COMMONWEALTH OF PENNSYLVANIA
DEPARTMENT OF PUBLIC WELFARE

INFORMATION TECHNOLOGY STANDARD

Name Of Standard: **IS Measures of Performance**	Number: **STD-ENSS036**
Domain: **Security**	Category:
Date Issued: **11/13/2013**	Issued By Direction Of:  Shirley Monroe, Dir of Div of Tech Engineering
Date Revised:	

Abstract:
The department has established a Risk & Performance Dashboard solution to assist the department's efforts to continuously monitor and report on information security measures of performance. This includes definition of the establishment of key risks, associated key risk indicators and the collection of metrics related to these indicators.

A performance indicator is an essential element for organizational performance measurement. It is commonly used to evaluate an organization success on a particular activity in which it is engaged. Success is measured in terms of making progress toward strategic goals or simply the repeated achievement of some level operational goals.

General:
The information security measures of performance standard apply to the Department of Public Welfare (DPW; "Department"). The processes outlined in this document should assist the department to better manage the monitoring and reporting of performance by establishing key risk/performance indicators and metrics related to the indicators.

Standard:
This standard provides an overview of the steps required to deliver a comprehensive risk & performance process and dashboard solution. This includes definition of key risks, KRI/KPIs and associate to an operating environment; establishment of thresholds, weights; a baseline escalation process and triggers.

Establish Key Risks, KRI and associate to operating environment
The department should, as part of leading industry practices, develop and incorporate the following steps to establish a baseline for the risk performance process:

- DPW shall identify key risks/areas or components to be monitored

- Key Risk Indicators (KRIs) shall then be identified and defined to be used in a key risk monitoring system (e.g., eGRC tools, dashboards, reports on performance, steering committee presentations)
- For each KRI selected, the organization shall identify where in the DPW operating environment the KRI exists.
- Associate the indicators with DPW operating environment.

Establish Roles & Responsibilities

- The department shall define roles and responsibilities to provide management comment on performance results and adequate incident response plan.
- Beyond normal BAU (Business As Usual) activities, roles and responsibilities shall be documented to define the proper communication channels, and the additional steps that need to be taken.
- The organization shall identify specific roles and responsibilities to approve the values, weights, and thresholds that may have been identified.
- Access authorizations to dashboards views shall be configured and documented for various users and roles.

Establish Thresholds and Weights

The CISO or his/her designee shall work with the management team to establish thresholds for determining whether a control is operating effectively. As part of this activity, the minimum requirements are described as follow:

- DPW organization shall define thresholds and tuning values for selected KRIs
- DPW individual indicator owners shall identify those thresholds
- The levels each indicator will be at to move from green to yellow and yellow to red shall be defined
- For indicators that are combined to derive a risk value, the weights (e.g., importance) of each indicator shall be established.
- The frequency of each DPW indicators (e.g., quarterly, monthly, weekly, daily, or hourly) shall be defined.
- Any timing issues and interdependencies shall be documented.

Refine Thresholds and Weights

The CISO or his/her designee shall periodically work with DPW management to refine, document and revise as necessary the following:

- Thresholds and weights shall be refined annually to effectively monitor and report on key risks
- Existing DPW indicators shall be reviewed periodically for automation
- Thresholds and weights shall be monitored as the environment expands and contracts.

Design Escalation Process and Triggers

The CISO or his/her designee shall design at a minimum, the following security controls:

- Triggers/notifications that would initiate an escalation process for each risk/ indicator shall be clearly defined
- Escalation process for those risks/indicators shall be designed and documented
- Detailed process document for the refined process shall be developed.

Configure Reports and Dashboards
This section provides an overview of the steps required to deliver a risk & performance dashboard solution. This includes definition of reporting requirements, establishment of key risks, risk and performance criteria, associated indicators and metrics collection process related to these indicators;

The DPW organization shall work with each individual indicator owners, mid-level management, and senior management to identify:

- reporting product owners & end users
- reporting requirements, formats and input sources
- existing ad-hoc reporting and current gaps
- report generation process (e.g., timing, dependencies, calculations, analytics)
- reporting product submission timeline

In addition, the organization shall review interim report products with external / internal stakeholders.

Train Users
DPW shall continuously conduct training for the various types of system users, including:

- Executive management
- Line management
- Dashboard and end users
- KR & KRI owners
- Technical administrators
- Business analysts

The following table describes a list of department key performance indicators and the corresponding threshold requirements for each item:

Thread	**Key Performance Indicators**	**Thresholds**		
		High	Medium	Low
Identity and Access Management	Availability	< 99%	< 99.8%	> 99.8%
	Change in user base	+- 10%	+- 5%	+- 3%
	User Authentications	+- 10%	+- 5%	+- 3%
	User Authorizations	+- 10%	+- 5%	+- 3%
	DPRA Usage Count	TBD	TBD	TBD
	BPSS Admin Password Reset (New)	TBD	TBD	TBD
	IAM ACD Calls	TBD	TBD	TBD
	IAM VHD Tickets	TBD	TBD	TBD
Security Incident Management	Reported security incidents	2+	1	0
	External network intrusions[4]	2+	1	0
Vulnerability Management	Identified in Production	2+	1	0
	DPW Microsoft Server Security Patch Compliance (660 clients)	< 80%	80-90%	> 90%
	DPW Microsoft Desktop Security Patch Compliance (17,886 clients)	< 80%	80-90%	> 90%
	PACSES Server Security Patch Compliance(130 clients)	< 80%	80-90%	> 90%
	PACSES Desktop Server Security Patch Compliance (3,149 clients)	< 80%	80-90%	> 90%
IT Risk Management	Percentage of critical security and compliance projects "at risk"	> 30%	20-30%	< 20%
	External audit responses that have not been submitted on schedule (in past 12 months)	> 30%	20-30%	< 20%
	Self-assessments that have been scheduled but not conducted on-time(in past 12 months)	> 30%	20-30%	< 20%
	Number of findings from internal assessments and external audits	TBD	TBD	TBD
	Past due Corrective Action Plans (CAP) – management, technical and operational	> 30%	20-30%	< 20%

Regulatory Compliance	Days since the last IT security risk framework revision	> 365	183-365	< 183
	DPW policies and standards that were planned for revision and reviewed in the last month	Non-compliant		Compliant
Training and awareness	DPW employees and contractors who have not completed mandatory trainings[1] on-time within the past 12 months	> 30%	20-30%	< 20%
	Management role with staff that are past due (> 30 days) for compliance with mandatory security awareness training	> 30%	20-30%	< 20%
	Information Security and Technology awareness communications (email distributions and bulletin board postings) distributed within the past 12 months	TBD	TBD	TBD

[1] Includes security awareness trainings

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:

Standard Revision Log:

Change Date	Version	Change Description	Author and Organization
10/11/2013	1.0	Initial Draft	Mathieu Saury
11/13/2013	1.0	Sign Off	Clifton Van Scyoc