

CSF Assurance Program Assessment Report

Business Associate ABC

January 31, 2011

Distribution of this report is limited to the following external organizations. Distribution beyond these organizations is a violation of the Participation Agreement and requires written permission from HITRUST:

- 1. Third Party Relying Organization**

Contents

1. HITRUST Background	3
2. Letter of Validation	4
3. Representation Letter from Management	5
4. Assessment Context.....	6
5. Overall Security Program Summary.....	7
6. Breakdown by CSF Control Areas Required for Certification.....	9
7. Compliance Scorecards.....	13
Appendix A – Corrective Action Plan	18
Appendix B – Questionnaire Results.....	19

SAMPLE

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 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.

For more information about HITRUST, the HITRUST CSF and other HITRUST offerings and programs, visit www.HITRUSTalliance.net.

2. Letter of Validation

January 31, 2011

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

Based upon representation from management as to the accuracy and completeness of information provided in the HITRUST CHIP Questionnaire and the limited procedures performed by HITRUST, the following business unit(s) and system(s) of the organization is(are) CSF Validated:

Business Associate ABC Health Solutions

HITRUST defines multiple levels of assurance for assessments performed under the CSF Assurance program: self assessment, remote assessment, or on-site assessment. The type of assessment performed for the above business unit is a self assessment.

The self assessment utilizes a questionnaire aligned with the compliance requirements of the healthcare industry. No testing was performed by a third party CSF Assessor to validate the results provided by the organization. The completed questionnaire was sent to HITRUST for review and final validation.

CSF Validated assessments allow both healthcare organizations and their business associates to realize the benefits of more assurance with fewer resources by aligning with the CSF and leveraging HITRUST's common reporting processes and tools. CSF Validated assessments are designed to occur along an incremental path towards certification. Organizations can actively move along the Validated path towards becoming CSF Certified in a measured way, while realizing at an early stage the benefits of a common means to assess security controls and communicate compliance.

Additional information on the CSF Assurance program can be found at the HITRUST website:
www.hitrustalliance.net.

HITRUST

3. Representation Letter from Management

January 31, 2011

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

In connection with our engagement of HITRUST LLC 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 Assurance program.
- We have responded fully to all inquiries made to us by you during the engagement.
- We have completed the HITRUST Self Assessment questionnaire to the best of our knowledge and with integrity as to what controls we have in place and are operating effectively, and where controls are not in place.
- 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 validation 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

Prepared For	Business Associate ABC 2 Business Associate St. Anchorage, AK 93127
Contact	Alan Park Director, Information Security Alan.park@baabc.com
Assessed Entity	Business Associate ABC
Date of Report	October 10, 2010
Period of Assessment	September 2010
Date of Quality Assurance by HITRUST	October 2010
Type of Assessment	Self Assessment
Company Background	Business Associate ABC is Alaska’s premier full service pharmacy benefit management (PBM) company.
Number of covered lives	7 Million
Geographic scope of operations considered for the assessment	Multi-state
Number of employees	1000
Authoritative sources in scope of the review	<ul style="list-style-type: none"> • HIPAA Security Rule
Systems in scope of the review	<ul style="list-style-type: none"> • Hardline • Quad • Customer CoOp
Summary of the organization’s security program	<p>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.</p> <p>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.</p>

5. 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	Relies on policies to enforce the majority of the HITRUST critical control areas and the individual controls apply to the majority of the systems within the assessment scope
Level 1+	Relies on policies to enforce all of the HITRUST critical control areas and the individual controls apply to the all of the systems within the assessment scope
Level 2-	Has policies and supporting procedures and technologies that can be used to enforce some of the HITRUST critical control areas and the individual controls apply to some of the systems within the assessment scope
Level 2	Has policies and supporting procedures and technologies that can be used to enforce the majority of the HITRUST critical control areas and the individual controls apply to the majority of the systems within the assessment scope
Level 2+	Has policies and supporting procedures and technologies that can be used to enforce all of the HITRUST critical control areas and the individual controls apply to all of the systems within the assessment scope
Level 3-	Has policies and supporting procedures and technologies that are consistently used to enforce some of the HITRUST critical control areas and the individual controls apply to some of the systems within the assessment scope
Level 3	Has policies and supporting procedures and technologies that are consistently used to enforce the majority of the HITRUST critical control areas and the individual controls apply to the majority of the systems within the assessment scope
Level 3+	Has policies and supporting procedures and technologies that are consistently used to enforce all of the HITRUST critical control areas and the individual controls apply to all of the systems within the assessment scope
Level 4-	Routinely conducts tests to evaluate the adequacy and effectiveness of implemented controls for some of the HITRUST critical control areas and the individual controls apply to some of the systems within the assessment scope

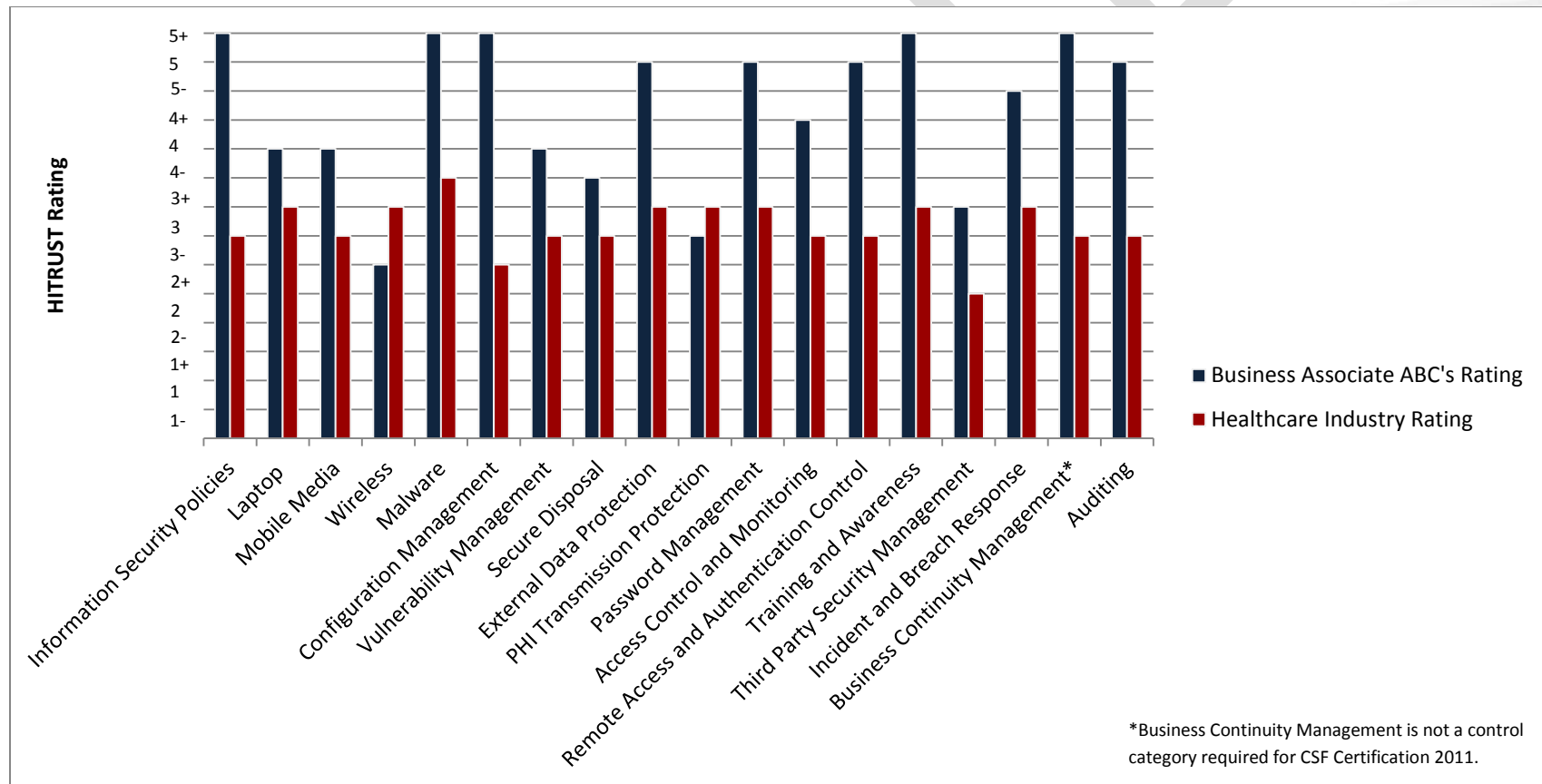
Maturity Level	Evidence is in place to demonstrate that the organization:
Level 4	Routinely conducts tests to evaluate the adequacy and effectiveness of implemented controls for the majority of the HITRUST critical control areas and the individual controls apply to the majority of the systems within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

6. 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 its 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
Information Security Policies	5+	None
Laptop Security	4	Higher ratings can be achieved by: <ul style="list-style-type: none"> 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.
Mobile Media Security	4	Higher ratings can be achieved by: <ul style="list-style-type: none"> 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. 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.
Wireless Security	3-	Higher ratings can be achieved by: <ul style="list-style-type: none"> Regularly scanning for rogue wireless access points in the organization's environment and disabling any devices found. 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.
Malware Protection	5+	None
Configuration Management	5+	None
Vulnerability Management	4	Higher ratings can be achieved by: <ul style="list-style-type: none"> Developing formal procedures and timelines for remediating any critical or high

		<p>vulnerabilities discovered as a result of the scans and/or assessments.</p> <ul style="list-style-type: none"> 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.
Secure Disposal	4-	<p>Higher ratings can be achieved by:</p> <ul style="list-style-type: none"> 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. Defining metrics for media disposal and monitoring and tracking operating effectiveness. The HITRUST CHIP-Questionnaire outlines a number of metrics that should be considered.
External Breach Protection	5	None
PHI Transmission Protection	3	<p>Higher ratings can be achieved by:</p> <ul style="list-style-type: none"> Regularly reviewing third party connections to confirm security, and that they are still required for business purposes. 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.
Password Management	5	None
Access Control and Monitoring	4+	<p>Higher ratings can be achieved by:</p> <ul style="list-style-type: none"> Defining metrics for user 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.
Remote Access and Authentication Control	5	None
Training and Awareness	5+	None

Third Party Security Management	3+	<p>Higher ratings can be achieved by:</p> <ul style="list-style-type: none"> • 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. • 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 practical solution. • 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.
Incident and Breach Response	5-	None
Business Continuity Management	5+	None
Auditing	5	None

7. 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

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.	
G	The assessment identified controls that are implemented and aligned with the requirements
Y	The assessment identified controls that are partially implemented and aligned with the requirements
R	The assessment identified no controls that are implemented and aligned with the requirements

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	Green
	Business Associate Contracts and Other Arrangements	(b)(1) Business associate contracts and other arrangements	Green
		(b)(2)(i) Business associate contracts and other arrangements - Covered Entity Exception	Green
		(b)(2)(ii) Business associate contracts and other arrangements - Group Health Plan or HMO Exception	Green
		(b)(2)(iii) Business associate contracts and other arrangements - Service Agency Exception	Green
		(b)(3) Business associate contracts and other arrangements	Green
		(b)(4) Written contract or other arrangement (Required)	Green
	Contingency Plan	(a)(7)(i) Emergency Response Policies and Procedures	Yellow-Green
		(a)(7)(ii)(A) Data backup plan (Required)	Green
		(a)(7)(ii)(B) Disaster recovery plan (Required)	Yellow
		(a)(7)(ii)(C) Emergency mode operation plan (Required)	Green
		(a)(7)(ii)(D) Testing and revision procedures (Addressable)	Yellow
		(a)(7)(ii)(E) Applications and data criticality analysis (Addressable)	Green
	Evaluation	(a)(8) Security Audits	Green

	Information Access Management	(a)(4)(i) Access Control Policies and Procedures	
		(a)(4)(ii)(A) Isolating health care clearinghouse functions (Required)	
		(a)(4)(ii)(B) Access authorization (Addressable)	
		(a)(4)(ii)(C) Access establishment and modification (Addressable)	
	Security Awareness and Training	(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)	
		(a)(5)(ii)(D) Password management (Addressable)	
	Security Incident Procedures	(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	

Appendix A – 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 6.

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
<p style="text-align: center; font-size: 48px; opacity: 0.2; transform: rotate(-15deg);">SAMPLE</p>											

Appendix B – Questionnaire Results

CHIP Questionnaire results would be inserted.