Legistar # 190668.

FINAL INTERIM REPORT II

Audit of the General Government Enterprise Resource Planning System Implementation

Interim Report II

December 5, 2019

A Report to the City Commission

Mayor
Lauren Poe

Mayor-Commissioner Pro Tem
Harvey Ward

Commission Members

David Arreola

Adrian Hayes-Santos

Gail Johnson

Gigi Simmons

Helen K. Warren

City Auditor's Office
City of Gainesville

Interim City Auditor
Leonard F. Loria

EXECUTIVE SUMMARY
December 5, 2019

FINAL INTERIM REPORT II

Why We Did This Audit

Properly configured processes are essential to the ERP implementation's overall success. Misconfigured processes and data reduces the ERP's ability to meet the needs of the business units. This audit is part two of the ERP that was included in the City Auditor's 2020 Fiscal Year Annual Audit Plan.

What We Recommend

The ERP project team should:

- Ensure that employees' personally identifiable information is adequately protected by including a data steward in the configuration phase.
- Work with the vendor to create a single consolidated view of all configuration changes.
- Ensure all data conversion information is accurate.
- Include data accuracy in configuration status reports to management.

BACKGROUND

The objective of the Configure and Prototype Stage is for business owners to review the configuration of the WORKDAY® application based on their current business process and configuration specifications. The cost to identify and fix errors increases once the application is implemented into production. Cost can be decreased by more than one third when errors are corrected in the development process in which they were introduced.

The Configure and Prototype phase (see Figure 1) was conducted from July 15, 2019 through September 20, 2019. To assist in identifying errors, Collaborative Solutions (Implementer) conducted customer confirmation sessions, updated requirements with members of general government, and performed unit testing.

OBJECTIVES

The objectives of this audit were to determine the overall effectiveness of the Enterprise Resource Planning (ERP) System's Configure and Prototype process in relation to the best practices delineated in *COBIT 2019 Build, Acquire, and Implement No. 10 Managed Configuration.* To accomplish our objectives, we focused on the following specific areas:

1. Is there an established configuration management model?
2. Are configuration documents stored in a repository?
3. Are reconfigured changes adequately documented and approved?
4. Are configuration status reports performed?

WHAT WE FOUND

- The Configure and Prototype process included active and retired employees' personal information, which is stored in different tenants[1] within the WORKDAY® Platform. Data security controls exist, however, they have not been reviewed and approved by a data steward to ensure that security is enforced and employee information remains secure.
- Configuration documents are adequately stored in SharePoint as a central repository. However, we did identify that three of the 51 SharePoint users were retired or terminated. Upon our notification, the accounts were disabled.
- Reconfigured Payroll and Data Conversion configuration changes were informally documented and approved.
- Configuration status is reported through multiple mechanisms, however, status reports did not include data accuracy results.

[1] A WORKDAY® tenant is a separate copy of the programming environment that is independent of other tenants.

SCOPE AND METHODOLOGY

This engagement focused on the configuration controls of the payroll and data conversion processes, respectively. The audit methodology was based on guidance provided by *COBIT*[2] 2019 *Build, Acquire, and Implement No. 10 Managed Configuration* and also the National Institute of Standards and Technology (NIST) Special Publication 800-53 Revision 5 Draft *Security and Privacy Controls for Information Systems and Organization* control objectives. During the engagement, we attended meetings, interviewed key personnel, observed and mapped processes, examined documents, and attended the payroll customer confirmation sessions.

OBJECTIVES AND CONCLUSIONS

1. Is there an established configuration management model?

Yes. The project follows the Cynergy™ Deployment Methodology, described below in Figure 1 – Implementation Methodology, provided by the vendor. The Configure and Prototype phase is the third of five phases in the overall implementation process. While attending customer confirmation sessions, we noted that an employee data snapshot was uploaded into the different WORKDAY® tenants. Typically, there are fewer data security controls while the project is in the pre-deployment phase. Business units had access to all of the data during the Configure and Prototype phase.

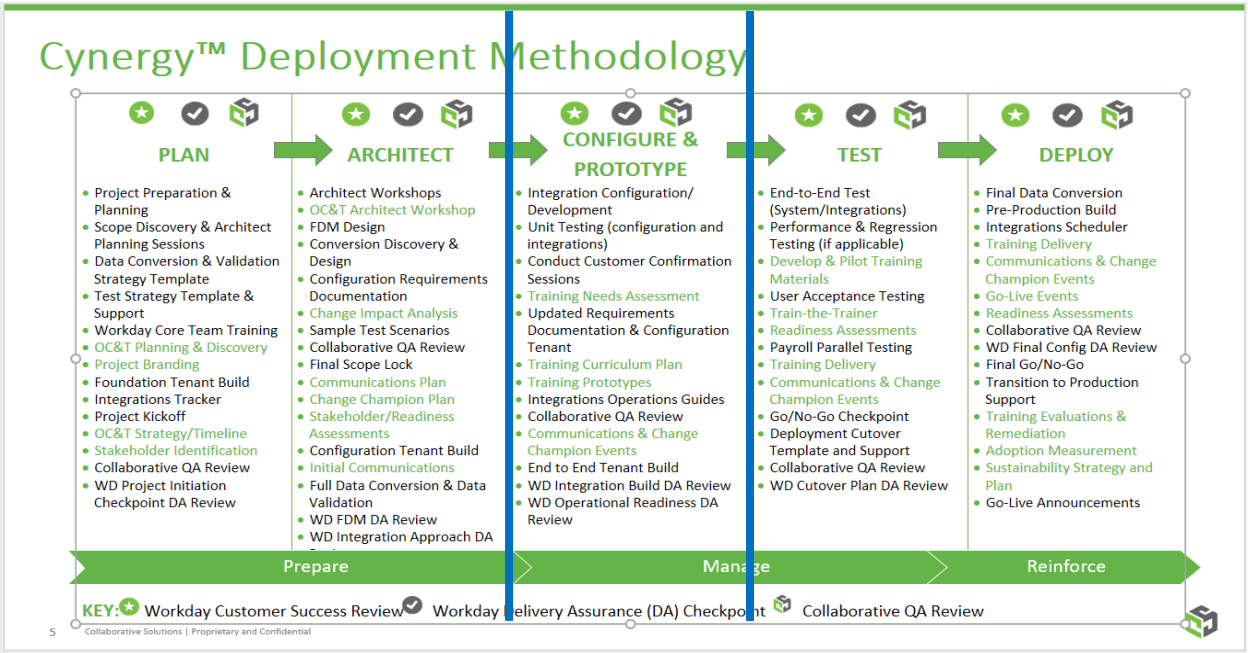

Figure 1 - Implementation Methodology

Sensitive data was uploaded to the WORKDAY® environment without the supervision and approval of a data steward[3]. Without an adequate review of the data security controls, active and retired employees' Personally Identifiable Information (PII), Personally Identifiable Financial Information (PIFI), and driver's license information is at an increased risk of unauthorized access or misuse (see Observation A).

[2] Control Objectives for Information and Related Technologies is a framework for the governance and management of enterprise information and technology.

[3] A data steward is a role that ensures that data governance processes are followed and that guidelines are enforced, as well as recommending improvements to data governance processes.

2. Are configuration documents stored in a repository?

Yes. Configuration documents and Excel spreadsheets are stored on the vendor's SharePoint site (see Figure 2). A central repository allows users real-time access to configuration changes. The site is accessible to the ERP Implementation Team members from both General Government and Gainesville Regional Utilities. Users are authenticated through single sign-on and the connection to the SharePoint site is encrypted.

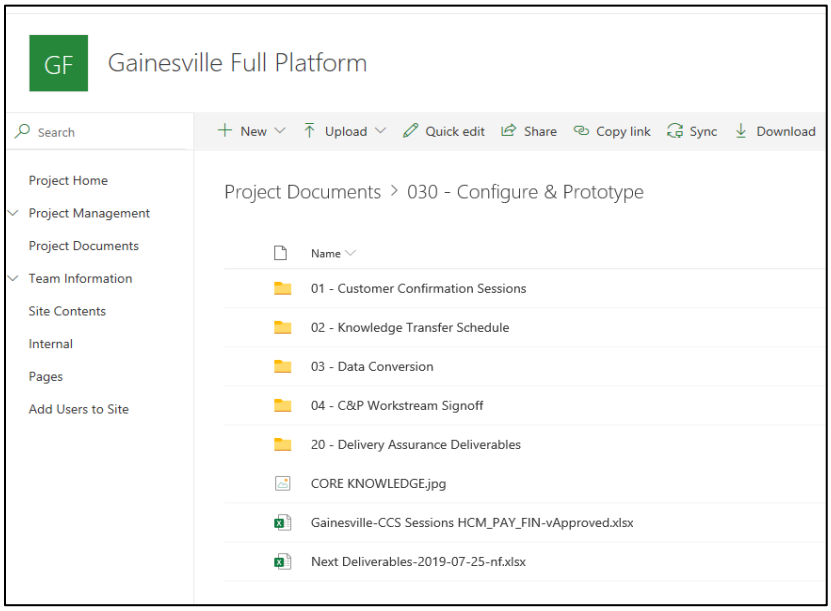

Figure 2 - Configure and Prototype SharePoint Site

We examined the SharePoint user list and identified that three of the 51 active users were either retired or terminated for 48, 71, and 91 days, respectively. Upon our notification, the user accounts were disabled by the vendor.

3. Are reconfigured changes adequately documented and approved?

Generally No. The vendor supplied business units with Excel spreadsheets (workbooks) to store their configuration settings. An examination of the payroll's workbook version history showed that the file was viewed by the Implementer, business unit, and General Government IT Department from July 26, 2019 through October 7, 2019, which aligns with the Configure and Prototype phase. However, the workbook version history does not document what, if any, changes were made to the workbook.

Configuration Settings:

Initially, payroll processes were approved on October 3, 2018, which was six months before the vendor's project timeline start date of April 2019. From August 7, 2019 to August 9, 2019, we attended the payroll customer confirmation sessions and observed that reconfigured workbook changes were verbally approved. On August 13, 2019, the vendor requested configuration sign-off from the payroll business unit. The sign-off was contingent on pushing back criteria not yet completed from the prior confirmation sessions.

The vendor uses multiple mechanisms to track reconfigured changes, which includes a Risks, Actions, Issues, and Decisions (RAID) log for issues and decisions, and a separate data conversion build issue log to track data issues. Currently, 52 of the 210 data conversion build issues were closed by the vendor. In our conversation with the vendor we noted that they were missing a reconfigured item in their tracking systems. Without a single consolidated view, more issues could go missing and affect the success of the implementation (see Observation B).

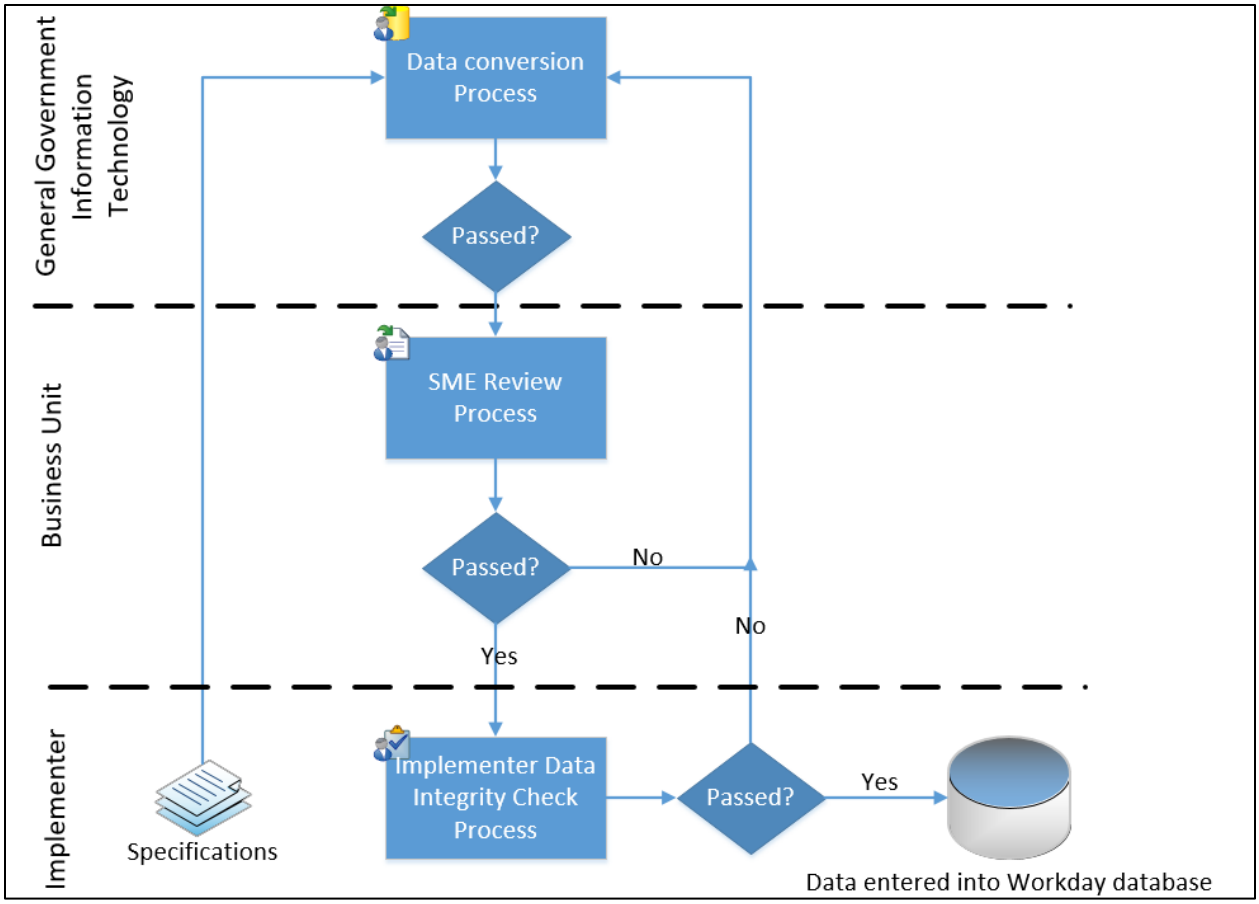

Figure 3 - Data Conversion Approval Flow

Configuration Data:

A snapshot of City employees' data was entered into the WORKDAY® tenant (see Figure 3) at the start of the Configure and Prototype phase. Prior payroll reviews consisted of the payroll business unit spot checking approximately six employees' data for accuracy. In perspective, the City has approximately 2,400 active employees and 2,300 retirees. We also noted instances where incorrect employee data affected the Implementer's payroll unit testing. The lack of comprehensive data reviews increases the risk that inaccurate data is entered into the WORKDAY® database and have an adverse effect on subsequent deployment phases (see Observation C).

4. Are configuration status reports performed?

Generally Yes. There were bi-weekly meetings with project sponsors to update them on project status, which included configuration. However, the accuracy of data was not provided to project sponsors during the configure and prototype phase.

A presentation from the vendor stated the configuration tenant must be developed with "100% data conversion and functional configuration builds, which is imperative to the payroll team's quality and unit testing to keep the project on track and on time". The success of the ERP implementation is dependent on the accuracy of the information in WORKDAY®. The lack of data accuracy reporting may impede the overall success of the ERP implementation (see Observation D).

AUDIT OBSERVATIONS

Internal controls help entities achieve important objectives and sustain and improve performance. The audit observations listed below are offered to help management ensure the successful implementation of the Enterprise Resource Planning application.

Observation A: Increased risk of unauthorized access and misuse of employee data.

Condition:

Active and retired employee data was uploaded and accessible in the WORKDAY® pre-production tenants without the supervision of a data steward.

Cause:

Application access controls such as least privilege and segregation of duties are not enforced in the pre-deployment phases.

Effect:

Employee data may be accessed or disseminated in an unauthorized manner.

Criteria:

National Institute of Standards and Technology (NIST) Special Publication 800-53 Revision 5 Draft *Security and Privacy Controls for Information Systems and Organization's* CM-3(4) Configuration Change Control states a Security Representative should be included in the configuration management team.

Risks:

- Unauthorized access.
- Misuse of data.
- Inappropriate dissemination of employee personally identifiable information.

Recommendation:

1) Data steward should be included in the configuration phase to ensure that employees' personally identifiable information is adequately protected.

Observation B: Consolidate issue tracking mechanisms to reduce the risk of missing configuration changes.

Condition:

A cumbersome reconfiguration process that makes tracking configuration changes difficult to follow.

Cause:

The vendor uses multiple mechanisms to track reconfigured changes.

Effect:

It is difficult for management to determine the status on all reconfigured changes.

Criteria:

COBIT 2019 Build, Acquire, and Implement (BAI) 03.09 Activity 2 Manage changes to requirements states changes to requirements should be tracked, enabling all stakeholders to monitor, review, and approve the changes to ensure that the outcomes of the change process are fully understood and agreed on by all the stakeholders and the sponsor/business process owners.

Risks:

- Changes made without the knowledge of management and/or project sponsors.

Recommendation:

2) Work with the vendor to create a single consolidated view of all configuration changes.

Observation C: Payroll data conversion configuration changes were not adequately reviewed.

Condition:

Payroll data for approximately 2,400 active and 2,300 retired employees from the Advantage CGI system is being converted to the WORKDAY® platform. Approximately six employees' payroll data was reviewed for accuracy.

Cause:

A lack of dedicated resources between Payroll business unit and General Government IT to properly review all of the data.

Effect:

High impact data, such as, incorrect earning/deduction information would increase the risk that payroll data is incorrect and not in compliance with applicable laws and regulations.

Criteria:

National Institute of Standards and Technology (NIST) Special Publication 800-53 Revision 5 Draft *Security and Privacy Controls for Information Systems and Organization's CM-3(2) Configuration Change Control Testing, Validation, and Documentation of Changes* should be completed before fully implementing the changes to the tenant.

Risks:

- Noncompliance with Fair Labor Standards Act (FLSA), U.S. Department of Labor, and Bargaining Agreements.
- Paychecks issued to employee contain incorrect information.

Recommendation:

3) The ERP Implementation Team should continue to work with the business units to ensure that all data conversion information is accurate.

Observation D: The lack of data accuracy reports may impede the overall success of the ERP implementation.

Condition:

The vendor stated that the configuration tenant must be developed with 100% data conversion, which is imperative to the payroll team's quality and unit testing to keep the project on track and on time.

Cause:

Accuracy reports were not performed during the Configure and Prototype phase.

Effect:

Incorrect data will have a negative effect on the overall success of the ERP implementation.

Criteria:

National Institute of Standards and Technology (NIST) Special Publication 800-53 Revision 5 Draft *Security and Privacy Controls for Information Systems and Organization's BAI-10.04 (1) Produce status and configuration reports* that identify status changes of configuration items and report against the baseline.

Risks:

- Data integrity.

Recommendation:

4) Include data accuracy in configuration status reports to management to ensure employee information aligns with project requirements.

GOVERNMENT AUDITING STANDARDS COMPLIANCE

We conducted this audit in accordance with generally accepted government auditing standards and ISACA[4] IS Audit and Assurance Standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our observations and conclusions based on our audit objectives.

AUDIT TEAM

Leonard F. Loria, CPA, Interim City Auditor

Vincent Iovino, CISA, CRISC, Information Technology Auditor

Eileen Marzak, CPA, CFE, Quality Assurance

[4] Previously known as the Information Systems Audit and Control Association, ISACA is an independent, nonprofit, global association that engages in the development, adoption and use of globally accepted industry-leading knowledge and practices for information systems.

APPENDIX A – MANAGEMENT RESPONSE AND CORRECTIVE ACTION PLAN

CITY OF GAINESVILLE

Office of the City Manager

Memo

To: Leonard F. Loria, Interim City Auditor

From: Lee R. Feldman, ICMA-CM, City Manager

Via: Dan Hoffman, Assistant City Manager
Lucian Badea, Director of Technology

Date: November 20, 2019

Re: Management's Response to Audit Report

Please see below response from the Office of the City Manager. Please feel free to contact me directly if you have any questions or you require additional information.

We believe that management is in a unique position to best understand their operations and may be able to identify more innovative and effective approaches, and we encourage them to do so when providing responses to our recommendations.

Recommendation	Concurrence and Corrective Action Plan	Proposed Completion Date
Recommendations for City Management:		
1) Data steward should be included in the configuration phase to ensure that employees' personally identifiable information is adequately protected.	Management concurs. As of Oct 7, 2019, a security lead to the project has been designated. The security lead will ensure access to sensitive data is properly controlled.	Completed
2) Work with the vendor to create a single consolidated view of all configuration changes.	Management concurs. We provided feedback to the vendor and we will be working with them to build a consolidated view of configuration changes	Feb 2020

APPENDIX A – MANAGEMENT RESPONSE AND CORRECTIVE ACTION PLAN

Recommendation	Concurrence and Corrective Action Plan	Proposed Completion Date
3) The ERP Implementation Team should continue to work with the business units to ensure that all data conversion information is accurate.	Management concurs. At every stage of the process, data is formally validated by business owners. We will continue to do so during the implementation process	Completed
4) Include data accuracy in configuration status reports to management to ensure employee information aligns with project requirements.	Management concurs. Configuration, as well as migrated data, is reviewed at every stage by business owners and subject matter experts. We will work with the implementer to see what tools they can provide to support this level of reporting.	Feb 2020

APPENDIX A – MANAGEMENT RESPONSE AND CORRECTIVE ACTION PLAN

We believe that management is in a unique position to best understand their operations and may be able to identify more innovative and effective approaches, and we encourage them to do so when providing responses to our recommendations.

Recommendation	Concurrence and Corrective Action Plan	Proposed Completion Date
Recommendations for City Management:		
1) Data steward should be included in the configuration phase to ensure that employees' personally identifiable information is adequately protected.	Management concurs. As of Oct 7, 2019, a security lead to the project has been designated. The security lead will ensure access to sensitive data is properly controlled.	Completed
2) Work with the vendor to create a single consolidated view of all configuration changes.	Management concurs. We provided feedback to the vendor and we will be working with them to build a consolidated view of configuration changes	Feb 2020
3) The ERP Implementation Team should continue to work with the business units to ensure that all data conversion information is accurate.	Management concurs. At every stage of the process, data is formally validated by business owners. We will continue to do so during the implementation process	Completed
4) Include data accuracy in configuration status reports to management to ensure employee information aligns with project requirements.	Management concurs. Configuration, as well as migrated data, is reviewed at every stage by business owners and subject matter experts. We will work with the implementer to see what tools they can provide to report this level of reporting.	Feb 2020