**Section 105.50 Audit Requirements**

a) CMS shall submit to an annual PKI compliance audit to be performed by the Auditor General of Illinois or an independent auditor selected by the Department contracted specifically for the purpose of auditing the State's PKI operations.

b) An independent auditor must demonstrate competence in the field of compliance audits and must regularly perform compliance audits as a primary responsibility, and shall attest that it has significant experience in the application of public key cryptographic technologies and computer security.

c) The annual audit investigates the operations of CMS and RAs with respect to the State PKI to ensure their compliance with the CP and the CPS. Areas of focus for these audits include, but are not limited to:

1) Identification & Authentication

A) Initial Registration

B) Routine Rekey

C) Rekey After Revocation

D) Revocation Request

2) Operational Requirements

A) Certificate Application

B) Certificate Issuance

C) Certificate Acceptance

D) Key Recovery

E) Certificate Suspension/Revocation

F) Computer Security Audit Procedures

G Records Archival

H) CA Key Changeover

I) Compromise and Disaster Recovery

J) CA Termination

3) Physical, Procedural & Personnel Security

A) Physical Security Controls

B) Procedural Controls

C) Personnel Security Controls

4) Technical Security Controls

A) Key Pair Generation & Installation

B) Private Key Protection

C) Other Aspects of Key Pair Management

D) Activation Data

E) Computer Security Controls

F) Lifecycle Security Controls

G) Network Security Controls

H) Cryptographic Module Engineering Controls

5) Certificate & CRL Profiles

A) Certificate Profile

B) CRL Profile

6) Specification Administration

A) Contact Information

B) Specification Change Procedures

C) Publication and Notification Procedures

D) Approval Procedures