Outsourcing IT Under BAA:

Exploring Cloud Certification for Healthcare

Chris Davis

Senior Solutions Architect

Verizon Enhanced Services

February 6, 2014

CONTENTS

Introductions

Who I am
What I do
What this is about

Approach

Context
Methods
Literature

Findings

SSAE 16 SOC 2
ISO 27001
PCI DSS
FedRAMP

Conclusions

Effectiveness
Opportunity

Introductions: Who I am

20 years in IT

- Information Security assessment and audit, architecture, management
- Compliance and Risk Management / GRC
- Software and Product Development

Multi-sector experience

- Healthcare
- Pharmaceutical
- Financial
- Federal
- Energy and Utility
- Retail

International scope

- Privacy in EMEA and APAC
- Cross-border data flows

Introductions: What I do

2002 – 2012

building consolidated information security, availability, quality, and privacy audit and assessment programs for multi-national corporations

ISO
BITS
FINANCIAL SERVICES ROUNDTABLE
CSA
FedRAMP℠
NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION
DIRECTOR OF CENTRAL INTELLIGENCE
INTELLIGENCE COMMUNITY
PCI
FFIEC
COBIT®
AICPA
DEPARTMENT OF DEFENSE
DODIIS
INTELLIGENCE INFORMATION SYSTEM
NIST
ITIL®
COSO

2012 - Present

hosting services for Healthcare and Pharmaceuticals

DEPARTMENT OF HEALTH & HUMAN SERVICES · USA
CMS
HITRUST
Health Information Trust Alliance
ISPE®
FDA

Introductions: What this is about

Commonalities between the HIPAA Security rule and common information security certification standards.

More precisely: how these certification standards, as applied to conventional IT Hosting architectures, could be leveraged to demonstrate compliance with HIPAA Security requirements.

Four certification standards:

- SSAE 16 SOC 2
- ISO 27001
- PCI DSS
- FedRAMP

Introductions: Why talk about this?

The economics work

The Cloud, alongside mobile technology, is the next step in computing evolution

Security is the #1 concern among customers when considering the Cloud and other IT hosting services

Approach: Context

Common basic IT hosting services: colocation, managed hosting, Cloud

Business Associate is willing to sign BAA

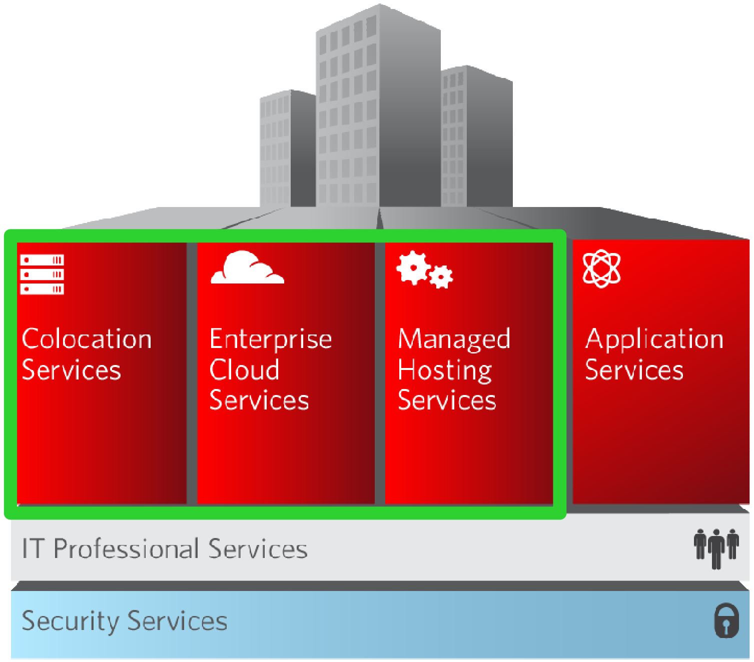
Authorizations

1) No authorization to access, use, or disclose ePHI
2) Only authorized access to information systems containing ePHI to perform routine administrative tasks

Business Associate responsibilities do not include applications or data

Services located in U.S. jurisdictions

ePHI does not traverse national boundaries



Approach: Methods

Methodology comparison

Is the certification process rigorous enough to also meet the audit protocol as specified by the ONC?

Sufficient

Potential

Insufficient

Evidence comparison

If a service provider is awarded certification X, could the evidence contained in the working papers of that certification also be used during a HIPAA Security audit?

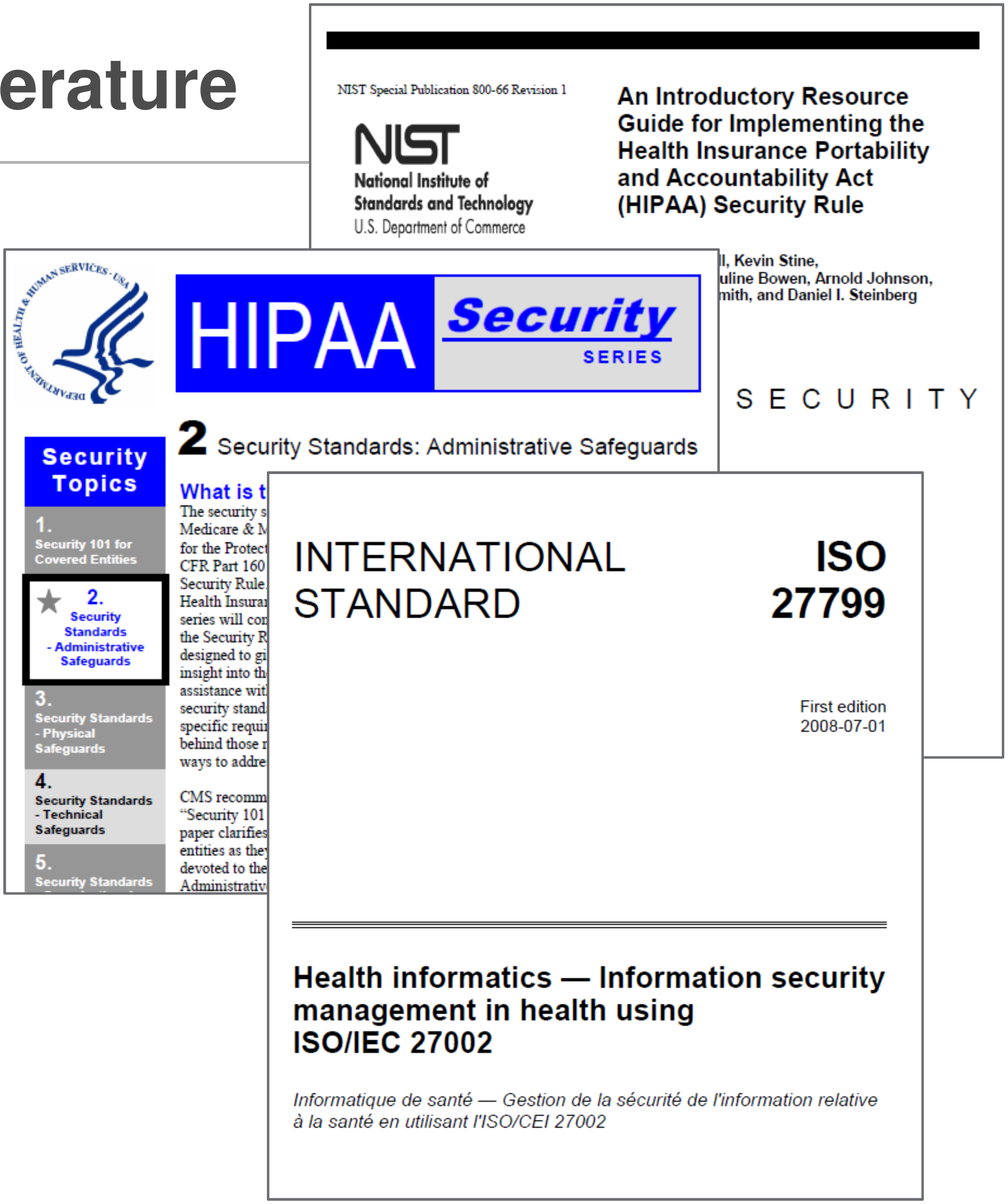
Supportive

Interpretive

Inadequate

Approach: Literature

- Prevalent guidance informed the general risk analysis
  - CMS HIPAA Security Series
  - NIST 800-66 (2008)
  - ISO 27799 (2008)
- Verizon HIPAA Security Office risk requirements
- Verizon Data Breach Investigative Report



NIST Special Publication 800-66 Revision 1

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule

ll, Kevin Stine,
uline Bowen, Arnold Johnson,
mith, and Daniel I. Steinberg

SECURITY

HIPAA *Security* SERIES

2 Security Standards: Administrative Safeguards

Security Topics

1. Security 101 for Covered Entities
2. ★ Security Standards - Administrative Safeguards
3. Security Standards - Physical Safeguards
4. Security Standards - Technical Safeguards
5. Security Standards

What is t

The security s
Medicare & M
for the Protect
CFR Part 160
Security Rule.
Health Insura
series will co
the Security R
designed to gi
insight into th
assistance wit
security stand
specific requi
behind those r
ways to addre

CMS recomm
"Security 101
paper clarifies
entities as they
devoted to the
Administrativ

INTERNATIONAL STANDARD

ISO 27799

First edition
2008-07-01

Health informatics — Information security management in health using ISO/IEC 27002

Informatique de santé — Gestion de la sécurité de l'information relative à la santé en utilisant l'ISO/CEI 27002

Approach: Literature
Data Breach Investigative Report (DBIR)

Released annually, since 2008

Provides insight into data breaches from 2004 to present

Spans more than 2,000 data breaches, totaling over one billion compromised records

AFP AUSTRALIAN FEDERAL POLICE

Australian Federal Police

POLITIE Korps landelijke politiediensten

Dutch National High Tech Crime Unit

IRISS Irish Reporting and Information Security Service

Irish Reporting & Information Security Service

PCeU Police Central e-crime Unit

Police Central e-Crime Unit of the London Metropolitan Police

United States Secret Service

***2013 Data Breach Investigations Report (DBIR)* Developed in Cooperation with International Crime Agencies**

Findings: SSAE 16 SOC 2 Type II

Certifiers	Certified Public Accountants (CPA)
Validity Period	6 months to 1 year
Used by	IT Service Organizations

Methodology	Evidence
Type I: Single point-in-time **Type II: Continuous over reporting period** SOC 1: Operational Assurance **SOC 2: Conformance with Trust Services Criteria** SOC 3: Auditor's Statement	

Confidential and proprietary materials for authorized Verizon personnel and outside agencies only. Use, disclosure or distribution of this material is not permitted to any unauthorized persons or third parties except by written agreement.

Findings: SSAE 16 SOC 2 Type II

Certifiers	Certified Public Accountants (CPA)

The following principles and related criteria have been developed by the AICPA and CPA Canada for use by practitioners in the performance of trust services engagements:

- Security. The system is protected against unauthorized access (both physical and logical).
- Availability. The system is available for operation and use as committed or agreed.
- Processing integrity. System processing is complete, accurate, timely, and authorized.
- Confidentiality. Information designated as confidential is protected as committed or agreed.
- Privacy. Personal information is collected, used, retained, disclosed, and destroyed in conformity with the commitments in the entity's privacy notice and with criteria set forth in generally accepted privacy principles issued by the AICPA and CPA Canada.

period

- Security

3.12 Encryption or other equivalent security techniques are used to protect transmissions of user authentication and other confidential information passed over the Internet or other public networks.

3.13 Procedures exist to identify, report, and act upon system confidentiality and security breaches and other incidents.

verizon

Findings: SSAE 16 SOC 2 Type II

AICPA

Certifiers	Certified Public Accountants (CPA)
Validity Period	6 months to 1 year
Used by	IT Service Organizations

Methodology

Type I: Single point-in-time
Type II: Continuous over reporting period

SOC 1: Operational Assurance
SOC 2: Conformance with Trust Services Criteria
SOC 3: Auditor’s Statement

Sufficient

Evidence

SOC 1: ToE’s policies and procedures
SOC 2: Trust Services Principles

- **Security**
- **Availability**
- Processing Integrity
- **Confidentiality**
- Privacy (GAAP)

SOC 3: Same as SOC2

Interpretive

Findings: ISO 27001

Certifiers	Accredited Auditors
Validity Period	3 years
Used by	Information Security Management

Methodology	Evidence
Statement of Applicability	
Point-in-time audit	
Review of ISMS inputs and outputs over reporting time period	
Review of risk management practices	

ISO/IEC 27002:2005 establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization. The objectives outlined provide general guidance on the commonly accepted goals of information security management. ISO/IEC 27002:2005 contains best practices of control objectives and controls in the following areas of information security management:

- security policy;
- organization of information security;
- asset management;
- human resources security;
- physical and environmental security;
- communications and operations management;
- access control;
- information systems acquisition, development and maintenance;
- information security incident management;
- business continuity management;
- compliance.

The control objectives and controls in ISO/IEC 27002:2005 are intended to be implemented to meet the requirements identified by a risk assessment. ISO/IEC 27002:2005 is intended as a common basis and practical guideline for developing organizational security standards and effective security management practices, and to help build confidence in inter-organizational activities.

t

Point-in-t

Review o
reporting

Review o

ology—
ecurity
nts

ology –
ce for

Findings: ISO 27001

Certifiers	Accredited Auditors
Validity Period	3 years
Used by	Information Security Management

Methodology	Evidence
Statement of Applicability Point-in-time audit Review of ISMS inputs and outputs over reporting time period Review of risk management practices	ISO 27001:2013 - Information technology—Security techniques — Information security management systems — Requirements ISO 27002: 2005 - Information technology – Security techniques – Code of practice for information security management

Potential

Interpretive

Confidential and proprietary materials for authorized Verizon personnel and outside agencies only. Use, disclosure or distribution of this material is not permitted to any unauthorized persons or third parties except by written agreement.

Findings: PCI DSS

Certifiers	Qualified Security Assessors (QSA)
Validity Period	1 year
Used by	Payment Card Industry

Methodology

Annual self-assessment

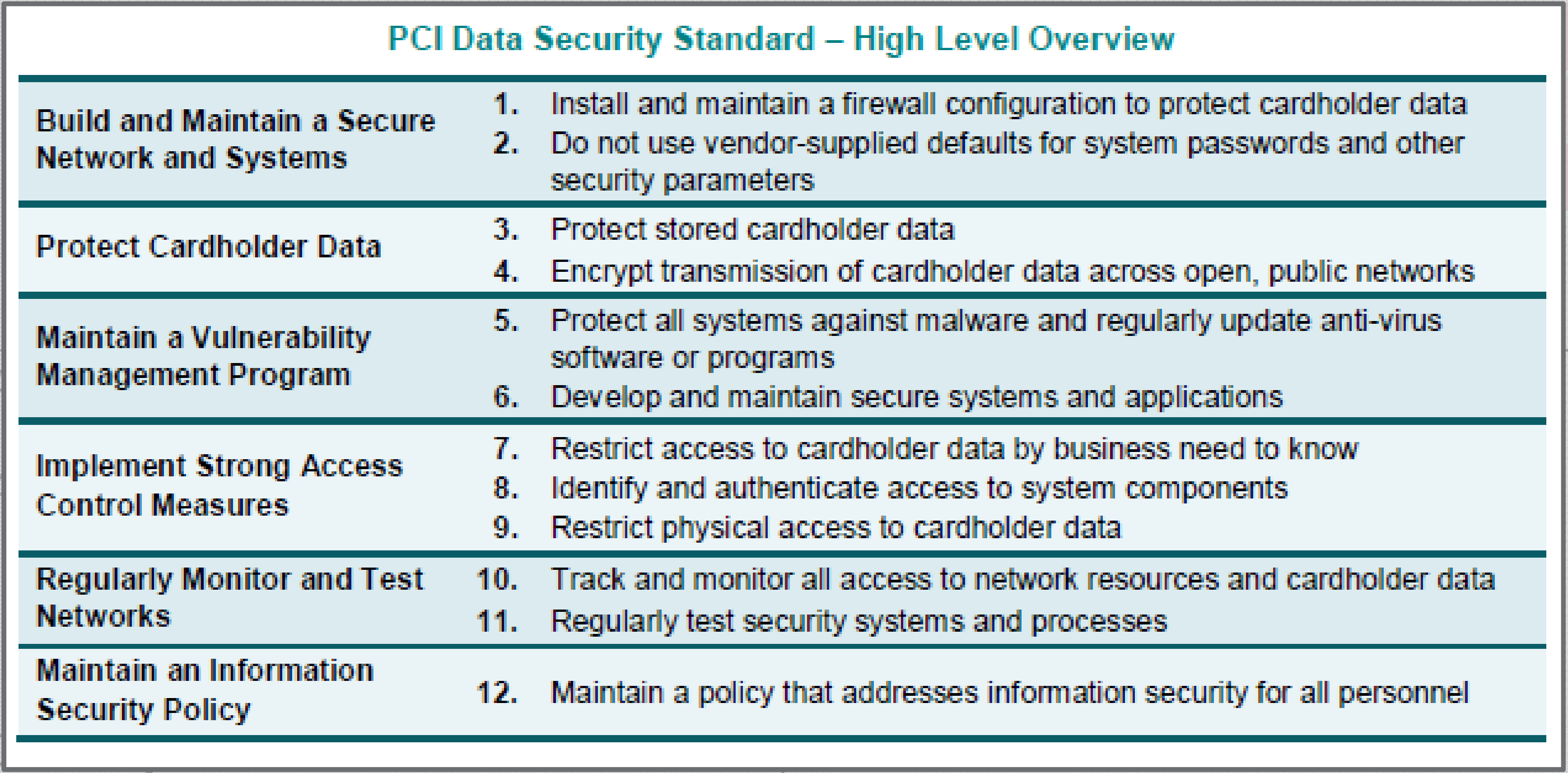
Annual audit for high-risk providers

- Interviews
- On-site Inspection
- Document review

Quarterly scans of cardholder environment

Evidence

Findings: PCI DSS



PCI Data Security Standard – High Level Overview

Build and Maintain a Secure Network and Systems	**1.** Install and maintain a firewall configuration to protect cardholder data **2.** Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	**3.** Protect stored cardholder data **4.** Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	**5.** Protect all systems against malware and regularly update anti-virus software or programs **6.** Develop and maintain secure systems and applications
Implement Strong Access Control Measures	**7.** Restrict access to cardholder data by business need to know **8.** Identify and authenticate access to system components **9.** Restrict physical access to cardholder data
Regularly Monitor and Test Networks	**10.** Track and monitor all access to network resources and cardholder data **11.** Regularly test security systems and processes
Maintain an Information Security Policy	**12.** Maintain a policy that addresses information security for all personnel

environment

Findings: PCI DSS

Certifiers	Qualified Security Assessors (QSA)
Validity Period	1 year
Used by	Payment Card Industry

Methodology

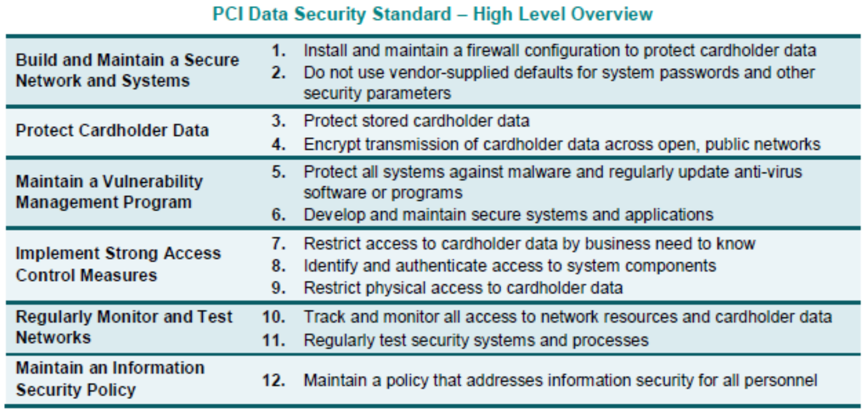
Annual self-assessment

Annual audit for high-risk providers
- Interviews
- On-site Inspection
- Document review

Quarterly scans of cardholder environment

Insufficient

Evidence



PCI Data Security Standard – High Level Overview

Build and Maintain a Secure Network and Systems	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Identify and authenticate access to system components 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel

Inadequate

Findings: FedRAMP

Certifiers	FedRAMP Accredited Assessors
Validity Period	At most 3 years
Used by	US Federal Agencies

Methodology

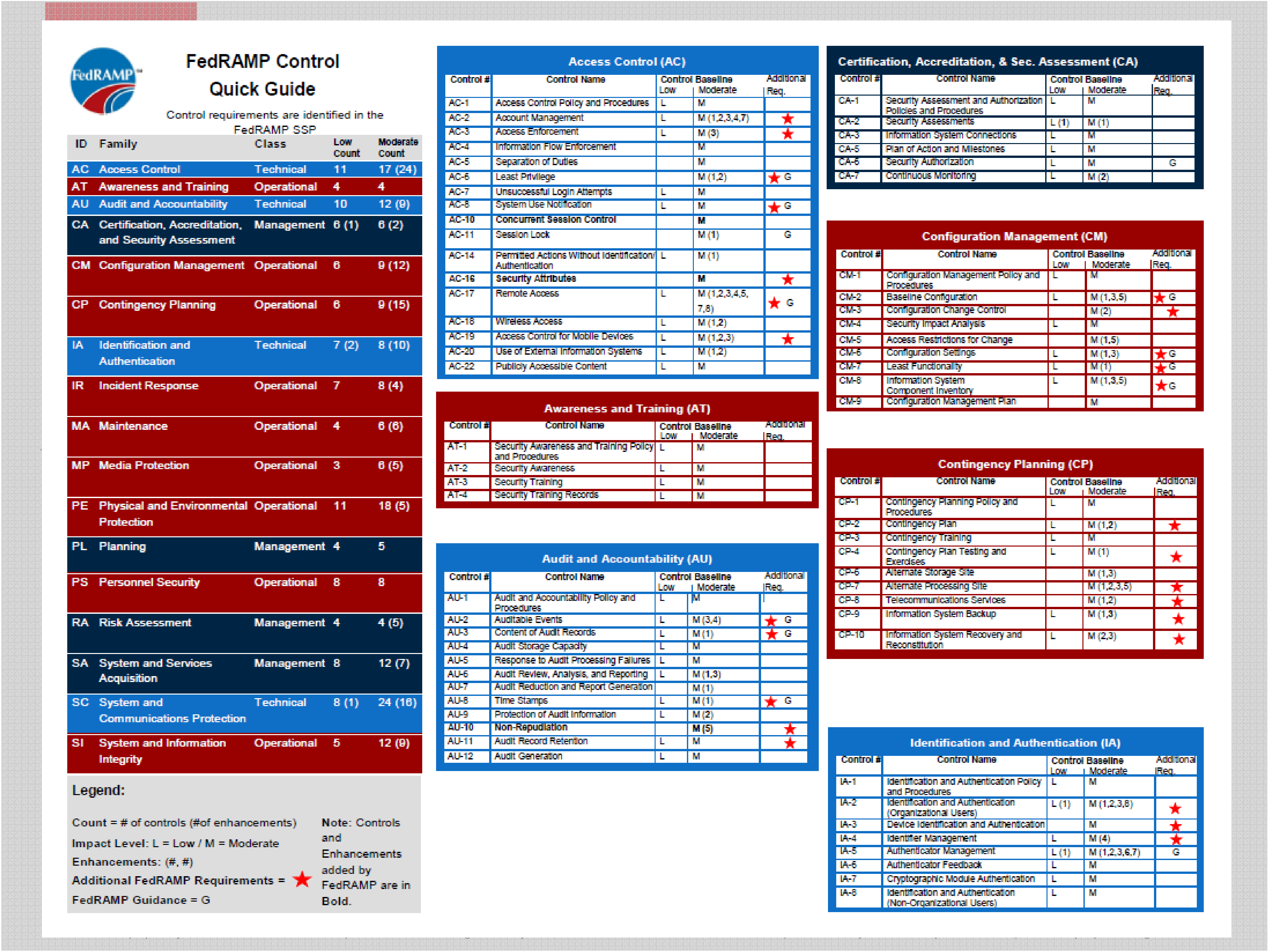
Security Assessment

- Documenting security controls
- Security testing

On-going Assessment and Authorization

- Continuous monitoring
- Plan of Action and Milestonese

Evidence



FedRAMP Control Quick Guide

Control requirements are identified in the FedRAMP SSP

ID	Family	Class	Low Count	Moderate Count
AC	Access Control	Technical	11	17 (24)
AT	Awareness and Training	Operational	4	4
AU	Audit and Accountability	Technical	10	12 (9)
CA	Certification, Accreditation, and Security Assessment	Management	6 (1)	6 (2)
CM	Configuration Management	Operational	6	9 (12)
CP	Contingency Planning	Operational	6	9 (15)
IA	Identification and Authentication	Technical	7 (2)	8 (10)
IR	Incident Response	Operational	7	8 (4)
MA	Maintenance	Operational	4	6 (6)
MP	Media Protection	Operational	3	6 (5)
PE	Physical and Environmental Protection	Operational	11	18 (5)
PL	Planning	Management	4	5
PS	Personnel Security	Operational	8	8
RA	Risk Assessment	Management	4	4 (5)
SA	System and Services Acquisition	Management	8	12 (7)
SC	System and Communications Protection	Technical	8 (1)	24 (16)
SI	System and Information Integrity	Operational	5	12 (9)

Legend:

Count = # of controls (#of enhancements)

Impact Level: L = Low / M = Moderate

Enhancements: (#, #)

Additional FedRAMP Requirements = ★

FedRAMP Guidance = G

Note: Controls and Enhancements added by FedRAMP are in Bold.

Access Control (AC)

Control #	Control Name	Control Baseline		Additional
		Low	Moderate	Req.
AC-1	Access Control Policy and Procedures	L	M	
AC-2	Account Management	L	M (1,2,3,4,7)	★
AC-3	Access Enforcement	L	M (3)	★
AC-4	Information Flow Enforcement		M	
AC-5	Separation of Duties		M	
AC-6	Least Privilege		M (1,2)	★ G
AC-7	Unsuccessful Login Attempts	L	M	
AC-8	System Use Notification	L	M	★ G
AC-10	**Concurrent Session Control**		**M**	
AC-11	Session Lock		M (1)	G
AC-14	Permitted Actions Without Identification/ Authentication	L	M (1)	
AC-16	**Security Attributes**		**M**	★
AC-17	Remote Access	L	M (1,2,3,4,5, 7,8)	★ G
AC-18	Wireless Access	L	M (1,2)	
AC-19	Access Control for Mobile Devices	L	M (1,2,3)	★
AC-20	Use of External Information Systems	L	M (1,2)	
AC-22	Publicly Accessible Content	L	M	

Awareness and Training (AT)

Control #	Control Name	Control Baseline		Additional
		Low	Moderate	Req.
AT-1	Security Awareness and Training Policy and Procedures	L	M	
AT-2	Security Awareness	L	M	
AT-3	Security Training	L	M	
AT-4	Security Training Records	L	M	

Audit and Accountability (AU)

Control #	Control Name	Control Baseline		Additional
		Low	Moderate	Req.
AU-1	Audit and Accountability Policy and Procedures	L	M	
AU-2	Auditable Events	L	M (3,4)	★ G
AU-3	Content of Audit Records	L	M (1)	★ G
AU-4	Audit Storage Capacity	L	M	
AU-5	Response to Audit Processing Failures	L	M	
AU-6	Audit Review, Analysis, and Reporting	L	M (1,3)	
AU-7	Audit Reduction and Report Generation		M (1)	
AU-8	Time Stamps	L	M (1)	★ G
AU-9	Protection of Audit Information	L	M (2)	
AU-10	**Non-Repudiation**		**M** (5)	★
AU-11	Audit Record Retention	L	M	★
AU-12	Audit Generation	L	M	

Certification, Accreditation, & Sec. Assessment (CA)

Control #	Control Name	Control Baseline		Additional
		Low	Moderate	Req.
CA-1	Security Assessment and Authorization Policies and Procedures	L	M	
CA-2	Security Assessments	L (1)	M (1)	
CA-3	Information System Connections	L	M	
CA-5	Plan of Action and Milestones	L	M	
CA-6	Security Authorization	L	M	G
CA-7	Continuous Monitoring	L	M (2)	

Configuration Management (CM)

Control #	Control Name	Control Baseline		Additional
		Low	Moderate	Req.
CM-1	Configuration Management Policy and Procedures	L	M	
CM-2	Baseline Configuration	L	M (1,3,5)	★ G
CM-3	Configuration Change Control		M (2)	★
CM-4	Security Impact Analysis	L	M	
CM-5	Access Restrictions for Change		M (1,5)	
CM-6	Configuration Settings	L	M (1,3)	★ G
CM-7	Least Functionality	L	M (1)	★ G
CM-8	Information System Component Inventory	L	M (1,3,5)	★ G
CM-9	Configuration Management Plan		M	

Contingency Planning (CP)

Control #	Control Name	Control Baseline		Additional
		Low	Moderate	Req.
CP-1	Contingency Planning Policy and Procedures	L	M	
CP-2	Contingency Plan	L	M (1,2)	★
CP-3	Contingency Training	L	M	
CP-4	Contingency Plan Testing and Exercises	L	M (1)	★
CP-6	Alternate Storage Site		M (1,3)	
CP-7	Alternate Processing Site		M (1,2,3,5)	★
CP-8	Telecommunications Services		M (1,2)	★
CP-9	Information System Backup	L	M (1,3)	★
CP-10	Information System Recovery and Reconstitution	L	M (2,3)	★

Identification and Authentication (IA)

Control #	Control Name	Control Baseline		Additional
		Low	Moderate	Req.
IA-1	Identification and Authentication Policy and Procedures	L	M	
IA-2	Identification and Authentication (Organizational Users)	L (1)	M (1,2,3,8)	★
IA-3	Device Identification and Authentication		M	★
IA-4	Identifier Management	L	M (4)	★
IA-5	Authenticator Management	L (1)	M (1,2,3,6,7)	G
IA-6	Authenticator Feedback	L	M	
IA-7	Cryptographic Module Authentication	L	M	
IA-8	Identification and Authentication (Non-Organizational Users)	L	M	

Findings: FedRAMP

Certifiers	FedRAMP Accredited Assessors
Validity Period	At most 3 years
Used by	US Federal Agencies

Methodology

Security Assessment

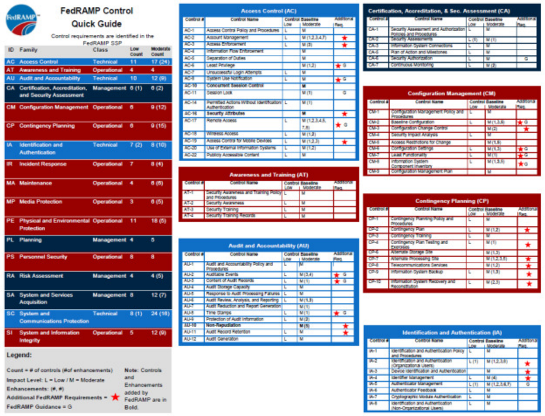
- Documenting security controls
- Security testing

On-going Assessment and Authorization

- Continuous monitoring
- Plan of Action and Milestonese

Sufficient

Evidence



FedRAMP Control Quick Guide

Control requirements are identified in the FedRAMP SSP

ID	Family	Class	Low Count	Moderate Count
AC	Access Control	Technical	11	17 (24)
AT	Awareness and Training	Operational	4	4
AU	Audit and Accountability	Technical	10	12 (9)
CA	Certification, Accreditation, and Security Assessment	Management	6 (1)	6 (2)
CM	Configuration Management	Operational	6	9 (12)
CP	Contingency Planning	Operational	6	9 (15)
IA	Identification and Authentication	Technical	7 (2)	8 (10)
IR	Incident Response	Operational	7	8 (4)
MA	Maintenance	Operational	4	6 (6)
MP	Media Protection	Operational	3	6 (5)
PE	Physical and Environmental Protection	Operational	11	18 (5)
PL	Planning	Management	4	5
PS	Personnel Security	Operational	8	8
RA	Risk Assessment	Management	4	4 (5)
SA	System and Services Acquisition	Management	8	12 (7)
SC	System and Communications Protection	Technical	8 (1)	24 (16)
SI	System and Information Integrity	Operational	5	12 (9)

Legend:

Count = # of controls (#of enhancements)
Impact Level: L = Low / M = Moderate
Enhancements: (#, #)
Additional FedRAMP Requirements = ★
FedRAMP Guidance = G

Note: Controls and Enhancements added by FedRAMP are in Bold.

Access Control (AC)

Control #	Control Name	Control Baseline Low	Moderate	Additional Req.
AC-1	Access Control Policy and Procedures	L	M	
AC-2	Account Management	L	M (1,2,3,4,7)	★
AC-3	Access Enforcement	L	M (3)	★
AC-4	Information Flow Enforcement		M	
AC-5	Separation of Duties		M	
AC-6	Least Privilege		M (1,2)	★ G
AC-7	Unsuccessful Login Attempts	L	M	
AC-8	System Use Notification	L	M	★ G
AC-10	**Concurrent Session Control**		**M**	
AC-11	Session Lock		M (1)	G
AC-14	Permitted Actions Without Identification/ Authentication	L	M (1)	
AC-16	**Security Attributes**		**M**	★
AC-17	Remote Access	L	M (1,2,3,4,5, 7,8)	★ G
AC-18	Wireless Access	L	M (1,2)	
AC-19	Access Control for Mobile Devices	L	M (1,2,3)	★
AC-20	Use of External Information Systems	L	M (1,2)	
AC-22	Publicly Accessible Content	L	M	

Awareness and Training (AT)

Control #	Control Name	Control Baseline Low	Moderate	Additional Req.
AT-1	Security Awareness and Training Policy and Procedures	L	M	
AT-2	Security Awareness	L	M	
AT-3	Security Training	L	M	
AT-4	Security Training Records	L	M	

Audit and Accountability (AU)

Control #	Control Name	Control Baseline Low	Moderate	Additional Req.
AU-1	Audit and Accountability Policy and Procedures	L	M	
AU-2	Auditable Events	L	M (3,4)	★ G
AU-3	Content of Audit Records	L	M (1)	★ G
AU-4	Audit Storage Capacity	L	M	
AU-5	Response to Audit Processing Failures	L	M	
AU-6	Audit Review, Analysis, and Reporting	L	M (1,3)	
AU-7	Audit Reduction and Report Generation		M (1)	
AU-8	Time Stamps	L	M (1)	★ G
AU-9	Protection of Audit Information	L	M (2)	
AU-10	**Non-Repudiation**		**M (5)**	★
AU-11	Audit Record Retention	L	M	★
AU-12	Audit Generation	L	M	

Certification, Accreditation, & Sec. Assessment (CA)

Control #	Control Name	Control Baseline Low	Moderate	Additional Req.
CA-1	Security Assessment and Authorization Policies and Procedures	L	M	
CA-2	Security Assessments	L (1)	M (1)	
CA-3	Information System Connections	L	M	
CA-5	Plan of Action and Milestones	L	M	
CA-6	Security Authorization	L	M	G
CA-7	Continuous Monitoring	L	M (2)	

Configuration Management (CM)

Control #	Control Name	Control Baseline Low	Moderate	Additional Req.
CM-1	Configuration Management Policy and Procedures	L	M	
CM-2	Baseline Configuration	L	M (1,3,5)	★ G
CM-3	Configuration Change Control		M (2)	★
CM-4	Security Impact Analysis	L	M	
CM-5	Access Restrictions for Change		M (1,5)	
CM-6	Configuration Settings	L	M (1,3)	★ G
CM-7	Least Functionality	L	M (1)	★ G
CM-8	Information System Component Inventory	L	M (1,3,5)	★ G
CM-9	Configuration Management Plan		M	

Contingency Planning (CP)

Control #	Control Name	Control Baseline Low	Moderate	Additional Req.
CP-1	Contingency Planning Policy and Procedures	L	M	
CP-2	Contingency Plan	L	M (1,2)	★
CP-3	Contingency Training	L	M	
CP-4	Contingency Plan Testing and Exercises	L	M (1)	★
CP-6	Alternate Storage Site		M (1,3)	
CP-7	Alternate Processing Site		M (1,2,3,5)	★
CP-8	Telecommunications Services		M (1,2)	★
CP-9	Information System Backup	L	M (1,3)	★
CP-10	Information System Recovery and Reconstitution	L	M (2,3)	★

Identification and Authentication (IA)

Control #	Control Name	Control Baseline Low	Moderate	Additional Req.
IA-1	Identification and Authentication Policy and Procedures	L	M	
IA-2	Identification and Authentication (Organizational Users)	L (1)	M (1,2,3,8)	★
IA-3	Device Identification and Authentication		M	★
IA-4	Identifier Management	L	M (4)	★
IA-5	Authenticator Management	L (1)	M (1,2,3,6,7)	G
IA-6	Authenticator Feedback	L	M	
IA-7	Cryptographic Module Authentication	L	M	
IA-8	Identification and Authentication (Non-Organizational Users)	L	M	

Interpretive

Findings: Summary View

Standard	Methodology	Evidence
SSAE 16 SOC 2	Sufficient	Interpretive
ISO 27001	Potential	Interpretive
PCI DSS	Insufficient	Inadequate
FedRAMP	Sufficient	Interpretive

Conclusions: Effectiveness

As they exist, prevalent information security certification standards are insufficient to address all HIPAA Security requirements.

Appropriate interpretation of existing certification standards *should* be sufficient

Conclusions: Opportunity

Establish information security baseline for IT hosting in healthcare

Improve consistency of security posture across hosting providers serving covered entities

Standardize method to report information security posture

Reduce barriers for outsourcing IT hosting functions to covered entities by increasing confidence in the security of these functions