Control Standards: Managing Encryption Keys

First Published: 8/3/2012 10:54 AM Last Updated: 6/10/2021 8:56 AM

General

About

Control Standards

The Control Standards application serves as a central repository for authoring and displaying corporate standards that are mapped to policies, authoritative sources and control procedures. You can also assess the criticality of control standards based on the objectives and regulations they support and any known control weaknesses. Additionally, the application provides an overall compliance rating for each control standard based on testing performed against related control procedures.

Through the Control Standards application, you can:

- Use pre-loaded control standards from the RSA Archer eGRC Content Library, and import your own standards using the Data Import Manager.
- Rationalize standards by mapping them to the policies they support and to authoritative sources, such as PCI, ISO/IEC, COBIT, FFIEC, HIPAA, NIST and privacy legislation.
- Identify the control procedures that support each standard, and track compliance testing against those procedures.
- Use automated workflow to ensure proper review and approval of all control standard content before publication.
- Communicate new and updated control standards across your enterprise.

General Information

Standard Name:	Managing Encryption Keys	**Standard ID:**	ATCS-248
Status:	Published		

Statement:

Encryption key owners are responsible for the protection and management of public and private encryption keys entrusted to them and shall adhere to the following standards:

- Key owners shall not print out private keys
- Private Keys shall be transmitted through separate channels than other supporting information (i.e. import passwords, Certificate Signing Requests, etc.) to assure that the interception of a single message or correspondence will not allow the compromise of the Private Key. Import passwords shall be communicated via a separate communication mechanism than that which is used to transmit the private key (i.e. convey the password via phone message if the key is distributed via email).
- All encryption systems shall be protected with appropriate security controls approved by Information Security
- Private keys shall be classified at the same level as the information being encrypted
- Access to private keys shall be on a need-to-know basis and in no circumstances may they be accessed by anyone not authorized by Information Security
- Systems shall be configured to use enterprise authentication and authorization systems (i.e. Active Directory) to govern access to keys used to encrypt Aetna data. A sufficient authorization model shall be implemented to assure that only individuals who require access based on their organizational role and job responsibilities receive access to encryption keys and that only authorized service accounts and systems are granted access to encryption keys.
- Personnel authorized by Information Security in possession of keys or key components shall be required to prevent the disclosure of those keys or key components
- Private keys may shall not be revealed to third parties without the approval of Information Security.
- Key-encrypting keys are at least as strong as the data-encrypting keys they protect.
- Key-management procedures specify processes to prevent unauthorized substitution of keys.

Keys shall only be used for a single purpose, and are unique to a communicating pair.

The company requires the use of full-length key components. For example, a 64-bit key generated as two components results in two 64-bit components, not two 32-bit components.

Cryptographic keys shall be generated only on an internal and trusted system approved by Information Security. Keys shall be generated purely randomly using a suitable cryptographic key generation routine. Symmetric keys shall be generated using a trueâ€ random generation method approved by Information Security.

This standard prohibits the sharing of keys between more than two parties. A key shall never be included in a key sharing transaction with a third party, even if they are a trusted partner. This practice both reduces the number of parties that must be contacted in the event of a key compromise and prevents the third party from accessing confidential data or the keys necessary to decrypt that data.

Keys stored within a TRSM shall be encrypted under the KKS (key encrypting key for storage), also known as the Local Master Key. It shall not be possible for the KKS itself to be exported from the TRSM in its entirety, but only as components.

Company issued certificates and keys shall not be shared amongst production and non-production environments. Individual keys/certificates should be requested for each environment.

Business Division:	Aetna Digital Healthcare Benefits (HCB)

Associated Links

Associated Links:	

Publication Information

Control Standard Owner:	Graff, Michael Rana, Usman	**Control Standard Backup Owner:**	Birchette, Taylor Singla, Namita
Grouping:	Encryption HiTrust PCI	**Stakeholders:**	Abrams, Mark Farrell, Brendan Gonzalez, Julieanne Kowalewski, Kimberly Liu, Min-hwei Semeraro, Larissa
Classification:	Preventive	**Effective Date:**	3/14/2019
Content Source:	Aetna	**Next Review Date:**	6/10/2022

Related Control Standards

Standard Name	Standard ID	Next Review Date
No Records Found		

Governance

Policy:

- 07.0 Communications Management Policy
  - 07.1 Encryption
    - 07.1.03 Key Management
- 14.0 IT Management Policy
  - 14.1 Cloud Management
    - 14.1.2 Cloud Management

Authoritative Sources:

- NIST SP 800-53 (Revision 5)
  - 17 SYSTEM AND SERVICES ACQUISITION
    - SA-09 EXTERNAL SYSTEM SERVICES
      - SA-09 (06) EXTERNAL SYSTEM SERVICES | ORGANIZATION-CONTROLLED CRYPTOGRAPHIC KEYS
  - 18 SYSTEM AND COMMUNICATIONS PROTECTION
    - SC-12 CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT
      - SC-12 (01) CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | AVAILABILITY
      - SC-12 (02) CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | SYMMETRIC KEYS
      - SC-12 (03) CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | ASYMMETRIC KEYS
      - SC-12 (06) CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | PHYSICAL CONTROL OF KEYS
    - SC-17 PUBLIC KEY INFRASTRUCTURE CERTIFICATES
    - SC-28 PROTECTION OF INFORMATION AT REST

- SC-28 (03) PROTECTION OF INFORMATION AT REST | CRYPTOGRAPHIC KEYS

- ISO/IEC 27001:2013(E)
  - A.10 Cryptography
    - A.10.01 Cryptographic controls
      - A.10.01.02 Key management
- EU Regulatory Technical Standards for Authentication (November 2017)
  - 04 Confidentiality and Integrity of the Payment Service Users' Personalized Security Credentials (Chapter 04)
    - 04.01 General requirements (Article 22)
      - 04.01.03 Documentation of cryptographic material (Article 22, 3)
- Baseline Security Recommendations for IoT (November 2017)
  - 04 Security measures and good practices
    - 04.03 Technical Measures (4.3)
      - 04.03.10 Cryptography (4.3.10)
      - 04.03.12 Secure Interfaces and network services (4.3.12)
  - 08 Annex A: Detailed Security measures / Good practices
    - 08.14 Cryptography
      - 08.14.02 Securely Manage Cryptographic Keys (GP-TM-35)
    - 08.16 Secure Interfaces and network services
      - 08.16.03 Avoid Using the Same Secret Key (GP-TM-49)
  - 09 Annex B: Security measures and threats mapping
    - 09.14 Cryptography
      - 09.14.02 Securely Manage Cryptographic Keys (GP-TM-35)
    - 09.16 Secure Interfaces and network services
      - 09.16.03 Avoid Using the Same Secret Key (GP-TM-49)
- CMS ARS 100-25 (January 2018)
  - 07 Appendix B. ARS Controls (B)
    - 07.16 System and Communications Protection (SC) (B.16)
      - 07.16.23 Cryptographic Key Establishment and Management (SC-12)
- Payment Card Industry Data Security Standard v3.2.1
  - Requirement 03: Protect stored cardholder data
    - Requirement 03.05

- Requirement 03.05.01
- Requirement 03.05.02
- Requirement 03.05.03
- Requirement 03.05.04
- Requirement 03.06
    - Requirement 03.06.01
    - Requirement 03.06.02
    - Requirement 03.06.04
    - Requirement 03.06.05
    - Requirement 03.06.06
    - Requirement 03.06.07
    - Requirement 03.06.08

NIST SP 800-171 Revision 1 (December 2016)

- 09 Appendix F: Discussion
    - 09.13 System and Communications Protection (3.13)
        - 09.13.10 - Cryptographic Key Management (3.13.10)

Australian Government Information Security Manual Controls (November, 2017)

- 06-30 - Cryptography - ASD Approved Cryptographic Algorithms
    - 06-30.03 - Controls - Using Diffie-Hellman
        - 06-30.03.01 - Diffie-Hellman 1024 Bits (0472)
        - 06-30.03.02 - Diffie-Hellman 2048 Bits (1475)

FFIEC Information Security Booklet (September, 2016)

- 02 Information Security Program Management (FFIEC: II)
    - 02.03 Risk Mitigation (FFIEC: II.C)
        - 02.03.19 Encryption (FFIEC: II.C.19)
- 05 Examination Procedures (FFIEC: Appendix A)
    - 05.06 Objective 6 - Control Implementation
        - 05.06.30 Procedure 30 - Encryption

NIST SP 800-82 Guide to Industrial Control Systems (ICS) Security (Revision 2)

- 06 Applying Security Controls to ICS
    - 06.02 Guidance on the Application of Security Controls to ICS
        - 06.02.16 System and Communications Protection

MAS - Technology Risk Management Guidelines

- APPENDIX C: CRYPTOGRAPHY
    - C.3 Cryptographic Key Management
        - C.3.1

- C.3.2
- C.3.3
- C.3.6

France - Federal Data Protection Act 78-17

- 03: The Commission nationale de l'informatique et des libert?s (CNIL)
  - The Commission nationale de l'informatique et des libert?s (CNIL)
    - Article 11
    - Article 12
    - Article 16
- 04: Formalities prior to commencing data processing
  - Authorisation
    - Article 25
  - Formalities prior to commencing data processing
    - Article 22

NCS TIB 05-4 (SCADA)

- 04 Recommendations
  - 04.01 Security Tools
    - 04.01.02 Encryption

NIST 800-82 Guide to Industrial Control Systems (ICS) Security

- 06 ICS Security Controls
  - 06.03 Technical Controls
    - 06.03.04 System and Communications Protection

MAS IBTRM Guidelines v3.0

- 04.0 Security and Control Objectives
  - 4.1 Data Confidentiality
    - 4.1.3

HKMA TM-G-1

- 3. Security Management
  - 3.1 Information classification and protection
    - 3.1.4

FedRAMP Revision 4

- IDENTIFICATION AND AUTHENTICATION
  - IA-05 AUTHENTICATOR MANAGEMENT
- SYSTEM AND COMMUNICATIONS PROTECTION
  - SC-01 SYSTEM AND COMMUNICATIONS PROTECTION POLICY AND PROCEDURES
  - SC-07 BOUNDARY PROTECTION
    - SC-07 (4) BOUNDARY PROTECTION | EXTERNAL TELECOMMUNICATIONS SERVICES

- SC-07 (13) BOUNDARY PROTECTION | ISOLATION OF SECURITY TOOLS / MECHANISMS / SUPPORT COMPONENTS

- SC-08 TRANSMISSION CONFIDENTIALITY AND INTEGRITY
  - SC-08 (1) TRANSMISSION CONFIDENTIALITY AND INTEGRITY | CRYPTOGRAPHIC OR ALTERNATE PHYSICAL PROTECTION
- SC-10 NETWORK DISCONNECT
- SC-12 CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT
  - SC-12 (2) CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | SYMMETRIC KEYS
- SC-13 CRYPTOGRAPHIC PROTECTION
- SC-15 COLLABORATIVE COMPUTING DEVICES
- SC-28 PROTECTION OF INFORMATION AT REST

NIST SP 800-53 (Revision 4)

- IDENTIFICATION AND AUTHENTICATION
  - IA-05 AUTHENTICATOR MANAGEMENT
- SYSTEM AND COMMUNICATIONS PROTECTION
  - SC-01 SYSTEM AND COMMUNICATIONS PROTECTION POLICY AND PROCEDURES
  - SC-02 APPLICATION PARTITIONING
    - SC-02 (1) APPLICATION PARTITIONING | INTERFACES FOR NON-PRIVILEGED USERS
  - SC-03 SECURITY FUNCTION ISOLATION
    - SC-03 (1) SECURITY FUNCTION ISOLATION | HARDWARE SEPARATION
    - SC-03 (2) SECURITY FUNCTION ISOLATION | ACCESS / FLOW CONTROL FUNCTIONS
    - SC-03 (3) SECURITY FUNCTION ISOLATION | MINIMIZE NONSECURITY FUNCTIONALITY
    - SC-03 (4) SECURITY FUNCTION ISOLATION | MODULE COUPLING AND COHESIVENESS
    - SC-03 (5) SECURITY FUNCTION ISOLATION | LAYERED

STRUCTURES

SC-04 INFORMATION IN SHARED RESOURCES

- SC-04 (2) INFORMATION IN SHARED RESOURCES | PERIODS PROCESSING

SC-05 DENIAL OF SERVICE PROTECTION

- SC-05 (1) DENIAL OF SERVICE PROTECTION | RESTRICT INTERNAL USERS
- SC-05 (2) DENIAL OF SERVICE PROTECTION | EXCESS CAPACITY / BANDWIDTH / REDUNDANCY
- SC-05 (3) DENIAL OF SERVICE PROTECTION | DETECTION / MONITORING

SC-06 RESOURCE AVAILABILITY

SC-07 BOUNDARY PROTECTION

- SC-07 (3) BOUNDARY PROTECTION | ACCESS POINTS
- SC-07 (4) BOUNDARY PROTECTION | EXTERNAL TELECOMMUNICATIONS SERVICES
- SC-07 (5) BOUNDARY PROTECTION | DENY BY DEFAULT / ALLOW BY EXCEPTION
- SC-07 (7) BOUNDARY PROTECTION | PREVENT SPLIT TUNNELING FOR REMOTE DEVICES
- SC-07 (8) BOUNDARY PROTECTION | ROUTE TRAFFIC TO AUTHENTICATED PROXY SERVERS
- SC-07 (9) BOUNDARY PROTECTION | RESTRICT THREATENING OUTGOING COMMUNICATIONS TRAFFIC
- SC-07 (10) BOUNDARY PROTECTION | PREVENT UNAUTHORIZED EXFILTRATION
- SC-07 (11) BOUNDARY PROTECTION | RESTRICT INCOMING COMMUNICATIONS TRAFFIC
- SC-07 (12) BOUNDARY PROTECTION | HOST-BASED PROTECTION
- SC-07 (13) BOUNDARY PROTECTION | ISOLATION OF SECURITY TOOLS / MECHANISMS / SUPPORT COMPONENTS
- SC-07 (14) BOUNDARY

			PROTECTION | PROTECTS AGAINST UNAUTHORIZED PHYSICAL CONNECTIONS SC-07 (15) BOUNDARY PROTECTION | ROUTE PRIVILEGED NETWORK ACCESSES SC-07 (16) BOUNDARY PROTECTION | PREVENT DISCOVERY OF COMPONENTS / DEVICES SC-07 (17) BOUNDARY PROTECTION | AUTOMATED ENFORCEMENT OF PROTOCOL FORMATS SC-07 (18) BOUNDARY PROTECTION | FAIL SECURE SC-07 (19) BOUNDARY PROTECTION | BLOCKS COMMUNICATION FROM NON-ORGANIZATIONALLY CONFIGURED HOSTS SC-07 (20) BOUNDARY PROTECTION | DYNAMIC ISOLATION / SEGREGATION SC-07 (21) BOUNDARY PROTECTION | ISOLATION OF INFORMATION SYSTEM COMPONENTS SC-07 (22) BOUNDARY PROTECTION | SEPARATE SUBNETS FOR CONNECTING TO DIFFERENT SECURITY DOMAINS SC-07 (23) BOUNDARY PROTECTION | DISABLE SENDER FEEDBACK ON PROTOCOL VALIDATION FAILURE SC-08 TRANSMISSION CONFIDENTIALITY AND INTEGRITY SC-08 (1) TRANSMISSION CONFIDENTIALITY AND INTEGRITY | CRYPTOGRAPHIC OR ALTERNATE PHYSICAL PROTECTION SC-08 (2) TRANSMISSION CONFIDENTIALITY AND INTEGRITY | PRE / POST TRANSMISSION HANDLING SC-08 (3) TRANSMISSION CONFIDENTIALITY AND INTEGRITY | CRYPTOGRAPHIC PROTECTION FOR MESSAGE EXTERNALS SC-08 (4) TRANSMISSION CONFIDENTIALITY AND INTEGRITY | CONCEAL / RANDOMIZE COMMUNICATIONS SC-10 NETWORK DISCONNECT

- SC-11 TRUSTED PATH
  - SC-11 (1) TRUSTED PATH | LOGICAL ISOLATION
- SC-12 CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT
  - SC-12 (1) CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | AVAILABILITY
  - SC-12 (2) CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | SYMMETRIC KEYS
  - SC-12 (3) CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | ASYMMETRIC KEYS
- SC-13 CRYPTOGRAPHIC PROTECTION
- SC-15 COLLABORATIVE COMPUTING DEVICES
  - SC-15 (1) COLLABORATIVE COMPUTING DEVICES | PHYSICAL DISCONNECT
  - SC-15 (3) COLLABORATIVE COMPUTING DEVICES | DISABLING / REMOVAL IN SECURE WORK AREAS
  - SC-15 (4) COLLABORATIVE COMPUTING DEVICES | EXPLICITLY INDICATE CURRENT PARTICIPANTS
- SC-16 TRANSMISSION OF SECURITY ATTRIBUTES
  - SC-16 (1) TRANSMISSION OF SECURITY ATTRIBUTES | INTEGRITY VALIDATION
- SC-17 PUBLIC KEY INFRASTRUCTURE CERTIFICATES
- SC-18 MOBILE CODE
  - SC-18 (1) MOBILE CODE | IDENTIFY UNACCEPTABLE CODE / TAKE CORRECTIVE ACTIONS
  - SC-18 (2) MOBILE CODE | ACQUISITION / DEVELOPMENT / USE
  - SC-18 (3) MOBILE CODE | PREVENT DOWNLOADING / EXECUTION
  - SC-18 (4) MOBILE CODE | PREVENT AUTOMATIC EXECUTION
  - SC-18 (5) MOBILE CODE | ALLOW EXECUTION ONLY IN CONFINED ENVIRONMENTS
- SC-19 VOICE OVER INTERNET PROTOCOL

SC-20 SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE)

- SC-20 (1) SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE) | CHILD SUBSPACES
- SC-20 (2) SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE) | DATA ORIGIN / INTEGRITY

SC-21 SECURE NAME / ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVER)

SC-22 ARCHITECTURE AND PROVISIONING FOR NAME / ADDRESS RESOLUTION SERVICE

SC-23 SESSION AUTHENTICITY

- SC-23 (1) SESSION AUTHENTICITY | INVALIDATE SESSION IDENTIFIERS AT LOGOUT
- SC-23 (3) SESSION AUTHENTICITY | UNIQUE SESSION IDENTIFIERS WITH RANDOMIZATION
- SC-23 (5) SESSION AUTHENTICITY | ALLOWED CERTIFICATE AUTHORITIES

SC-24 FAIL IN KNOWN STATE

SC-25 THIN NODES

SC-26 HONEYPOTS

SC-27 PLATFORM-INDEPENDENT APPLICATIONS

SC-28 PROTECTION OF INFORMATION AT REST

- SC-28 (1) PROTECTION OF INFORMATION AT REST | CRYPTOGRAPHIC PROTECTION
- SC-28 (2) PROTECTION OF INFORMATION AT REST | OFF-LINE STORAGE

SC-29 HETEROGENEITY

- SC-29 (1) HETEROGENEITY | VIRTUALIZATION TECHNIQUES

SC-30 CONCEALMENT AND MISDIRECTION

- SC-30 (2) CONCEALMENT AND MISDIRECTION | RANDOMNESS
- SC-30 (3) CONCEALMENT AND MISDIRECTION | CHANGE PROCESSING / STORAGE LOCATIONS
- SC-30 (4) CONCEALMENT AND MISDIRECTION | MISLEADING

  - INFORMATION
  - SC-30 (5) CONCEALMENT AND MISDIRECTION | CONCEALMENT OF SYSTEM COMPONENTS
- SC-31 COVERT CHANNEL ANALYSIS
  - SC-31 (1) COVERT CHANNEL ANALYSIS | TEST COVERT CHANNELS FOR EXPLOITABILITY
  - SC-31 (2) COVERT CHANNEL ANALYSIS | MAXIMUM BANDWIDTH
  - SC-31 (3) COVERT CHANNEL ANALYSIS | MEASURE BANDWIDTH IN OPERATIONAL ENVIRONMENTS
- SC-32 INFORMATION SYSTEM PARTITIONING
- SC-34 NON-MODIFIABLE EXECUTABLE PROGRAMS
  - SC-34 (1) NON-MODIFIABLE EXECUTABLE PROGRAMS | NO WRITABLE STORAGE
  - SC-34 (2) NON-MODIFIABLE EXECUTABLE PROGRAMS | INTEGRITY PROTECTION / READ-ONLY MEDIA
  - SC-34 (3) NON-MODIFIABLE EXECUTABLE PROGRAMS | HARDWARE-BASED PROTECTION
- SC-35 HONEYCLIENTS
- SC-36 DISTRIBUTED PROCESSING AND STORAGE
  - SC-36 (1) DISTRIBUTED PROCESSING AND STORAGE | POLLING TECHNIQUES
- SC-37 OUT-OF-BAND CHANNELS
  - SC-37 (1) OUT-OF-BAND CHANNELS | ENSURE DELIVERY / TRANSMISSION
- SC-38 OPERATIONS SECURITY
- SC-39 PROCESS ISOLATION
  - SC-39 (1) PROCESS ISOLATION | HARDWARE SEPARATION
  - SC-39 (2) PROCESS ISOLATION | THREAD ISOLATION
- SC-40 WIRELESS LINK PROTECTION
  - SC-40 (1) WIRELESS LINK PROTECTION | ELECTROMAGNETIC INTERFERENCE
  - SC-40 (2) WIRELESS LINK PROTECTION | REDUCE DETECTION POTENTIAL

SC-40 (3) WIRELESS LINK PROTECTION | IMITATIVE OR MANIPULATIVE COMMUNICATIONS DECEPTION

SC-40 (4) WIRELESS LINK PROTECTION | SIGNAL PARAMETER IDENTIFICATION

SC-41 PORT AND I/O DEVICE ACCESS

SC-42 SENSOR CAPABILITY AND DATA

SC-42 (1) SENSOR CAPABILITY AND DATA | REPORTING TO AUTHORIZED INDIVIDUALS OR ROLES

SC-42 (2) SENSOR CAPABILITY AND DATA | AUTHORIZED USE

SC-42 (3) SENSOR CAPABILITY AND DATA | PROHIBIT USE OF DEVICES

SC-43 USAGE RESTRICTIONS

SC-44 DETONATION CHAMBERS

Cloud Security Alliance - Cloud Controls Matrix - v3.0.1

Encryption & Key Management

EKM-01: Entitlement

EKM-02: Key Generation

EKM-04: Storage and Access

U.S. State Cyber Laws

New York State DFS Cyber Security Requirements

500.15 - Encryption of Nonpublic Information

Australian Government Information Security Manual Principles (2016)

24 Cryptography

24.04 Principle - Management of Cryptographic Systems

HITRUST CSF v9.3.1

06.01 Compliance with Legal Requirements

06.d Data Protection and Privacy of Covered Information

10.03 Cryptographic Controls

10.g Key Management

Control Standard Change Requests

Tracking ID	Status	Change Name	Change Type	Change Summary	First Published	Last Updated
1707102	Completed	Major Statement Modification	Major Statement Modification	Modify standards to address PCI related finding; add the following statements: • Key-encrypting keys are at least as strong as the data-encrypting keys they protect • Key-management procedures specify processes to prevent unauthorized substitution of keys. Also remove reference to CIST documents in standards which are retired (CIST-0018 and CIST-0111) from statement and title of standard.	4/12/2021 4:29 PM	4/12/2021 4:42 PM

Control Procedures

Procedure ID	Procedure Name	Type	Next Review Date	SOX Scoping	Technical Domain	Compliance
CP-1399171	Bitlocker	Process	1/4/2021			✓
CP-1399280	Encryption Key Rotation	Process	1/4/2021			
CP-1399334	Governance for High Risk Certificates	Process	1/4/2021			
CP-1399345	High Risk Certificate Inventory	Process	2/4/2021			
CP-1399399	Key management	Technical	2/4/2021		Cryptography Key Management	
CP-1399555	Periodic Review of CertPortal Access Logs	Process	2/4/2021			
CP-1399642	Restrict access to Aetna Certificate Portal to authenticated users	Technical	3/4/2021		User management	
CP-1399643	Restrict access to Venafi Management Console to authenticated administrators	Technical	3/4/2021		User management	
CP-1399674	Secure Aetna issued SSL certificates	Process	3/4/2021		System configuration	
CP-1399799	Undertaking of Encryption Certificate responsibility	Technical	3/4/2021			

Documents Repository

Title	Owner	Next Attestation Date	Category	Subcategory
Cloud Data at Rest Encryption Reference Security Architecture	Fretz, Kurt	11/30/2021	Security Architecture Artifact	Reference Artifact

Issues Management

Findings

Finding ID	Overall Status	zSource	Target
No Records Found			

Compliance Status

Compliance Rating:	▬ ▬ 🟩	**% of Non-Compliant Controls:**	0 %

Corporate Information

Company

Company	Description	Address	City	State	Zip Code
No Records Found					

Division

Division	Description	Key Contacts
No Records Found		

Business Unit

Business Unit	Description	Unit Head	Key Contacts
No Records Found			

Enterprise Data Migration

CVSH Policy:	CIST-0016 CIST-0018 CIST-0101 CITD-0005 CITD-0014 DOC-022425 ISPOL-061668	**hAetna First Published:**	7/8/2009
Published Date:	6/10/2021	**hAetna Standard ID (Numeric):**	248
		hAetna Standard Classification:	
Changed to top key control:		**Top Key Control ?:**	Yes
		Risk Category:	Data Protection Management - Encryption
Master Assessment:		**Tracking ID:**	151379
Change Request Status:	Completed	**Legacy Source Environment:**	hAetna
Record Status:	Updated		