KPMG LLP
Mission Towers I
Suite 100
3975 Freedom Circle Drive
Santa Clara, CA 95054

Independent Accountants' Report

To the Management of
Aetna Life Insurance Company:

We have examined the assertion by the management of Aetna Life Insurance Company ("Aetna"), regarding the disclosure of its key and certificate life cycle management business practices and the effectiveness of its controls over key and SSL certificate integrity, the authenticity of subscriber information, logical and physical access to CA systems and data, the continuity of key and certificate life cycle management operations, and development, maintenance and operation of systems integrity, based on the WebTrust® for Certification Authorities – SSL Baseline Requirements Audit Criteria, during the period January 1, 2015 through December 31, 2015, for the Aetna Inc. Certificate Authority (the "Aetna CA").

Aetna's management is responsible for its assertion. Our responsibility is to express an opinion on management's assertion based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants, and accordingly, included:

- Obtaining an understanding of Aetna's key and SSL certificate life cycle management business practices and its controls over
  - The key and SSL certificate integrity;
  - The continuity of key and certificate life cycle management operations;
  - The development, maintenance, and operation of systems integrity;
- Selectively testing transactions executed in accordance with disclosed SSL certificate life cycle management business practices;
- Testing and evaluating the operating effectiveness of the controls; and
- Performing such other procedures as we considered necessary in the circumstances.

We believe that our examination provides a reasonable basis for our opinion.

We noted the following issues that resulted in a modification of our opinion:

	WebTrust for CAs Baseline Criteria Requirements	Issues Noted
1	Principle 1, Criterion 1 requires that the CA discloses on its website its: • Certificate practices, policies and procedures, • all Cross Certificates that identify the CA as the Subject, provided that the CA arranged for or accepted the establishment of the trust relationship (i.e. the Cross Certificate at issue), and • its commitment to conform to the latest version of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates issued by the CA/Browser Forum. Principle 1, Criterion 4 requires that the Certificate Authority has controls to provide reasonable assurance that the CA CP and/or CPS that describes how the CA implements the latest version of the Baseline Requirements are updated annually. Principle 1, Criterion 5 requires that the CA and its Root has controls to provide reasonable assurance that there is public access to the CP and/or CPS on a 24x7 basis, and the content and structure of the CP and/or CPS are in accordance with either RFC 2527 or RFC 3647.	It was noted that: • The CPS does not reference the Baseline Requirements; • The CPS had not been updated or reviewed since 2011; • There is no process in place to update the CPS periodically; and • The CPS content and structure is not in accordance with the RFC 2527 or 3647 guidelines. It was also noted that Aetna's CA operations were inconsistent with the practices specified in the CPS including; Identification, Application Requirements, Certificate Information, Certificate Revocation, Physical Access Controls, CA Key Pair, Business Continuity Management, and Event Logging. This caused WebTrust for CAs Baseline SSL Requirements (WTBR) Principle 1, Criteria 1, 4 and 5 not to be met.
2	Principle 2, Criterion 4.1 requires that the CA maintains controls and procedures to provide reasonable assurance that as of the date the Certificate was issued, the CA obtains confirmation in accordance with the SSL Baseline Requirements Section 11.1 related to the Fully-Qualified Domain Name(s) and IP address(es) listed in the Certificate. Principle 2, Criterion 4.2 requires that the CA maintains controls and procedures to provide reasonable assurance that the following information provided by the Applicant is verified directly by performing the steps established by the SSL Baseline Requirements Section 11.2: • Identity • DBA/Trade name • Authenticity of Certificate Request • Verification of Individual Applicant • Verification of Country Principle 2, Criterion 4.3 requires that the CA maintains controls and procedures to provide reasonable assurance that it inspects any document relied upon for identity confirmation for alteration or falsification.	The Aetna CPS Section 3.1 states that, "all enrollment forms are subject to review, approval, and acceptance." Aetna compares certificate requests against a pre-validated list of domains and certificate requesters against a list of authorized requesters. However, it was noted that there was no process in place to revalidate the lists of domains and authorized requesters. It was also noted that there were 36 certificates issued to Coventry Health Care, a subsidiary of Aetna, during the examination period and each certificate included incorrect location information. This caused WTBR Principle 2, Criteria 4.1, 4.2 and 4.3 not to be met.

WebTrust for CAs Baseline Criteria Requirements		Issues Noted
3	Principle 2, Criterion 5.3 requires that the CA maintains controls to provide reasonable assurance that Certificates are revoked within 24 hours if any of the following events occurs: - The Subscriber requests in writing that the CA revoke the Certificate; - The CA is made aware that the Certificate was not issued in accordance with these Requirements or the CA's Certificate Policy or Certification Practice Statement.	We were informed that Aetna does not require response to revocation requests within a 24 hour period, as required by WTBR. We were informed that Aetna's standard procedures and guidelines are to respond to requests within 5 days. However, there is no structured or formal process for submitting revocation requests. This caused WTBR Principle 2, Criterion 5.3 not to be met.
4	Principle 2, Criterion 7.2 requires that the CA maintains controls to provide reasonable assurance that the following events are recorded: • CA and Subscriber Certificate lifecycle management events, including: - all verification activities stipulated in the Baseline Requirements and the CA's Certification Practice Statement - acceptance and rejection of certificate requests • security events, including: - entries to and exits from CA facility. • Log entries must include the following elements: - Date and time of entry - Identity of the person making the journal entry - Description of entry Principle 2, Criterion 7.3 requires that the CA has a policy and maintains controls to provide reasonable assurance that audit logs generated after the effective date of the Baseline Requirements are retained for at least seven years.	It was noted that: • physical *access* to the cage housing the CA system was not logged; • event logs for the CA prior to July 2015 were not available; and • logs are not reviewed periodically. This caused WTBR Principle 2, Criteria 7.2 and 7.3 not to be met.

WebTrust for CAs Baseline Criteria Requirements		Issues Noted
5	Principle 2, Criterion 7.2 requires that the CA maintains controls to provide reasonable assurance that: - the CA provides all personnel performing information verification duties (Validation Specialists) with skills-training that covers basic Public Key Infrastructure (PKI) knowledge, authentication and vetting policies and procedures (including the CA's Certificate Policy and/or Certification Practice Statement), common threats to the information verification process (including phishing and other social engineering tactics), and these Requirements. - the CA requires all Validation Specialists to pass an examination provided by the CA on the information verification requirements outlined in the Baseline Requirements. Principle 3, Criterion 5 requires that the Certificate Management Process MUST include: 4. user management, separate trusted-role assignments, education, awareness, and training	It was noted that no training programs were in place for Trusted Role personnel. This caused WTBR Principle 2, Criterion 7.2 and Principle 3, Criterion 5 not to be met.
6	Principle 2, Criterion 3.4 requires that the CA maintains controls and procedures to provide reasonable assurance that the CA, prior to the issuance of a Certificate, obtains a Subscriber and/or Terms of Use agreement in accordance with the SSL Baseline Requirements Section 10.3.1. That agreement contains provisions imposing obligations and warranties on the Application relating to: - the accuracy of information - reporting and revocation - termination of use of certificate - responsiveness	It was noted that Aetna has a subscriber agreement in place, but does not cover the following areas: · The accuracy of the information · Reporting and revocation · Termination of use of certificate, and · Responsiveness This caused WTBR Principle 2, Criterion 3.4 not to be met.
7	Principle 2, Criterion 4.7 requires that the CA maintains controls and procedures to provide reasonable assurance that the CA uses an internal database of all previously revoked Certificates and previously rejected certificate requests to identify subsequent suspicious certificate requests.	It was noted that Aetna maintains a database with all previously revoked certificates but it is not referenced during the validation portion of the certificate issuance process. It was also noted that previously rejected certificate requests are not stored in a database or referenced during the validation process to identify subsequent suspicious certificate requests. This caused WTBR Principle 2, Criterion 4.7 not to be met.

	WebTrust for CAs Baseline Criteria Requirements	Issues Noted
8	Principle 2, Criterion 8.3 requires that the CA maintains controls to provide reasonable assurance that it performs ongoing self-assessments on at least a quarterly basis against a randomly selected sample of at least three percent (3%) of the Certificates issued during the period commencing immediately after the previous self-assessment samples was taken.	It was noted that Aetna did not perform any audits on certificate issuance during the period. This caused WTBR Principle 2, Criterion 8.3 not to be met.
9	Principle 3, Criterion 2 requires that the CA performs a risk assessment at least annually that: • Identifies foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any Certificate Data or Certificate Management Processes; • Assesses the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Certificate Data and Certificate Management Processes; and • Assesses the sufficiency of the policies, procedures, information systems, technology, and other arrangements that the CA has in place to counter such threats. (See SSL Baseline Requirements Section 16.2)	It was noted that a security risk assessment of the Aetna CA operations was not performed during the examination period. This caused WTBR Principle 3, Criterion 2 not to be met.
10	Principle 3, Criterion 4 requires that the CA develops, implement, and maintain a Business Continuity Plan that includes at a minimum: - The conditions for activating the plan, - A maintenance schedule for the plan; - Awareness and education requirements; The Business Continuity Plan is tested at least annually, reviewed, and updated.	It was noted that the Aetna PKI business continuity plan does not cover the following: (1) conditions for activating the plan, (2) a maintenance schedule for the plan, and (3) awareness and education requirements. This caused WTBR Principle 3, Criterion 4 not to be met.
11	Principle 3, Criterion 5 requires that the Certificate Management Process MUST include: 4. user management, separate trusted-role assignments, education, awareness, and training Principle 4, Criterion 2 requires that the CA maintains controls to provide reasonable assurance that: - The responsibilities and tasks assigned to Trusted Roles are documented and “separation of duties” for such Trusted Roles based on the risk assessment of the functions to be performed is implemented. - Review all system accounts at least every 90 days and deactivate any accounts that are no longer necessary for operations	While Aetna has established a small team that is responsible for CA operations, It was noted that there is no separation of duties enforced within the team and each of the members of the team can perform the same level of system administration, certificate management, and key management functions. In addition, periodic logical access reviews of users with access to the CA systems were not performed during the period. This caused WTBR Principle 3, Criterion 5 and Principle 4, Criterion 2 not to be met.

WebTrust for CAs Baseline Criteria Requirements		Issues Noted
12	Principle 3, Criterion 7 requires that the CA maintains controls to provide reasonable assurance that CA systems development and maintenance activities are documented, tested, authorized, and properly implemented to maintain CA system integrity.	It was noted that approval was documented for each change but testing was not documented as required for the population of 6 PKI changes made during the examination period. This caused WTBR Principle 3, Criterion 7 not to be met.
13	Principle 4, Criterion 1 requires that the CA maintains controls to provide reasonable assurance that Certificate Systems are segmented into networks or zones based on their functional, logical, and physical (including location) relationship.	It was noted that the CA system and HSM are located within the Aetna data center and not physically or logically separated from the rest of Aetna's internal network. This caused WTBR Principle 4, Criterion 1 not to be met.
14	Principle 4, Criterion 1 requires that the CA maintains controls to provide reasonable assurance that configurations of Issuing Systems, Certificate Management Systems, Security Support Systems, and Front-End / Internal-Support Systems are reviewed on at least a weekly basis to determine whether any changes violated the CA's security policies. Principle 4, Criterion 3 requires that the CA maintains controls to provide reasonable assurance that Security Support System under the control of CA or Delegated Third Party Trusted Roles are implemented to monitor, detect, and report any security-related configuration change to Certificate Systems.	It was noted that the Aetna PKI issuing systems are not reviewed for configuration changes that violate their security policies. It was also noted that there were no tools implemented to monitor, detect, and report security-related configurations changes to Aetna's certificate systems. This caused WTBR Principle 4, Criteria 1 and 3 not to be met.
15	Principle 4, Criterion 4 requires that the CA maintains controls to provide reasonable assurance that: - Perform a Penetration Test on the CA's and each Delegated Third Party's Certificate Systems on at least an annual basis and after infrastructure or application upgrades or modifications that the CA determines are significant; and - Document that Vulnerability Scan and Penetration Test was performed by a person or entity with the skills, tools, proficiency, code of ethics, and independence necessary to provide a reliable Vulnerability Scan or Penetration Test.	It was noted that penetration testing was not performed on the PKI environment during the examination period. This caused WTBR Principle 4, Criterion 4 not to be met.

In our opinion, except for the effects of the matters discussed in the preceding table, in providing its Aetna SSL CA services at Hartford, Middletown, and Windsor, Connecticut, during the period January 1, 2015 through December 31, 2015, Aetna:

- Disclosed its certificate practices and procedures in its:
  - Aetna GeoRoot Certification Practice Statement, Version 1.1, dated September 24, 2011 ("Aetna CPS") on Aetna's website, including its commitment to provide SSL Certificates in

conformity with the applicable CA/Browser Forum Requirements, and provided such services in accordance with its disclosed practices

- Maintained effective controls to provide reasonable assurance that:
  - Subscriber information was properly collected, authenticated (for the registration activities performed by the CA, Registration Authority (RA) and subcontractor) and verified; and
  - the integrity of keys and certificates it manages was established and protected throughout their life cycles;
  - logical and physical access to CA systems and data was restricted to authorized individuals;
  - the continuity of key and certificate management operations was maintained; and
  - CA systems development, maintenance and operations were properly authorized and performed to maintain CA systems integrity.

based on the AICPA/CPA Canada WebTrust for Certification Authorities – SSL Baseline Requirements Audit Criteria, v2.0, for the Aetna CA.

The relative effectiveness and significance of specific controls at Aetna and their effect on assessments of control risk for subscribers and relying parties are dependent on their interaction with the controls, and other factors present at individual subscriber and relying party locations. We have performed no procedures to evaluate the effectiveness of controls at individual subscriber and relying party locations.

Because of the nature and inherent limitations of controls, the ability of Aetna to meet the aforementioned criteria may be affected. For example, controls may not prevent, or detect and correct, error, fraud, unauthorized access to systems and information, or failure to comply with internal and external policies or requirements. Also, the projection of any conclusions based on our findings to future periods is subject to the risk that changes may alter the validity of such conclusions.

This report does not include any representation as to the quality of Aetna's certification services beyond those covered by the AICPA/ CPA Canada WebTrust for Certification Authorities – Baseline Requirements Audit Criteria, nor the suitability of any of Aetna's services for any customers intended purpose.

KPMG LLP

Certified Public Accountants
Santa Clara, California
May 11, 2016

Assertion of Management as to
Its Disclosure of its Business Practices and its Controls Over
its Certification Authority Operations
During the period from January 1, 2015 through December 31, 2015

May 11, 2016

Aetna Life Insurance Company ("Aetna") provides its Aetna SSL certification authority (CA) services through the Aetna Inc. Certificate Authority (the “Aetna CA”).

The management of Aetna has assessed the disclosure of its certificate practices and its controls over its Aetna CA services. Based on that assessment, in Aetna Management’s opinion, in providing its Aetna CA services at Hartford, Middletown, and Windsor, Connecticut, during the period from January 1, 2015 through December 31, 2015, Aetna:

- Disclosed its certificate practices and procedures in its
  - Aetna GeoRoot Certification Practice Statement, Version 1.1, dated September 24, 2011 (“Aetna CPS”) including its commitment to provide SSL Certificates in conformity with the applicable CA/Browser Forum Guidelines
- Maintained effective controls to provide reasonable assurance that:
  - subscriber information was properly collected, authenticated (for the registration activities performed by the CA, Registration Authority (RA) and subcontractor) and verified; and
  - the integrity of keys and certificates it manages was established and protected throughout their life cycles;
  - logical and physical access to CA systems and data was restricted to authorized individuals;
  - the continuity of key and certificate management operations was maintained; and
  - CA systems development, maintenance and operations were properly authorized and performed to maintain CA systems integrity.

based on the AICPA/CPA Canada WebTrust for Certification Authorities – SSL Baseline Requirements Audit Criteria v2.0, except for the effects of the matters noted below:

	WebTrust for CAs Baseline Criteria Requirements	Issues Noted
1	Principle 1, Criterion 1 requires that the CA discloses on its website its: • Certificate practices, policies and procedures, • all Cross Certificates that identify the CA as the Subject, provided that the CA arranged for or accepted the establishment of the trust relationship (i.e. the Cross Certificate at issue), and • its commitment to conform to the latest version of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates issued by the CA/Browser Forum. Principle 1, Criterion 4 requires that the Certificate Authority has controls to provide reasonable assurance that the CA CP and/or CPS that describes how the CA implements the latest version of the Baseline Requirements are updated annually. Principle 1, Criterion 5 requires that the CA and its Root has controls to provide reasonable assurance that there is public access to the CP and/or CPS on a 24x7 basis, and the content and structure of the CP and/or CPS are in accordance with either RFC 2527 or RFC 3647.	It was noted that: • The CPS does not reference the Baseline Requirements; • The CPS had not been updated or reviewed since 2011; • There is no process in place to update the CPS periodically; and • The CPS content and structure is not in accordance with the RFC 2527 or 3647 guidelines. It was also noted that Aetna's CA operations were inconsistent with the practices specified in the CPS including; Identification, Application Requirements, Certificate Information, Certificate Revocation, Physical Access Controls, CA Key Pair, Business Continuity Management, and Event Logging. This caused WebTrust for CAs Baseline SSL Requirements (WTBR) Principle 1, Criteria 1, 4 and 5 not to be met.
2	Principle 2, Criterion 4.1 requires that the CA maintains controls and procedures to provide reasonable assurance that as of the date the Certificate was issued, the CA obtains confirmation in accordance with the SSL Baseline Requirements Section 11.1 related to the Fully-Qualified Domain Name(s) and IP address(es) listed in the Certificate. Principle 2, Criterion 4.2 requires that the CA maintains controls and procedures to provide reasonable assurance that the following information provided by the Applicant is verified directly by performing the steps established by the SSL Baseline Requirements Section 11.2: • Identity • DBA/Trade name • Authenticity of Certificate Request • Verification of Individual Applicant • Verification of Country Principle 2, Criterion 4.3 requires that the CA maintains controls and procedures to provide reasonable assurance that it inspects any document relied upon for identity confirmation for alteration or falsification.	The Aetna CPS Section 3.1 states that, "all enrollment forms are subject to review, approval, and acceptance." Aetna compares certificate requests against a pre-validated list of domains and certificate requesters against a list of authorized requesters. However, it was noted that there was no process in place to revalidate the lists of domains and authorized requesters. It was also noted that there were 36 certificates issued to Coventry Health Care, a subsidiary of Aetna, during the examination period and each certificate included incorrect location information. This caused WTBR Principle 2, Criteria 4.1, 4.2 and 4.3 not to be met.

WebTrust for CAs Baseline Criteria Requirements		Issues Noted
3	Principle 2, Criterion 5.3 requires that the CA maintains controls to provide reasonable assurance that Certificates are revoked within 24 hours if any of the following events occurs: - The Subscriber requests in writing that the CA revoke the Certificate; - The CA is made aware that the Certificate was not issued in accordance with these Requirements or the CA's Certificate Policy or Certification Practice Statement.	We were informed that Aetna does not require response to revocation requests within a 24 hour period, as required by WTBR. We were informed that Aetna's standard procedures and guidelines are to respond to requests within 5 days. However, there is no structured or formal process for submitting revocation requests. This caused WTBR Principle 2, Criterion 5.3 not to be met.
4	Principle 2, Criterion 7.2 requires that the CA maintains controls to provide reasonable assurance that the following events are recorded: • CA and Subscriber Certificate lifecycle management events, including: - all verification activities stipulated in the Baseline Requirements and the CA's Certification Practice Statement - acceptance and rejection of certificate requests • security events, including: - entries to and exits from CA facility. • Log entries must include the following elements: - Date and time of entry - Identity of the person making the journal entry - Description of entry Principle 2, Criterion 7.3 requires that the CA has a policy and maintains controls to provide reasonable assurance that audit logs generated after the effective date of the Baseline Requirements are retained for at least seven years.	It was noted that: • physical *access* to the cage housing the CA system was not logged; • event logs for the CA prior to July 2015 were not available; and • logs are not reviewed periodically. This caused WTBR Principle 2, Criteria 7.2 and 7.3 not to be met.

	WebTrust for CAs Baseline Criteria Requirements	Issues Noted
5	Principle 2, Criterion 7.2 requires that the CA maintains controls to provide reasonable assurance that: - the CA provides all personnel performing information verification duties (Validation Specialists) with skills-training that covers basic Public Key Infrastructure (PKI) knowledge, authentication and vetting policies and procedures (including the CA's Certificate Policy and/or Certification Practice Statement), common threats to the information verification process (including phishing and other social engineering tactics), and these Requirements. - the CA requires all Validation Specialists to pass an examination provided by the CA on the information verification requirements outlined in the Baseline Requirements. Principle 3, Criterion 5 requires that the Certificate Management Process MUST include: 4. user management, separate trusted-role assignments, education, awareness, and training	It was noted that no training programs were in place for Trusted Role personnel. This caused WTBR Principle 2, Criterion 7.2 and Principle 3, Criterion 5 not to be met.
6	Principle 2, Criterion 3.4 requires that the CA maintains controls and procedures to provide reasonable assurance that the CA, prior to the issuance of a Certificate, obtains a Subscriber and/or Terms of Use agreement in accordance with the SSL Baseline Requirements Section 10.3.1. That agreement contains provisions imposing obligations and warranties on the Application relating to: - the accuracy of information - reporting and revocation - termination of use of certificate - responsiveness	It was noted that Aetna has a subscriber agreement in place, but does not cover the following areas: · The accuracy of the information · Reporting and revocation · Termination of use of certificate, and · Responsiveness This caused WTBR Principle 2, Criterion 3.4 not to be met.
7	Principle 2, Criterion 4.7 requires that the CA maintains controls and procedures to provide reasonable assurance that the CA uses an internal database of all previously revoked Certificates and previously rejected certificate requests to identify subsequent suspicious certificate requests.	It was noted that Aetna maintains a database with all previously revoked certificates but it is not referenced during the validation portion of the certificate issuance process. It was also noted that previously rejected certificate requests are not stored in a database or referenced during the validation process to identify subsequent suspicious certificate requests. This caused WTBR Principle 2, Criterion 4.7 not to be met.
8	Principle 2, Criterion 8.3 requires that the CA maintains controls to provide reasonable assurance that it performs ongoing self-assessments on at least a quarterly basis against a randomly selected sample of at least three percent (3%) of the Certificates issued during the period commencing immediately after the previous self-assessment samples was taken.	It was noted that Aetna did not perform any audits on certificate issuance during the period. This caused WTBR Principle 2, Criterion 8.3 not to be met.

WebTrust for CAs Baseline Criteria Requirements		Issues Noted
9	Principle 3, Criterion 2 requires that the CA performs a risk assessment at least annually that: • Identifies foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any Certificate Data or Certificate Management Processes; • Assesses the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Certificate Data and Certificate Management Processes; and • Assesses the sufficiency of the policies, procedures, information systems, technology, and other arrangements that the CA has in place to counter such threats. (See SSL Baseline Requirements Section 16.2)	It was noted that a security risk assessment of the Aetna CA operations was not performed during the examination period. This caused WTBR Principle 3, Criterion 2 not to be met.
10	Principle 3, Criterion 4 requires that the CA develops, implement, and maintain a Business Continuity Plan that includes at a minimum: - The conditions for activating the plan, - A maintenance schedule for the plan; - Awareness and education requirements; The Business Continuity Plan is tested at least annually, reviewed, and updated.	It was noted that the Aetna PKI business continuity plan does not cover the following: (1) conditions for activating the plan, (2) a maintenance schedule for the plan, and (3) awareness and education requirements. This caused WTBR Principle 3, Criterion 4 not to be met.
11	Principle 3, Criterion 5 requires that the Certificate Management Process MUST include: 4. user management, separate trusted-role assignments, education, awareness, and training Principle 4, Criterion 2 requires that the CA maintains controls to provide reasonable assurance that: - The responsibilities and tasks assigned to Trusted Roles are documented and “separation of duties” for such Trusted Roles based on the risk assessment of the functions to be performed is implemented. - Review all system accounts at least every 90 days and deactivate any accounts that are no longer necessary for operations	While Aetna has established a small team that is responsible for CA operations, It was noted that there is no separation of duties enforced within the team and each of the members of the team can perform the same level of system administration, certificate management, and key management functions. In addition, periodic logical access reviews of users with access to the CA systems were not performed during the period. This caused WTBR Principle 3, Criterion 5 and Principle 4, Criterion 2 not to be met.
12	Principle 3, Criterion 7 requires that the CA maintains controls to provide reasonable assurance that CA systems development and maintenance activities are documented, tested, authorized, and properly implemented to maintain CA system integrity.	It was noted that approval was documented for each change but testing was not documented as required for the population of 6 PKI changes made during the examination period. This caused WTBR Principle 3, Criterion 7 not to be met.

WebTrust for CAs Baseline Criteria Requirements		Issues Noted
13	Principle 4, Criterion 1 requires that the CA maintains controls to provide reasonable assurance that Certificate Systems are segmented into networks or zones based on their functional, logical, and physical (including location) relationship.	It was noted that the CA system and HSM are located within the Aetna data center and not physically or logically separated from the rest of Aetna's internal network. This caused WTBR Principle 4, Criterion 1 not to be met.
14	Principle 4, Criterion 1 requires that the CA maintains controls to provide reasonable assurance that configurations of Issuing Systems, Certificate Management Systems, Security Support Systems, and Front-End / Internal-Support Systems are reviewed on at least a weekly basis to determine whether any changes violated the CA's security policies. Principle 4, Criterion 3 requires that the CA maintains controls to provide reasonable assurance that Security Support System under the control of CA or Delegated Third Party Trusted Roles are implemented to monitor, detect, and report any security-related configuration change to Certificate Systems.	It was noted that the Aetna PKI issuing systems are not reviewed for configuration changes that violate their security policies. It was also noted that there were no tools implemented to monitor, detect, and report security-related configurations changes to Aetna's certificate systems. This caused WTBR Principle 4, Criteria 1 and 3 not to be met.
15	Principle 4, Criterion 4 requires that the CA maintains controls to provide reasonable assurance that: - Perform a Penetration Test on the CA's and each Delegated Third Party's Certificate Systems on at least an annual basis and after infrastructure or application upgrades or modifications that the CA determines are significant; and - Document that Vulnerability Scan and Penetration Test was performed by a person or entity with the skills, tools, proficiency, code of ethics, and independence necessary to provide a reliable Vulnerability Scan or Penetration Test.	It was noted that penetration testing was not performed on the PKI environment during the examination period. This caused WTBR Principle 4, Criterion 4 not to be met.

Aetna Life Insurance Company

Brian Heemsoth
Director, Information Security