Information Technology Risk Management (ITRM) Program

NOMINATING CATEGORY: RISK MANAGEMENT INITIATIVES

NOMINATOR: TERESA A. SHUCHART
DEPARTMENT OF PUBLIC WELFARE (DPW)
COMMONWEALTH OF PENNSYLVANIA
1006 HEMLOCK DR
HARRISBURG, PA 17110

PROJECT INITIATION DATE: JULY 2011
PROJECT COMPLETION DATE: DECEMBER 2011
Executive Summary

The Department of Public Welfare (DPW) is responsible for meeting the needs of more than two million Pennsylvanians with the assistance of 15,000 support workers, 500,000 providers, and 300,000 employers. Information technology plays a critical role in supporting DPW’s goals and objectives. The significance of the technology infrastructure required to manage this complex organization is reflected in the department’s annual information systems budget, which has averaged about $160 million in recent years.

DPW’s connected IT infrastructure exists in an environment that is governed by quickly evolving, complex regulatory requirements, including more than 40 DPW security standards, commonwealth policies, and state and federal regulations. Managing IT security risk and compliance in this complex regulatory environment is further complicated by overlapping and sometimes conflicting regulatory requirements, inconsistent interpretations of regulations, and confusion around acceptable minimum standards.

DPW’s regulatory landscape includes:

- Federal Internal Revenue Service (IRS) publication 1075
- Health Information Privacy and Accountability Act (HIPAA)
- Health Information Technology for Economic and Clinical Health (HITECH) Act
- Social Security Administration – Computer Matching and Privacy Protection Act

DPW’s IT Risk Management (ITRM) program is driven by the need for higher accountability and governance in the face of stricter regulatory requirements and rising citizen expectations. The ITRM program enables the department to act proactively to reduce risk exposure and unwanted surprises during external audits. This program helps DPW navigate the above challenges by identifying and satisfying relevant regulatory requirements with relevant reporting.

DPW’s ITRM program has streamlined and simplified the department’s existing regulatory audit management processes using a single security regulatory risk framework and centralized solution. As DPW’s program and technology requirements continue to grow and evolve, so will the demands placed on the ITRM program. With a view into the future, the ITRM program is established to help DPW management take effective, risk-based decisions and improve DPW’s compliance posture. The commonwealth is looking to expand and scale the successful implementation of DPW’s ITRM solution to the commonwealth IT enterprise in order to attain similar benefits.

Introducing DPW’s Security Risk Framework

DPW’s security risk framework effort rationalized more than 40 unique, authoritative security requirement sources and 3,491 individual requirements from DPW standards, Commonwealth policies, PA code, federal regulations and leading industry standards into 349 integrated and rationalized security requirements.
Business Problem and Solution Description


Challenge: Information is the lifeblood of DPW, whether it is citizen data or business partner information. The traditional landscape and scope for protecting this data will be entering a new era, as the federal government invests billions in health care as part of the recent health care reform legislation. Whether it is the broader purview of the HIPAA, or the widespread adoption and use of health information technologies (HIT) under the HITECH Act, there will be new and significant pressure to meet these ever-mounting security and privacy regulatory challenges.

Solution: DPW established an integrated security regulatory risk framework that rationalizes more than 4,000 individual requirements from more than 40 DPW standards, commonwealth policies, and state and federal regulations into 350 integrated requirements. The security risk framework enables DPW to assess and prioritize security, privacy and compliance risks, then identify the appropriate risk response strategy, such as mitigating risk through appropriate controls, risk transfer and accepting risk.

The department also uses the security risk framework to conduct periodic risk assessments on its IT assets and processes, select treatment options, monitor the effectiveness of mitigation techniques, and support annual reporting for federal and commonwealth compliance requirements. Figure 1 below illustrates DPW’s approach to develop the risk framework.

![Figure 1: DPW’s approach to develop an integrated security risk framework from applicable regulatory requirements.](image-url)
Benefit: The department’s vision of maintaining a single security regulatory risk framework helped to apply a unified security posture across the enterprise. This unified method helped to conduct quick gap analysis and take corrective actions – forming an effective approach to perform periodic self-assessments and manage the overall information security posture in the enterprise.

Case Study 2: Use of automation to facilitate continuous risk monitoring and remediation, and report assessment results

Challenge: DPW’s Risk Framework is a technology agnostic approach to managing risk and one of the pioneers in the public sector. At the time of inception, it was an extensive and detailed Microsoft Excel-based tool that contained more than 4,000 rows of security and privacy requirements and their associated controls. The manually intensive task of maintaining the risk framework, such as keeping the library of rationalized requirements current, tracking open compliance issues and generating assessment templates, could be an onerous and time-consuming activity.

Solution: DPW considered use of an automated risk management platform (DPW ITRM solution) to help alleviate many of the above challenges. Streamlining processes onto a single platform enabled DPW to help evaluate and satisfy multiple requirements with a single assessment. DPW selected EMC Archer as the platform for the ITRM solution. The figure below depicts modules of DPW ITRM solution.

![Figure 2: DPW ITRM solution components](image)

Benefit: DPW ITRM solution helped create automated workflows to support indexing, capturing and reporting on regulatory compliance requirements. More important, this solution helped improve the adoption and scalability of the risk assessment and management process across the enterprise. DPW used the automated platform to perform the following:

- Maintain the library of rationalized security and privacy requirements
- Develop risk profiles for critical assets
- Document technical controls and link them to authoritative sources
• Perform continuous risk and compliance monitoring and report results through self-assessments (by the responsible asset owner)
• Monitor remediation activities to mitigate gaps and audit findings

The figure below depicts a high-level overview of some of the regulatory findings on DPW’s key IT assets managed using ITRM solution.

![Open Findings by Assessment](image)

**Figure 3:** DPW ITRM solution dashboard depicting audit findings on some of DPW’s key IT assets

**Case Study 3: Authoritative source to manage regulatory audit reports and information**

**Challenge:** DPW is audited by more than 13 state and federal agencies annually, including:

- State Auditor General – Generally Acceptable Accounting Practices (GAAP) and Single Audit
- Internal Revenue Service (IRS) – onsite review of two key program areas every three years along with relevant annual/periodic reporting
- U.S. Department of Health and Human Services (HHS)
- U.S. Department of Agriculture (USDA)
- Social Security Administration (SSA)

The above mentioned agencies conduct independent audits on the applicable DPW program offices and provide reports and corrective actions. Previously, the related periodic audit reporting, onsite reviews and corrective action plans were managed independently by the audited program office. The data was stored in silos within the department’s program offices using Microsoft Access databases, Excel spreadsheets, documents and scanned reports. In addition, the department did not have a single audit calendar to help prepare in advance for upcoming regulatory audit reviews.

In some cases, simply being able to produce records of past audits was a challenge. One program area was unable to locate a regulatory audit response for two months. This effort identified a key challenge - “maintaining data in silos is inefficient,” – independently collecting and analyzing audit reports requires more effort than a central risk management solution.
Solution: DPW’s centralized DPW ITRM solution automated and streamlined the department’s regulatory audit and risk assessment processes – managed in a centralized location by one team. DPW ITRM solution helped transform traditional document/paper-based audit processes to an enterprise system that maintains a library of DPW’s regulatory requirements. This transformation has effectively reduced the redundant storage of audit reports in silos at multiple locations within the enterprise.

**Before – Information in silos**

- Audit Calendar (None)
- Assign stakeholders (Email)
- Audit reports (Documents/Print)
- Track Findings (Documents/Access)
- Corrective Action Plan (Documents)

**Current – Automated solution**

![Diagram showing the transformation of regulatory audit data management](image)

*Figure 4: DPW ITRM solution transformed regulatory audit data management*

**Benefit:** DPW’s ITRM solution has emerged as the authoritative repository to centrally manage audit reports, responses, findings and corrective actions in digital form. In addition, the platform has become the “unified solution” for requesting and accessing regulatory audit reports.

**Project Significance**

DPW’s adoption of the ITRM program and its subsequent introduction of the ITRM solution are part of the department’s enterprise mission to address many of its regulatory audit reporting challenges. It is likely that similar challenges are driving other states to take similar actions to realize improvements to their security risk management programs. The following list enumerates DPW-specific examples of how ITRM program impacted the department:

- Accessibility of real-time regulatory compliance reports helped the department’s management team **make decisions quickly and effectively.**
- The **centralized risk management platform** reduced the regulatory risk of information stored in silos within several program offices, and encouraged sharing of audit findings and related remediation plans in the enterprise.
- Maintaining regulatory reports and corrective action plans using the ITRM solution helped in **continuity of regulatory operations**, even in the absence of required stakeholders.
- Improved identification of gaps and implementing remediation controls helped to **meet several regulations using a single security risk framework.**
- **Scaling DPW ITRM solution to the commonwealth IT enterprise** will help attain similar benefits for the larger stakeholder group.

**Project Benefits**

DPW’s ITRM program is one of the very first undertakings using automation for risk and compliance management in the public sector. This program established an integrated security regulatory risk framework across the DPW enterprise.

Operationalizing of DPW’s ITRM solution is one of the key achievements of this program. The ITRM solution emerged into a centralized “single window” model to facilitate, respond to, and manage external audits – **effectively reducing redundancy in storage of audit data, increasing reliability of the stored regulatory audit information, and saving effort and cost associated with conducting redundant security risk assessments and remediation.** The ITRM solution has transformed into DPW’s authoritative source for maintaining regulatory audit-related information.

The ITRM solution’s dashboards are designed for decision makers and technical specialists to make informed decisions and **effectively delegate proactive steps towards corrective actions.** The ITRM solution provides a real-time dashboard of the department’s regulatory compliance posture to the executive management and business stakeholders. This dashboard can further detail the regulatory risk posture of a particular security domain, a business unit or an IT asset.

DPW recently used its ITRM solution to assist in managing information for two onsite audit reviews – IRS publication 1075 and HIPAA. ITRM solution helped manage pre-audit questionnaire, audit reports, corrective action plans (CAP) and supporting documents. **Use of ITRM solution reduced CAP turnaround to IRS to three weeks** – which prior to the integrated management process and tool would have taken months.

**Encouraging information sharing and reuse,** the data collected for the IRS audit was used to respond to the HIPAA pre-audit questionnaires. **The HIPAA pre-audit questionnaire response was provided to HHS within three days.** The quality of information management also enabled only a single meeting with HHS during its onsite review, using the material managed through the ITRM solution.