AUDIT REPORT

Citizens Data Warehouse

Audit Opinion:  Needs Improvement

Date:  June 9, 2014

Report Number: 2014-AUD-IT-01
## Table of Contents:

### Executive Summary

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Background</td>
<td>1</td>
</tr>
<tr>
<td>Management’s Assessment and Reporting on Controls</td>
<td>2</td>
</tr>
<tr>
<td>Audit Objectives and Scope</td>
<td>3</td>
</tr>
<tr>
<td>Individual Section Ratings</td>
<td>3</td>
</tr>
<tr>
<td>Audit Opinion</td>
<td>3</td>
</tr>
</tbody>
</table>

### Appendix

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Definitions</td>
<td>5</td>
</tr>
<tr>
<td>Issue Classifications</td>
<td>6</td>
</tr>
<tr>
<td>Distribution</td>
<td>8</td>
</tr>
<tr>
<td>Audit Performed By</td>
<td>8</td>
</tr>
</tbody>
</table>
Executive Summary

Background

Business Intelligence (BI) is a process of analyzing business information to enable more effective strategic, tactical, and operational insights and decision-making. A data warehouse is a collection of large volumes of data from multiple operational systems that is integrated and designed into one database for reporting and analysis.

At Citizens, the Enterprise Information Management (EIM) team is responsible for providing this service to business units through the Citizens Data Warehouse as well as Data Architecture and Information Management. The EIM team is led by the Manager – IT Enterprise Information Management, and consists of a staff of 23 individuals, 10 of which are temporary personnel. EIM is part of the Claims Policy and Billing Systems group which is led by the Director, Application Development and Delivery, and is part of the Application Delivery Services organization which is led by the VP, Application Delivery.

The BI solutions implemented with the Citizens Data Warehouse cover many of the standard capabilities for the insurance industry and are depicted in the following diagram:
Executive Summary

Citizens uses the Cognos® OLAP (Online Analytical Processing) tool which offers functionality called an Analytic Cube. Typically this is a representation of business important measures summarized by a selectable set of objects or dimensions. The cube provides summarized business facts for key business dimensions in a flexible presentation with quick response.

The Analytic Cubes for Personal Lines and Wind-only Underwriting and Claims information provide advanced insurance metrics in statistical, aggregated views of the information. The cubes are available via Analysis Services on the Cognos® Portal. The most commonly used Cubes have data that dates back to 2002 and are the Personal Residential Calendar Year, Accident Year, and Loss Development Cubes. Similar cubes are available that contain data from the Wind Policy System.

With Enterprise Dashboards, the business user is presented with graphical representations of key weekly Business Operations, Underwriting and Claims metrics. The dashboard reports provide an at-a-glance snapshot of the business metrics in an interactive presentation with filter criteria selectable by the business user.

Standard reports provide Claims, Underwriting and Agent Administration groups with traditional, list-based or summary reports. Ad-hoc reporting puts the power of selectable output fields, filter criteria, sorting and subtotaling functionality in the hands of the business user. Last, the EIM group has a Quick Response Report team of individuals to assist any business user with the creation of reports or extracts against complicated or limited access data.

With the implementation of the Citizens Insurance Suite (CIS) Claims Center in May, 2013, the EIM group has been engaged in integrating the data from CIS into the existing Business Intelligence solutions provided by CDW and Cognos. In addition, the Guidewire® application has its own data mart and provides near real-time reporting.

This audit marks the first time that OIA has assessed the control infrastructure around the Citizens Data Warehouse.

Management’s Assessment and Reporting on Controls

With this audit, and for the first time, the OIA has created an opportunity for the audit client to share its knowledge of any control weaknesses that are known to exist and their plans to remediate these known weaknesses. This process is intended to foster an environment whereby management and staff conduct periodic proactive reviews of controls and are aware of the risks to the business. It will also enable OIA to focus its audit efforts on areas where it can add the greatest value to the organization.

At the start of the CDW audit, EIM management shared with OIA the following control weaknesses and their remediation plans:

- **Administrative access to CDW databases** - EIM management reported that as part of the project to load Kronos data into CDW, it had undertaken an effort to “clean up” administrative access to the CDW servers and databases. This process commenced in November, 2013 and is not yet completed.
Executive Summary

- Developer access to production environments - EIM management reported that developers are involved in deploying new software into production systems. A project is targeted for kick-off in mid-year to enable IT Operations personnel to deploy new software into production systems.

In the course of the audit, OIA assessed the remediation plans, mentioned above, and noted that these are managed well and would be sufficient to mitigate the control failures identified.

Audit Objectives and Scope

The objective of this audit was to assess the input, processing, output and security controls to ensure that data provided by the Citizens Data Warehouse is available, accurate, accessible to only authorized individuals, and meets the information requirements of the organization.

The audit considered the following areas related to Citizens Data Warehouse:

- Source data extract, transformation and loading (ETL) into the CDW
- Administrative access to the CDW
- Disaster Recovery (DRP) and Business Continuity (BCP) capabilities
- Program change management procedures
- Training and documentation for use by end users in conjunction with Cognos® and Advanced Query Tool® (AQT)
- Existence and usage of “unofficial” (non-IT) data repositories for Business Intelligence purposes
- Restricted information stored in CDW

Individual Section Ratings

<table>
<thead>
<tr>
<th>Section</th>
<th>Rating</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source data extract, transformation, and loading (ETL)</td>
<td>Needs Improvement</td>
</tr>
<tr>
<td>Administrative access</td>
<td>Needs Improvement</td>
</tr>
<tr>
<td>Disaster Recovery (DRP) and Business Continuity (BCP)</td>
<td>Satisfactory</td>
</tr>
<tr>
<td>Program change management procedures</td>
<td>Needs Improvement</td>
</tr>
<tr>
<td>Training and documentation for use by end-users</td>
<td>Needs Improvement</td>
</tr>
<tr>
<td>Existence and usage of “unofficial” (non-IT) data repositories; end user access to CDW data</td>
<td>Needs Improvement</td>
</tr>
<tr>
<td>Restricted information stored in CDW</td>
<td>Needs Improvement</td>
</tr>
</tbody>
</table>

Audit Opinion

The overall effectiveness of the processes and controls evaluated during the audit is rated as Needs Improvement.

We found that generally, the CDW is serving the needs of the organization. New software releases are implemented at least weekly to deliver new BI capabilities related to CIS, as well as new feature requests and routine fixes. EIM is currently working with Ernst and Young and the business units on a project to enhance the CDW and provide even greater BI capabilities to the organization.
Our work, however, indicated specific areas where opportunities for improvement were noted. These include:

- **The need to better understand source data extract, transformation, and loading (ETL) related to the Guidewire® (CIS) data mart** - Guidewire® uses a different method of storing data in its data mart than that which is used in the CDW. As a result, the data must be queried differently than data is queried from the CDW, and in some cases the required results cannot readily be obtained. Standard reports and end-user ad hoc queries which do not take this difference into consideration may provide inaccurate results.

- **The need to manage administrative access to CDW databases** - There is a considerable number of IT personnel who have full administrative access (sysadmin) to the CDW databases and activity for these individuals is not monitored. Nefarious activity by these users, including the use of Restricted Information related to policyholders, claimants, adjusters, etc., which is located on the Staging and Reporting servers, could go undetected.

- **The need to improve Program Change Management** - Segregation of duties is lacking whereby developers from the ETL and Cognos® groups are involved in deploying new software into production systems. Allowing developers to have access to production systems increases the risk that software that has not been reviewed, tested and approved may be installed. Also, the process to manage and report on open defect tickets for CDW, especially those which are priority 5 (required to be able to do business and there is no manual work around), should be enhanced. Unresolved defects may adversely impact business performance and decision-making.

- **The need to better understand, manage and monitor the Existence and Usage of “Unofficial” (non-IT) Data Repositories and End User Access to CDW Data** - Users who have been granted access to extract data directly from CDW database tables are not required to complete a formal training program before they are granted access. While data models and data dictionaries exist, not all of these users are aware of them, and those who are aware of them have varying degrees of understanding. There are no controls in place to limit or monitor what data is extracted and the organization does not have a policy to govern how the information is used to support business activities. A lack of appropriate training and understanding of data models and data dictionaries may result in unreliable information being used to support the business and may be incongruous with the goals of the Enterprise Information Management program. Furthermore, if Restricted Information from the CDW was contained in any of these data extracts, there is virtually no way to protect it or control its use or distribution.

- **The need to encrypt Restricted Information Stored in CDW** - Restricted Information related to policyholders, claimants, adjusters, etc., from legacy systems such as CAIS, CTS, ePAS and eWind is not encrypted in the CDW. The failure to encrypt Restricted Information stored in the CDW increases the risk that the Restricted Information could be used for illegitimate purposes, resulting in adverse legal and financial consequences for Citizens. Since Restricted Information from legacy systems will remain in CDW for historical reporting long after the legacy systems are retired from use, it is important that this Restricted Information be secured.

We would like to thank management and staff for their cooperation and professional courtesy throughout the course of this audit.
Appendix 1

Definitions

Audit Ratings

Satisfactory:
Critical internal control systems are functioning in an acceptable manner. There may be no or very few minor issues, but their number and severity relative to the size and scope of the operation, entity, or process audited indicate minimal concern. Corrective action to address the issues identified, although not serious, remains an area of focus.

Needs Improvement:
Internal control systems are not functioning in an acceptable manner and the control environment will require some enhancement before it can be considered as fully effective. The number and severity of issues relative to the size and scope of the operation, entity, or process being audited indicate some significant areas of weakness. Overall exposure (existing or potential) requires corrective action plan with priority.

Unsatisfactory:
One or more critical control deficiencies exist which would have a significant adverse effect on loss potential, customer satisfaction or management information. Or the number and severity of issues relative to the size and scope of the operation, entity, or process being audited indicate pervasive, systemic, or individually serious weaknesses. As a result the control environment is not considered to be appropriate, or the management of risks reviewed falls outside acceptable parameters, or both. Overall exposure (existing or potential) is unacceptable and requires immediate corrective action plan with highest priority.
### Issue Classifications

<table>
<thead>
<tr>
<th>Control Category</th>
<th>High</th>
<th>Medium</th>
<th>Low</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Financial Controls</strong>&lt;br&gt;(Reliability of financial reporting)</td>
<td>• Actual or potential financial statement misstatements &gt;USD 5 million&lt;br&gt;• Control issue that could have a pervasive impact on control effectiveness in business or financial processes at the business unit level&lt;br&gt;• A control issue relating to any fraud committed by any member of senior management or any manager who plays a significant role in the financial reporting process</td>
<td>• Actual or potential financial statement misstatements between USD 2.5 million to 5 million&lt;br&gt;• Control issue that could have an important impact on control effectiveness in business or financial processes at the business unit level</td>
<td>• Actual or potential financial statement misstatements below USD 2.5 million&lt;br&gt;• Control issue that does not impact on control effectiveness in business or financial processes at the business unit level</td>
</tr>
<tr>
<td><strong>Operational Controls</strong>&lt;br&gt;(Effectiveness and efficiency of operations)</td>
<td>• Actual or potential losses &gt;USD 2.5 million&lt;br&gt;• Achievement of principal business objectives in jeopardy&lt;br&gt;• Customer service failure (e.g., excessive processing backlogs, unit pricing errors, call centre non responsiveness for more than a day) impacting 10,000 policyholders or more or negatively impacting a number of key corporate accounts&lt;br&gt;• Actual or potential prolonged IT service failure impacts one or more applications and/or one or more business units&lt;br&gt;• Actual or potential negative publicity related to an operational control issue&lt;br&gt;• An operational control issue relating to any fraud committed by any member of senior management or any manager who plays a significant role in operations&lt;br&gt;• Any operational issue</td>
<td>• Actual or potential losses between USD 0.5 to 2.5 million&lt;br&gt;• Achievement of principal business objectives may be affected&lt;br&gt;• Customer service failure (e.g., processing backlogs, unit pricing errors, call centre non responsiveness) impacting 1,000 policyholders to 10,000 or negatively impacting a key corporate account&lt;br&gt;• Actual or potential IT service failure impacts more than one application for a short period of time&lt;br&gt;• Any operational issue</td>
<td>• Actual or potential losses below USD 0.5 million&lt;br&gt;• Achievement of principal business objectives not in doubt&lt;br&gt;• Customer service failure (e.g., processing backlogs, unit pricing errors, call centre non responsiveness) impacting less than 1,000 policyholders&lt;br&gt;• Actual or potential IT service failure impacts one application for a short period of time</td>
</tr>
</tbody>
</table>
### Appendix 2

<table>
<thead>
<tr>
<th>Control Category</th>
<th>High</th>
<th>Medium</th>
<th>Low</th>
</tr>
</thead>
<tbody>
<tr>
<td>Leading to death of an employee or customer</td>
<td>Actual or potential for public censure, fines or enforcement action (including requirement to take corrective actions) by any regulatory body which could have a significant financial and/or reputational impact on the Group</td>
<td>Actual or potential for public censure, fines or enforcement action (including requirement to take corrective action) by any regulatory body</td>
<td>Actual or potential for non-public action (including routine fines) by any regulatory body</td>
</tr>
<tr>
<td>Compliance Controls (Compliance with applicable laws and regulations)</td>
<td>Any risk of loss of license or regulatory approval to do business</td>
<td>Areas of non-compliance identified which could ultimately lead to the above outcomes</td>
<td>Areas of non-compliance identified which could ultimately lead the above outcome</td>
</tr>
<tr>
<td></td>
<td>Areas of non-compliance identified which could ultimately lead to the above outcomes</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>A control issue relating to any fraud committed by any member of senior management which could have an important compliance or regulatory impact</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remediation timeline</td>
<td>Such an issue would be expected to receive immediate attention from senior management, but must not exceed 60 days to remedy</td>
<td>Such an issue would be expected to receive corrective action from senior management within 1 month, but must be completed within 90 days of final Audit Report date</td>
<td>Such an issue does not warrant immediate attention but there should be an agreed program for resolution. This would be expected to complete within 3 months, but in every case must not exceed 120 days</td>
</tr>
</tbody>
</table>
Appendix 3

Distribution

Addressees: Aditya Gavvala, V.P., Application Delivery
Robert Sellers, V.P., IT Infrastructure and Operations
Mitch Brockbank, Director, IT Security and Risk

Copies: Tom Lynch, Citizens Audit Committee Chairman
Juan Cocuy, Citizens Audit Committee Member
Freddie Schinz, Citizens Audit Committee Member
Barry Gilway, President/CEO/Executive Director
Kelly Booten, Chief – Systems and Operations
Curt Overpeck, Chief Information Officer
John Rollins, Chief Risk Officer
Dan Sumner, General Counsel and Chief Legal Officer
Christine Turner Ashburn, V.P. – Communications, Legislative and External Affairs
Debby Kearney, Ethics and Compliance Officer
Bruce Meeks, Inspector General
Gary Bryant, Director – IT Operations
Chris Jobczynski, Director – Application Development and Delivery
Greg Niehoff, Manager – Enterprise Information Management
Johnson Lambert, LLP (External Auditors)

Following Audit Committee Distribution
The Honorable Rick Scott, Governor
The Honorable Jeff Atwater, Chief Financial Officer
The Honorable Pam Bondi, Attorney General
The Honorable Adam Putnam, Commissioner of Agriculture
The Honorable Don Gaetz, President of the Senate
The Honorable Will Weatherford, Speaker of the House of Representatives

Audit Performed By

Auditor in Charge Gary Sharrock
Audit Director Karen Wittlinger

Under the Direction of Joe Martins, Chief of Internal Audit