The Computerworld Honors Program

Honoring those who use Information Technology to benefit society

Final Copy of Case Study

Status:
Laureate

Year:
2013

Organization Name:
Department of Public Welfare

Organization URL:
http://www.dpw.state.pa.us

Project Name:
Information Technology Risk Management (ITRM) program

Please select the category in which you are submitting your entry:
Safety & Security

Please provide an overview of the nominated project. Describe the problem it was intended to solve, the technology or approach used, how it was innovative and any technical or other challenges that had to be overcome for successful implementation and adoption. (In 300 words or less.)

The Commonwealth of Pennsylvania's Department of Public Welfare (DPW) is the state's largest agency. DPW's Information Technology (IT) infrastructure routinely handles sensitive Personally Identifiable Information (PII) to maintain eligibility programs supporting the needs of over two million citizens. Protecting citizen PII is statutorily required and is vitally important to safeguard citizen trust in DPW and the Commonwealth. Challenge: DPW's ITRM program is driven by the need to better manage information security risks, protect citizen data and avoid surprises during external audits. The recent large-scale data breaches in other state governments and private industry underscore the requirements for a robust security program. In addition, the DPW's IT environment is governed by evolving regulatory requirements derived from Federal requirements, over 45

DPW standards, Commonwealth policies and regulations, including: Internal Revenue Service publication 1075, Health Information Privacy and Accountability Act, Health Information Technology for Economic and Clinical Health Act, and Social Security Administration. As DPW's program and technology requirements evolved, so did the demands placed on its ITRM program. Solution: The ITRM program helps DPW to navigate the above challenges by proactively identifying IT security risks and reducing their exposure. This program streamlines DPW's existing regulatory audit management processes starting with establishing a security risk framework and embracing automation for a centralized ITRM solution. DPW's security risk framework rationalizes more than 4,000 individual regulatory requirements into 350 unique integrated requirements (depicted in Appendix 1). This detailed Microsoft Excel-based framework contains the regulatory requirements and their integrated controls. This technology agnostic approach to manage risks is still a pioneer in state governments. With a view into the future, DPW has embraced automation, using an RSA Archer solution, to make effective risk-based decisions, constantly monitor and review DPW's compliance posture and prepare

When was this project implemented or last updated? (Please specify month and year.) Has it incorporated new technologies and/or other innovations since its initial deployment? (In 300 words or less.)

DPW continues to stay abreast of its growing regulatory needs through the ITRM program. This program was operationalized through the following phases: Phase 1 Development and operationalizing the DPW security risk framework: Feb 2010 to August 2010. Phase 2 Embracing automation: DPW's adoption of IT for enterprise risk management included the following sub-phases: DPW ITRM solution Product selection: September 2010 December 2010, DPW ITRM solution (EMC Archer) hardware, software configuration: Feb 2011 April 2011, DPW ITRM solution customization and integration of DPW security risk framework: May 2011 July 2011, Operationalizing DPW ITRM solution to support IRS 1075 questionnaires, reports, external audits and internal assessments: August 2011 December 2012, Operationalizing DPW ITRM solution to support HIPAA questionnaires, reports, external audits and internal assessments: Jan 2012 March 2012, Operationalizing DPW ITRM solution to support SSA (for DPW mainframe) external audits and internal assessments: Apr-May 2012, Operationalizing DPW ITRM solution to support U.S. Department of Agriculture Temporary Assistance for Needy Families (TANF)/National Directory for New Hires (NDNH), Pennsylvania State GAAP external audits and internal assessments: June 2012 Sep 2012, and Operationalizing DPW ITRM solution to support DPW's SSA State On-line Query (SOLQ) interface (for DPW web application) external audit, security design plan and self-certification: Oct 2012 Dec 2012.

Is implementation of the project complete? If no, please describe the project's phases and which phase the project is now in. (In 300 words or less.)

Yes, the department's ITRM program is operational. The project implementation timelines are provided in response to Q6. The department continues to enhance the solution to expand to the growing demands of the enterprise and changes to its regulatory landscape to effectively monitor the regulatory compliance posture of the DPW enterprise. The department is also sharing the best practice with other Commonwealth agencies.

Please provide at least one example of how the technology project has benefited a specific individual or organization. Feel free to include personal quotes from individuals who have directly benefited from the work. (In 300 words or less.)

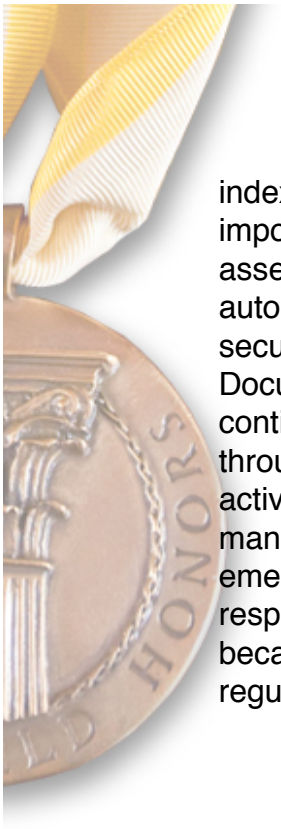
This program is one of the first undertakings using automation for risk and compliance management in the public sector. Operationalizing DPW's ITRM solution is one of the key achievements of this program. The ITRM solution emerged into a centralized "single window" model to facilitate, respond to, and 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 (Appendix 3). The ITRM solution has transformed into DPW's authoritative source for maintaining regulatory audit-related information. In addition, the ITRM solution is helping to better articulate security risks to the business stakeholders and document risk management decisions and rationale. The ITRM solution's dashboards (Appendix 4) are designed for decision makers to make better, 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 DPW's 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 help manage information for periodic audit reviews IRS 1075, SSA 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 for HIPAA pre-audit questionnaires. The HIPAA pre-audit questionnaire response was provided to HHS within three days. The quality of information management managed by the ITRM solution enabled only a single meeting with HHS during

Would this project be considered an innovation, a best practice or other notable advancement that could be adopted by or tailored for other organizations and uses? If yes, please describe that here. (In 300 words or less.)

Yes. DPW's ITRM program is one of the most effective adoptions of technology for enterprise risk management and original in its application amongst state governments. This program uses an innovative shared services model to be efficient in mitigating regulatory risks at the state government level. Through this program, DPW is effectively able to govern and manage its IT security risks and compliance. DPW is realizing the following benefits from its ITRM program: 1. Improved security risk management. The department's IT management and business stakeholders have better visibility into its real-time compliance posture. This visibility helps DPW effectively manage, measure, and improve the department's security risks and maintain compliance. 2. Efficiency and cost savings. DPW is able to utilize critical project resources and technology more efficiently by sharing application risk management expertise and experience across the enterprise. The centralized platform reduces the regulatory risk information stored in silos within several program offices, and encourages sharing of audit findings and related remediation plans in the enterprise. 3. Assess once comply with many. DPW is able to integrate a variety of regulatory requirements into a single, holistic security risk framework based approach for assessing, understanding, reporting, and managing security risks as part of periodic internal assessments across the breadth of the DPW IT infrastructure. This allows DPW to be more prepared for federal and state regulatory audits and reduce its information security risk exposure. It is likely that similar challenges are driving other states and take similar actions. The DPW ITRM program's shared service approach opens the possibility of establishing a similar model for intra-state and inter-state risk management in the future. The Commonwealth is looking to expand and scale the successful implementation of DPW's ITRM solution to the Commonwealth IT enterprise for achieving similar

If there are any other details that the judges should know about this project, please note them here. (In 300 words or less.)

The benefits obtained from the ITRM program includes: 1. DPW Security Risk Framework An Integrated Repository of Security Regulatory Requirements: 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. 2. Use of automation to facilitate continuous risk monitoring and remediation, and report assessment results: 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 a 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 assessment results through self-assessments (by the responsible asset owner). Monitor remediation activities to mitigate gaps and audit findings. 3. Having an authoritative source to manage regulatory audit reports and information: 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 became the "unified solution" for security risk management and performing regulatory audit reports.