 128-bit encryption, internet AS2 secure file transfer, and Connect:Direct over AT&T's Global Network Services.
- Employs physical security procedures including badge access, 24 hour monitoring, CCTV, and alarm systems; Business Associate ABC's data center is managed by EDS Enterprise Services (formerly EDS) that provides Business Associate ABC with an annual SAS 70 Type II report.
- Screens personnel based on job roles and responsibilities including criminal history, sex offender registry, federal watch lists, SSN trace, education verification, employment verification, professional license/registration, and drug screening.
- Trains personnel on corporate security policies during new hire orientation and annually thereafter; courses include HIPAA Privacy and Security, Code of Conduct, Internal Controls, and Confidential Information Protection.
- Regularly engages in independent, third party security assessments including annual PCI DSS compliance audits.
- Manages the overall security program via a cross-functional Information Protection Steering Committee providing strategic direction, business impact guidance, prioritization, governance, new ideas, and advocacy for information protection initiatives; the Committee is facilitating a shift from compliance-oriented information security to a risk-based, continual assessment and improvement model.

---

<sup>1</sup> This control summary is jointly created by the CSF Assessor's findings and the Assessed Entity's own documentation and description.

## Appendix B – Testing Summary

Below is a summary of the documentation reviewed and personnel interviewed for the controls outlined in the CHIP Questionnaire and CSF.

<b>Documentation</b>	<ul style="list-style-type: none"><li>• PCI DSS v1.2 Report on Compliance: February 2010</li><li>• SAS 70 Type II EDS Enterprise Services: October 2008 – September 2009</li><li>• Information System Security Policies v6.0: October 2009<ul style="list-style-type: none"><li>○ Acceptable Use Policies</li><li>○ Information Protection Policies</li><li>○ Perimeter Security Policies</li><li>○ Remote Access Policies</li><li>○ Physical Security Policies</li><li>○ Personnel Security Policies</li></ul></li><li>• Policies and Procedures for the Disposal of Desktops/Laptops and Destruction of Hard Drives and Blackberry Devices v3.1: October 2009</li><li>• Policies and Procedures for Teleworking</li><li>• Business Associate ABC Perimeter Networks Diagram v2.0: October 2009</li><li>• Sample of Disaster Recovery plans</li><li>• Sample of Third Party contracts</li><li>• Sample of Security Roles and Responsibilities</li></ul>
<b>Interviews</b>	<ul style="list-style-type: none"><li>• Jamie Hawk – Internal Audit</li><li>• John Whale – Midrange Application Management</li><li>• John Heisman – Midrange Application Management</li><li>• Shane Inland – Midrange Application Management</li><li>• Steve Rank – Security Administration/Verification</li><li>• Dan Ash – Security Administration/Verification</li><li>• Mary Canton – EDS Enterprise Services Security Management</li><li>• Nate Riser – Windows Security</li><li>• Christine Glenzer – Asset and Inventory Management</li><li>• Gene Cole – BCP/DR</li><li>• Matt Modin – Identity Management</li><li>• Jim Birch – Threat and Vulnerability Management</li><li>• Rob Roteger – Email Security</li><li>• Todd Stalsworth – B2B Gateway Manager</li><li>• Mark Cain – Security Compliance/Regulatory Support</li><li>• Jacob Larme - Security Compliance/Regulatory Support</li><li>• Dennis Hoster - Security Compliance/Regulatory Support</li><li>• Simon Cheng – Enterprise Architecture Security</li><li>• Colin Hallow – Enterprise Architecture Security</li><li>• Chris Lewman – Database Management</li></ul>

## Appendix C – Corrective Action Plan

HITRUST requires that an organization define a Corrective Action Plan (CAP) for all CSF Certification controls not met at a Level 3 PRISMA score. For general recommendations on areas of improvement, please see [Section 10](#).

1	2	3	4	5	6	7	8	9	10	11	12
Weakness Identifier	Weakness	HITRUST CSF Control Mapping	Point of Contact (POC)	Resources Required	Scheduled Completion Date	Milestones with Completion Dates	Changes to Milestones	How Identified	Status	Comments	Risk Level
<div style="position: absolute; top: 50%; left: 50%; transform: translate(-50%, -50%); opacity: 0.1; font-size: 100px; pointer-events: none;">           SAMPLE         </div>											

## Appendix D – Questionnaire Results

CHIP Questionnaire results would be inserted.

SAMPLE

## Appendix E – System Profile

The System Profile List developed by the CSF Assessor in conjunction with Business Associate ABC includes all of the systems that were within the scope of the assessment. The list includes the application name, platform, database information and if the system was included in other third-party assessments, such as a SAS 70.

System Characteristics							
System Name / ID	Group	Application	Hardware Platform	O/S	Database	Location	Prior Audit / Assessment
Customer CoOp	Customer CoOp	Customer CoOp	HP-UX	UNIX	Oracle	San Francisco, CA (EDS Hosting)	PCI_Feb. 2010
Hardline Rebates	Hardline Rebates	Quad	IBM Mainframe	AIX	DB2 Flat Files	San Francisco, CA (EDS Hosting)	PCI_Feb. 2010
IT Claims_BCR	IT Claims	BCR	IBM Mainframe	AIX	DB2	San Francisco, CA (EDS Hosting)	PCI_Feb. 2010
IT Claims_Benefit and Drug	IT Claims	Benefit and Drug	IBM Mainframe	AIX	Oracle DB2 UDB Flat Files	San Francisco, CA (EDS Hosting)	PCI_Feb. 2010
			Creed	Creed		San Francisco, CA (EDS Hosting)	PCI_Feb. 2010
IT Claims_Comm. and PharmA Claims	IT Claims	Commercial and PharmA Claims Systems	Hardline Mainframe		DB2 VSAM Files	San Francisco, CA (EDS Hosting)	PCI_Feb. 2010
			PharmA Mainframe		DB2 VSAM Files		
			Midrange	AIX	DB2 VSAM Files		
IT Claims_Hardline	IT Claims	Hardline	IBM Mainframe	AIX	DB2	San Francisco, CA (EDS Hosting)	PCI_Feb. 2010
IT Claims_Eligibility	IT Claims	Eligibility	IBM Mainframe	AIX	DB2 Oracle	San Francisco, CA (EDS Hosting)	SAS 70_EDS_Sep. 2009
Anchor Datawarehouse	Anchor Datawarehouse	Hardline Commercial	IBM Mainframe	AIX	DB2 Flat Files	San Francisco, CA (EDS Hosting)	SAS 70_EDS_Sep. 2009
ADW_Quick Contact	ADW	Quick Contact	HP-UX Apollo	UNIX Apollo	Oracle	San Francisco, CA (EDS Hosting)	SAS 70_EDS_Sep. 2009
ADW_ADW	ADW	ADW	IBM Mainframe	AIX Teradata	DB2 Teradata	San Francisco, CA (EDS Hosting)	SAS 70_EDS_Sep. 2009