Review of Roles Based Access in ERP

Office of the City Auditor

Executive Summary

Why we did this project

- The City of Tulsa has recently implemented the core financials module of a new Enterprise Resource Planning (ERP) financial system. ERPs integrate management of core business processes using real time data collection, storage and reporting. While the ERP delivers opportunities to increase efficiencies for the City's financial functions, automating these processes alters financial workflow and duties. Segregation of duties in an ERP system is a needed internal control established to reduce the potential for errors and fraud initiated by one party without the detection or approval of management and other system users. This project reviewed key aspects of segregation in functional and individual roles of the ERP's core financials module in Accounts Payable, General Ledger, Purchasing, Employee Reimbursement, and Accounts Receivable functions.

- Roles now control access and task permissions in the ERP; this differs from the previous system's user based access. While this is the most efficient process to manage permissions, this increases the risk that conflicting permissions may be overlooked, which could eliminate or reduce segregation of duties. To mitigate the risk of assigning conflicting permissions, Internal Auditing performed a review of the role based accesses for both the individual roles and individual users' combination of assigned permissions. This review helps strengthen assurance that the major conflicting tasks (detailed at Appendix II) are avoided.

How we did this project

Internal Auditing created an Audit Command Language (ACL) script, which is a series of automated instructions, to analyze segregation in the ERP system. This script can be repeated by the Finance department, and can be used to monitor potential conflicts on an ongoing basis. (Details of the script are included for reference at Appendix I).

To develop the script, the Information Systems Audit and Control Association's (ISACA) *List of Conflicting Tasks That Pose a High Risk* was used as the benchmark and compared to the ERP's task permissions. The City Controller and ERP functional area team leaders then helped create a key table to establish the ERP tasks which were equivalent to the ISACA listing.

Using the key table, the **individual role** ERP tasks were compared to high risk ISACA task conflicts. Any ERP roles identified at high risk for conflict were captured by the ACL script and exported to an Excel-based report for the Controller's review.

Additionally, the combination of roles assigned to a **single user** was reviewed to determine whether an ISACA high segregation risk existed due to the multiple roles assigned to various users. These potential user segregation risks were also captured by the ACL script and exported to an Excel-based report for the Controller's review.

Project Results

The ACL script review showed 35 roles had been created which posed potential segregation of duties conflicts; 23 of these roles were assigned to users, and 12 of these roles did not have active, assigned users at the time of our review.

There were an additional 27 roles which did not have inherent segregation issues, but which posed apparent segregation conflicts based on the combination of roles assigned to a user.

We also noted three roles were created for 88 'super users' which granted wide access across the various ERP permissions for training purposes; these were slated to be removed when the City officially went 'live' at the December 11, 2017 ERP implementation.

Next Steps

The Controller and ERP functional area leads agreed to review the role and user segregation of duties conflicts identified by the ACL script, and then used the script to make changes deemed necessary prior to ERP system implementation (which occurred in December 2017).

Recommendation

As an ongoing best practice, the Controller should periodically run this ACL script for both roles and users to review for potential segregation conflicts. When new modules go live or the ERP system adds new permission functions, additional review and ISACA categorization of these new permissions and roles should be appended to the key conflicting tasks table.

Appendix I

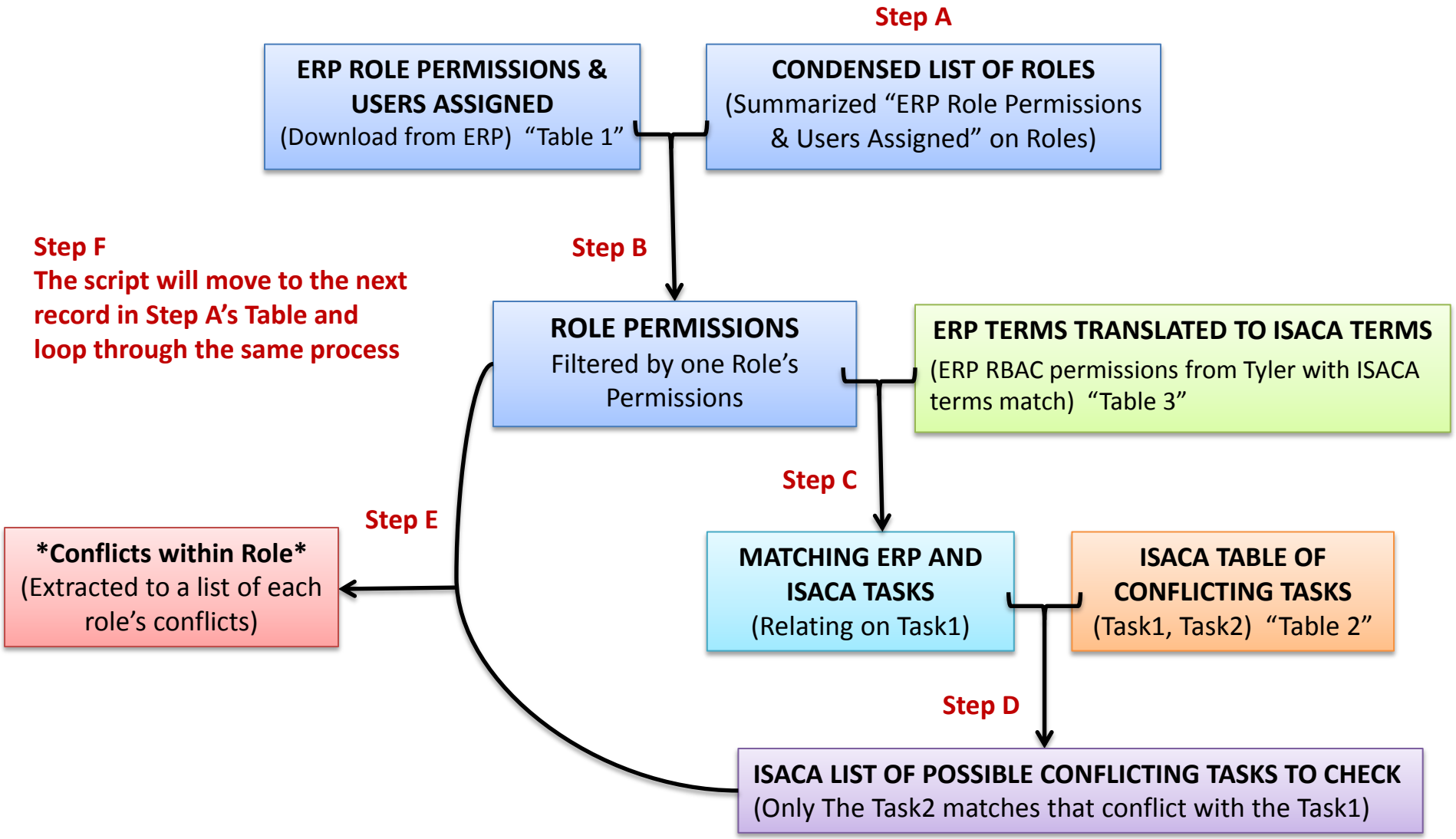
ACL Script Summary:

I. Import Tables:
   1) ERP download of all roles and users assigned
   2) Information Systems Audit and Control Association's high risk separation of duties conflicting tasks
   3) List of ERP terms matched to ISACA terms with the City Controller and the functional area leads.

II. Script Analysis:
   - By Role: (See Flowchart 1, following pages)
     A. Create a condensed list of roles
     B. Filter the ERP download of roles (Import Table 1) for only the first role from the created condensed list.
     C. Find their ERP equivalent term if they have one from the list of ERP terms to matched to ISACA terms (Import Table 3)
     D. Take these matched permissions' ERP terms and relate the ISACA table of conflicting tasks (Import Table 2) to find the tasks that conflict with the matched permissions.
     E. Use the list of tasks that conflict with the permissions and relate this back to the original ERP download of roles (Import Table 1) to see if there are matches. This identifies if a conflict exists and exports and appends to an excel table.
     F. The script will loop through to the next role in the created condensed list of roles and repeat the analysis until the end of the list of roles.
   - By Person: (See Flowchart 2, following pages)
     A. Create a condensed list of users
     B. Create a list of all the roles with their assigned users and filter for the first user
     C. Filter the ERP download of roles (Import Table 1) for the first person's list of roles assigned from the created condensed list filtered for their roles.
     D. Find their ERP equivalent term if they have one from the list of ERP terms to matched to ISACA terms (Import Table 3)
     E. Take these matched permissions' ERP terms and relate the ISACA table of conflicting tasks (Import Table 2) to find the tasks that conflict with the matched permissions.
     F. Use the list of tasks that conflict with the permissions and relate this back to the original ERP download of roles to see if there are matches. This identifies if a conflict exists and exports and appends to an excel table.
     G. The script will loop through to the next person in the created condensed list of users and repeat the analysis until the end of the list of users.

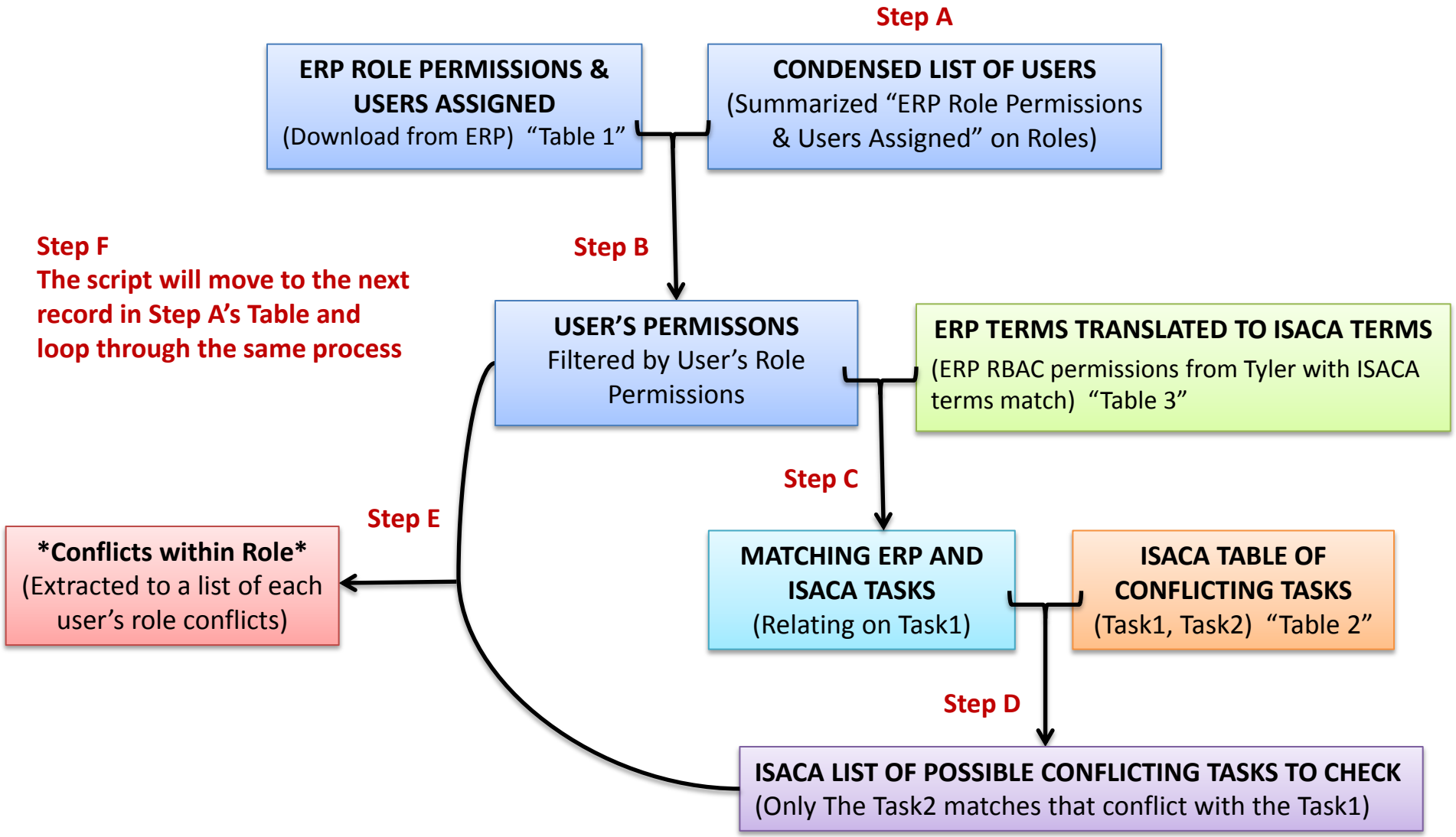
Flowchart 1

Flowchart for ACL Separation of Duties Script By Role



Flowchart 2

Flowchart for ACL Separation of Duties Script By User



Appendix II

List of Conflicting Tasks for Core Financials

(Source: Best Practices to Resolve Segregation of Duties Conflicts - ISACA)

Task 1	Task 2	Description of Risk
Maintain Asset Document	Process Vendor Invoices	Pay an invoice and hide it in an asset that would be depreciated over time.
Maintain Asset Document	Goods Receipts to PO	Create an invoice through ERS goods receipt and hide it in an asset that would be depreciated over time.
Cash Application	Bank Reconciliation	Allows differences between cash deposited and cash collections posted to be covered up
Maintain Asset Master	Goods Receipts to PO	Create the asset and manipulate the receipt of the associated asset.
Maintain Bank Master Data	Cash Application	Maintain a non bona-fide bank account and divert incoming payments to it.
Vendor Master Maintenance	Process Vendor Invoices	Maintain a fictitious vendor and enter a Vendor invoice for automatic payment
Maintain Purchase Order	Process Vendor Invoices	Purchase unauthorized items and initiate payment by invoicing
Maintain Purchase Order	Goods Receipts to PO	Enter fictitious purchase orders for personal use and accept the goods through goods receipt
Process Vendor Invoices	Goods Receipts to PO	Enter fictitious vendor invoices and accept the goods via goods receipt
Vendor Master Maintenance	Maintain Purchase Order	Create a fictitious vendor and initiate purchases to that vendor
Bank Reconciliation	Process Vendor Invoices	Can hide differences between bank payments & posted AP records
PO Approval	Goods Receipts to PO	Approve the purchase of unauthorized goods and hide the misuse of inventory by not fully receiving the order
PO Approval	Process Vendor Invoices	Release a non bona-fide purchase order and initiate payment for the order by entering invoices
PO Approval	Vendor Master Maintenance	Create a fictitious vendor or change existing vendor master data and approve purchases to this vendor
Vendor Master Maintenance	Purchasing Agreements	Risk of entry of fictitious Purchasing Agreements and the entry of fictitious Vendor or modification of existing Vendor especially account data.
Purchasing Agreements	Goods Receipts to PO	Modify purchasing agreements and then receive goods for fraudulent purposes.

This is a condensed list of the conflicting task pairs that was identified as applicable to ERP core financial modules. Additional conflicting tasks pairs from ISACA's full list may be applicable when the City implements additional ERP modules and/or expands existing permissions in the future.

List of Conflicting Tasks for Core Financials

(Source: Best Practices to Resolve Segregation of Duties Conflicts - ISACA)

Task 1	Task 2	Description of Risk
Process Vendor Invoices	Purchasing Agreements	Enter unauthorized items to a purchasing agreement and create an invoice to obtain those items for personal use
Maintain Purchase Order	PO Approval	Where release strategies are utilized, the same user should not maintain the purchase order and release or approve it.
Cash Application	Maintain Billing Documents	Create a billing document for a customer and inappropriately post a payment from the same customer to conceal non-payment.
Maintain Customer Master Data	AR Payments	Create a fictitious customer and initiate payment to the unauthorized customer.
Process Customer Credit Memos	AR Payments	Initiate an unauthorized payment to the customer by entering fictitious credit memos.
Cash Application	Maintain Customer Master Data	Risk of the same person entering changes to the Customer Master file and modifying the Cash Received for the customer.
Maintain Customer Master Data	Maintain Billing Documents	User can create a fictitious customer and then issue invoices to the customer.
Process CRM Sales Order	Maintain Billing Documents	Inappropriately create or change sales documents and generate the corresponding billing document in R3.

This is a condensed list of the conflicting task pairs that was identified as applicable to ERP core financial modules. Additional conflicting tasks pairs from ISACA's full list may be applicable when the City implements additional ERP modules and/or expands existing permissions in the future.