Government Information Quarterly 32 (2015) 316–322

Contents lists available at ScienceDirect

Government Information Quarterly

journal homepage: www.elsevier.com/locate/govinf

# Government data does not mean data governance: Lessons learned from a public sector application audit

Nik Thompson [a,*], Ravi Ravindran [b], Salvatore Nicosia [b]

[a] School of Engineering and Information Technology, Murdoch University, South Street, Murdoch, Western Australia, Australia
[b] Murdoch University, Australia

ARTICLE INFO

*Article history:*
Received 18 November 2014
Received in revised form 11 May 2015
Accepted 16 May 2015
Available online 4 June 2015

*Keywords:*
Data protection
Public sector
Governance
Case study
Data management

ABSTRACT

Public sector agencies routinely store large volumes of information about individuals in the community. The storage and analysis of this information benefits society, as it enables relevant agencies to make better informed decisions and to address the individual's needs more appropriately. Members of the public often assume that the authorities are well equipped to handle personal data; however, due to implementation errors and lack of data governance, this is not always the case. This paper reports on an audit conducted in Western Australia, focusing on findings in the Police Firearms Management System and the Department of Health Information System. In the case of the Police, the audit revealed numerous data protection issues leading the auditors to report that they had no confidence in the accuracy of information on the number of people licensed to possess firearms or the number of licensed firearms. Similarly alarming conclusions were drawn in the Department of Health as auditors found that they could not determine which medical staff member was responsible for clinical data entries made. The paper describes how these issues often do not arise from existing business rules or the technology itself, but a lack of sound data governance. Finally, a discussion section presents key data governance principles and best practices that may guide practitioners involved in data management. These cases highlight the very real data management concerns, and the associated recommendations provide the context to spark further interest in the applied aspects of data protection.



## 1. Introduction

The massive uptake and sheer pervasiveness of technological innovation in the private and public sectors have facilitated the creation of vast information repositories. The storage, analysis and interpretation of these repositories are only possible due to the strides in technology. This analysis and interpretation allows agencies to make faster and better informed decisions to best serve the needs of the people. However, with this data storage come concerns about privacy and security. Public concerns about large scale data collection often invoke an emotional response, as the dystopian "Big Brother" image is invoked. These concerns have generally increased over time, and the recent media attention given to the topic of government surveillance does little to allay these fears.

States have addressed these concerns with statutes designed to regulate how data is handled and thus protect the people. Indeed, for many people there is an implicit assumption that public sector agencies are capable and well equipped to handle this data with which they have been entrusted. In practice, this is not a straightforward issue. Setting aside any potential issues directly within the statutes, the key issue with technical environments is that for the statutes to be enforced adequately, data custodians must be experts in both technology as well as policy.

This paper considers the management of information assets within the public sector, with specific case references made to findings by the Western Australian (WA) Office of the Auditor General and the US Government Accountability Office. Though the affected agencies specified provide high level recommendations to any adverse findings in their own reports, this paper will provide more detailed suggestions to address the deficiencies from an organizational data management perspective.

## 2. Background

The WA Office of the Auditor General benchmarks selected public sector agencies primarily against the ISO 27002 international standard for Information Security (International Organization for Standardization, 2013b) while also referring occasionally to other established standards. As the standards used are international or nationally recognized, this paper will be relevant for any other organizations that have information assets to manage and protect. Furthermore, it is to be noted that many of the issues identified are not directly linked to the standards or statutes in play, but relate more to general principles of how private data should

* Corresponding author.
*E-mail address:* n.thompson@murdoch.edu.au (N. Thompson).

http://dx.doi.org/10.1016/j.giq.2015.05.001
0740-624X/

be handled. In a similar way to the WA Office of the Auditor General, the US Government Accountability Office refers to established legislation and standards such as the US Federal Information Security Management Act of 2002 (FISMA) when determining compliance within agencies (United States Government, 2002). FISMA recognizes the importance of data protection and mandates the protection of US federal information and information systems through various controls, including yearly audits to be conducted in federal agencies.

The ISO 27002 standard is a code of practice for information security; as such it contains a large number of best practices and controls which may be implemented to support the development of organizational security standards. These controls are placed into groupings to identify relevant subject areas in familiar domains such as physical and environmental security, HR security, asset management and communications security. As ISO 27002 is not a management standard it is not possible to obtain certification to this standard, instead it is to be considered complementary to the ISO 27001 — Information Security Management certification (International Organization for Standardization, 2013a) as it provides greater detail and specifications of controls. In Western Australian public sector agencies, compliance with these standards is not mandatory, however as the framework is internationally recognized and proven, it forms a useful baseline against which auditing and evaluation may be performed. A further benefit of using such widely recognized standards is the fact that there is often a relatively direct mechanism by which to map between controls in the various standards. For instance, a mapping has already been created across ISO27001/27002, the SANS 20 Critical Security controls and the NIST SP 800-53 (Johnson, 2013).

On March 27, 2007, Justice (Commissioner) Kevin Hammond of the WA Corruption and Crime Commission (CCC) made what is considered by many as a landmark frank and honest statement about the behavior of some senior public servants in Western Australia. Justice Hammond stated "*it is clear there are many quite influential public officers who wouldn't recognise a conflict of interest if it walked up and kicked them in the backside*" (Hammond, 2007). In a report to the WA Parliament in 2010, the CCC reported on the alleged access of a confidential information system by an Associate to a Judge of the District Court of Western Australia. The Judge's Associate had numerous associations with drug dealers and had inappropriately accessed information from the Court's information systems. This report re-emphasized the CCC view that that there was no such thing as an innocuous enquiry of a confidential database when the persons driving the enquiry are operating with criminal intent (Parliament of Western Australia, 2010). In a similar vein, the US Government suffered a historically significant and embarrassing security leak when a relatively junior US service officer, Bradley Manning was able to access and subsequently release thousands of US government classified documents in 2010.

The above examples are indicative of the scale and potential for breaches within the public sector. The WA Office of the Auditor General has made many findings and recommendation on the behavior and practices of public sector agencies in managing their information assets. The US Government Accountability Office in Sept 2013 found that almost all of the major federal agencies had flaws with their controls in detecting and limiting access to information systems (US Government Accountability Office, 2013).

There is an expectation from the community that information collected, accessed and used by public sector agencies will be protected and also used only for the purpose it was intended. There is also a community expectation that there will be standards, practices and procedures in relation to data access, data privacy, data security and data disposal with overarching data governance in place.

The following sections of this paper will discuss some examples of improper practices identified by WA Office of the Auditor General in the area of controlling and protecting information assets specifically in an information systems environment. These examples are gleaned from the Information Systems Audit Report (Western Australian Auditor General, 2013) which details an application audit conducted on five applications at four agencies. The audit process for these business applications involved a systematic review of the documentation and operational aspects of the applications to provide assurance in the following domains:

1. Policies and procedures.
2. Data preparation (input and processing).
3. Interface control suitability to enforce data quality requirements.
4. Maintenance of master data files.
5. Audit trail of activities.
6. Segregation of duties (staff must perform duties relevant to their role only).
7. Backup and recovery provisions in the event of system malfunction or disaster.

The agencies were selected due to the fact that inappropriate management or controls in these agencies would cause a significant impact. The four agencies chosen were Western Australia Police, Department of Finance, Department of Mines and Petroleum and Department of Health (2 applications). While there were minor issues identified in all of the agencies, the cases presented in subsequent sections will elaborate on the findings in two of these agencies as these are particularly problematic and very relevant to the data management focus of this paper. The paper will go on to introduce some high level recommendations and potential solutions to mitigate the effect of these issues.

Although the case study primarily uses examples from the WA Public Sector, it is not implied that the problem is unique to Western Australia. It is the strong belief of the authors that the issues reported are consistent across the globe and the recommendations may serve as a guide to IT practitioners in various industries when they evaluate their data management protocols.

## 3. The importance of data protection

Data management is defined within the DAMA Data Management Body of Knowledge (DAMA-DMBOK) as the development, execution and supervision of plans, policies, programs and practices that control, protect, deliver and enhance the value of data and information asset (Mosley, Brackett, Earley, & Henderson, 2009).

There is a justifiably strong emphasis on the protection of information assets within DAMA-DMBOK. Public sector agencies in the course of their work routinely collect a vast amount of information relating to organizations, partner agencies and of course individuals. The Western Australia Police Service for example maintains details of the criminal activity, allegations, and investigations on many individuals within Western Australia, as well as detailed historical records, the integrity of which is crucial in order for the Police Service to fulfill their duties. Using this agency as an example, unauthorized access of their information holdings may have the potential impact of:

- Causing reputational and physical damage to individuals or organizations.
- Tipping off individuals to ongoing investigations.
- Causing loss of confidence in the officers of the service.
- Creating operational delays and inefficiencies due to internal reviews and investigations.

The Western Australian Planning Commission as another example maintains details of future plans. Within the repositories of this agency lie details of potential land and building deals, preferred contractors and details of tenders. Should this information fall into the wrong hands, it may have the potential impact of:

- Individuals or companies taking advantage of insider information to benefit financially from land procurement.