COMMONWEALTH OF PENNSYLVANIA
DEPARTMENT'S OF PUBLIC WELFARE, INSURANCE AND AGING

INFORMATION TECHNOLOGY STANDARD

Name Of Standard: **Risk Management**	Number: **STD-ENSS031**
Domain: **Security**	Category:
Date Issued: **09/07/2012**	Issued By Direction Of:
Date Revised: **10/11/2013**	 Shirley A. Monroe, Dir of Div Technical Engineering

Abstract:

The department has established an IT Risk Management (ITRM) solution to assist the department's efforts to continuously monitor the regulatory compliance posture of the IT assets. As part of this effort, the department requires the appropriate program office (system stakeholder) to conduct a security risk assessment.

Risk management is the process of identifying risk, assessing risk and developing mitigating controls to reduce that risk. The purpose of this standard is to assist the department in meeting this goal.

The Risk Management Standard also helps to achieve following:
Better secure the IT systems that store, process, or transmit organizational information.
Enable management to make well-informed risk management decisions to justify the expenditures that are part of the IT budget.
Assist management in authorizing the IT systems on the basis of the supporting documentation resulting from the performance of the risk assessment.

General:

The Risk Management Standard applies to the Department of Public Welfare (DPW; "Department"). The processes outlined in this document should assist the department to better manage IT risks by establishing acceptable level of controls and associated measurable compliance criteria.

Standard:

The Chief Information Security Officer (CISO) or his/her designee shall adhere to the following general risk management process.

Identify risk trigger: The risk process is triggered by periodic events that require formal risk assessment. The CISO or his/her designee shall identify the risk trigger based on the following criteria:

1. Mandated risk assessments conducted on a periodic basis, such as those required by regulatory drivers
2. Event based risk assessments that are triggered by one of the following:
    - introduction of new systems/applications
    - system/application upgrades
    - significant technology changes
    - security incidents

Determine risk assessment scope: The scope of the risk assessment shall be defined and documented by the CISO or his/her designee before the risk assessment begins. This documentation shall include all applicable assessment assumptions and exceptions.

Assess risk: The CISO or his/her designee shall assess the extent of potential threats and vulnerabilities associated with department assets. The output of this process shall assist to validate or identify appropriate controls for reducing or eliminating risk during the risk mitigation process. The assessment activities are divided into the following categories:

- IT systems risk assessment (e.g., IT Infrastructure)
- Internal risk assessment/inspection of DPW facilities

The IT systems risk assessment shall be conducted on a periodic basis or after one of the risk triggers identified above. A baseline assessment shall be conducted at least once every year.

The appropriate system owners shall submit a security risk self-assessment questionnaire using the department's ITRM RSA Archer solution. The department's security architecture section shall review the self-assessment and determine potential risks to:

- IT infrastructure
- application/software – both COTS and custom development

The internal risk assessment/inspection of the DPW headquarters, Data Power House (DPH) and Vital Records Incorporated (VRI) facilities shall be conducted annually. An internal risk assessment/inspection of the County Assistance Offices (CAO) shall be conducted once every 3 years. The appropriate system owners shall submit a security risk self-assessment questionnaire using the department's ITRM RSA Archer solution.

The department's security architecture section shall review the self-assessment and determine potential risks to:

- headquarters location
- field offices
- data center (DPH)
- offsite storage facilities

Please refer to the department's Web/Mobile Application and Infrastructure Vulnerability Assessment standards for details on conducting the respective assessments. Please also refer to the security practices at the end of this section for a description documentation to incorporate into the risk management process.

Develop risk response: The CISO or his/her designee shall develop a response plan that considers all possible alternatives, including whether to avoid a risk, accept it and mitigate where possible, and/or transfer it.

The risk response plan shall include an evaluation of recommended preventive, detective, deterrent and corrective control options. The objective is to select the most appropriate control options for minimizing risk.

DPW management shall review the presented risk response plan and determine if the risk, given current controls, is acceptable. The CISO or his/her designee shall document management's decision and resources shall be prioritized and allocated before the selected plan is executed.

Track compliance: The CISO or his/her designee shall collect, maintain and follow-up on results of the risk assessment and the department's adherence to the implements controls.

Sustain and continuously improve: The CISO or his/her designee shall work with DPW management to evaluate risk management process and implement periodic improvements as necessary.

Security Practices

The department should, as part of leading industry practices, develop and incorporate the following as part of the documentation of the risk management process.

Information Security Policy

The CISO or his/her designee shall work with DPW management to document and periodically revise a comprehensive security policy.

Information Classification

The CISO or his/her designee shall work with DPW management to document and periodically revise an information classification scheme and information handling guidelines.

Roles & Responsibilities

The CISO or his/her designee shall work with DPW management to define, document and revise as necessary, all the dedicated functions within the department's security architecture section.

Legal & Regulatory Compliance

The CISO or his/her designee shall work with DPW management to document, track and assess compliance with relevant security and privacy laws and regulations.

Asset Management

The CISO or his/her designee shall work with the appropriate system owners to identify, classify and track department hardware/software in an asset inventory.

Physical Protection

The CISO or his/her designee shall work with DPW management to document and assess the mechanisms in place to control access to department facilities. An inspection of the physical protection controls shall be conducted annually.

Identity & Access Management

The CISO or his/her designee shall work with DPW management to document and periodically revise the various identity and access management processes.

Baseline Configuration

The CISO or his/her designee shall work with the appropriate system owners to identify, documents and periodically revise baseline configuration for department systems and applications. A baseline assessment shall be conducted every 3 years.

Patch Management
The CISO or his/her designee shall work with the appropriate system owners to document and periodically revise a formalized patch management process.

Backup Management
The CISO or his/her designee shall work with the appropriate system owners to document and periodically revise a formalized data backup and restoration process.

Security Assessments
The CISO or his/her designee shall work with the appropriate system owners and application developers, to conduct and document scheduled risk/vulnerability assessments of department network infrastructure and applications.

Security Monitoring
The CISO or his/her designee shall work with the appropriate system owners to document and assess the mechanisms in place for malware protection, intrusion detection and security event logging. The overall security posture shall be measured and reported on a periodic basis.

Incident Response Management
The CISO or his/her designee shall work with DPW management to define, document and revise as necessary, incident response and notification procedures.

Plan of Action & Milestones (POA&M) & Corrective Action Plan (CAP)
System owners shall develop and submit a Plan Of Action & Milestones (POA&M) / CAP for the information system using the DPW/ITRM solution (e.g., RSA Archer) to document DPW's planned remedial actions to correct weaknesses and/or deficiencies (e.g., findings on security controls assessment, security impact analysis and monitoring activities) and help reduced known vulnerabilities.

Exemptions from this Standard:
Any team that is unable to comply with this standard must discuss any exemption request with the department's Chief Information Security Officer (CISO).

Refresh Schedule:
All standards and referenced documentation identified in this standard will be subject to review and possible revision annually or upon request by the DPW Information Technology Standards Team.

Standard Supplements:
None

References:
1. NIST SP800-30: Risk Management Guide for Information Technology Systems

Standard Revision Log:

Change Date	Version	Change Description	Author and Organization
09/07/2012	1.0	Risk Management	Clifton Van Scyoc
10/11/2013	1.1	Updated Security practices, POA&M, CAP and Security Authorization	Pamela Skelton
07/29/2014	1.1	Reviewed, no changes	Pamela Skelton