## BACKGROUND/INTRODUCTION

Segregation of duties is a key internal control, and one of the most difficult to achieve. In practice, it means no individual has control over two or more phases of a transaction or operation. Segregation provides two benefits. It is much more likely to find errors, and a deliberate fraud is more difficult to commit because it requires collusion of two or more persons.

**Previous external *and* internal audits identified segregation weaknesses for Accounts Payable-related processes and tasks.** Finance management plans to remediate these by configuring segregation into the under-development Workday software Finance module. Finance management also requested Auditor consultation on Workday's segregation structure, which led to this project.

## EXECUTIVE SUMMARY

Workday is designed to leverage ***roles and business processes*** to establish segregation. Workday ***also grants access and action privileges through membership in security groups, domain level access, and default security settings. 'Custom' modifications to any of these areas can also change segregation profiles*.** Management is currently testing the roles and business processes in the end-to-end testing for phase 3 Finance implementation. Security will need to continue to be reviewed with plans to analyze additional segregation layers **after** system implementation in 2024.

To provide support for future segregation evaluation, Audit shared detail analysis with Finance management. **This analysis noted potential risks within security groups for August 2023 *development-phase data* for key Finance roles**. This *data structure will change throughout the remaining development, testing and early implementation phases, and Audit's segregation information is for management's consideration and guidance in those phases.* Additionally, Audit suggests management consider these factors when future segregation analysis is conducted**:**

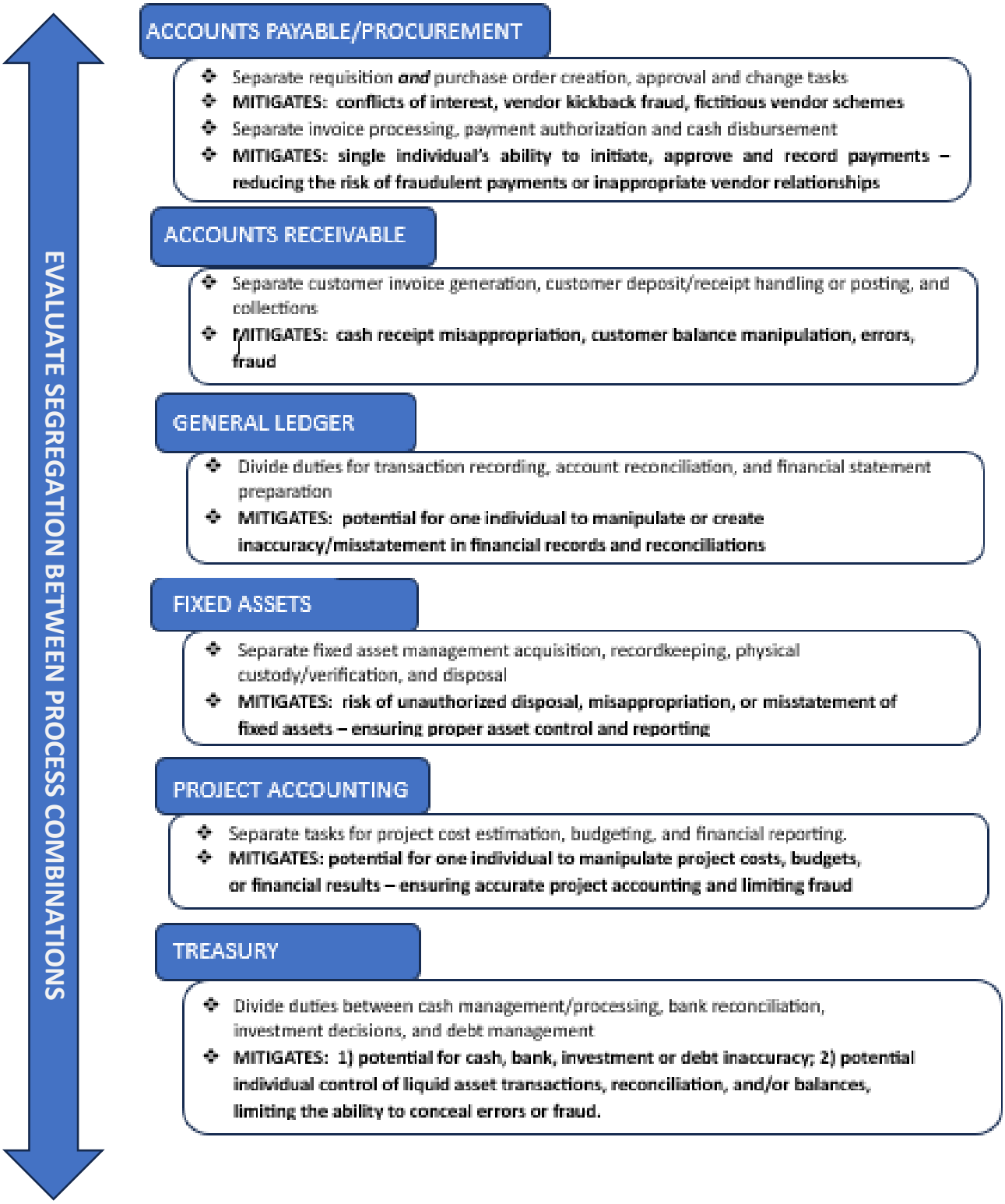
- **the *added levels* of potential risk exposure** which *group and domain privileges may create by allowing **additional, potentially unknown access/actions beyond those granted by user roles***
- **the risks *combinations* of roles/processes/group privileges may create** by allowing *a* single user to access/perform actions ***in multiple processes/functional areas***
- **the *earliest feasible timing* for full segregation analysis**, *due to the potential for process and/or structure changes* which may trigger additional work beyond the term of the system consulting contract, which could trigger additional cost
- **the potential for unmitigated segregation risk** to lead to an external audit **significant deficiency or material weakness finding**
- **the potential to use *compensating/mitigating controls to reduce segregation risk;*** these controls may *help **avoid the need for extensive Workday changes and their potential for related cost***

For management's additional reference, information on process and task segregation is at **page 2**. An illustration of Workday's security control structure is **at page 3**. Information on compensating/mitigating controls is at **page 4**. Management's responses are at **page 5.** This project's scope is at **Appendix I, page 6**.

The Auditor appreciates the time, assistance and expertise provided to this project by the Finance, Accounting, Workday Implementation, and Information Technology teams.

## EXAMPLES OF PROCESSES/TASKS TO SEGREGATE – for management's consideration

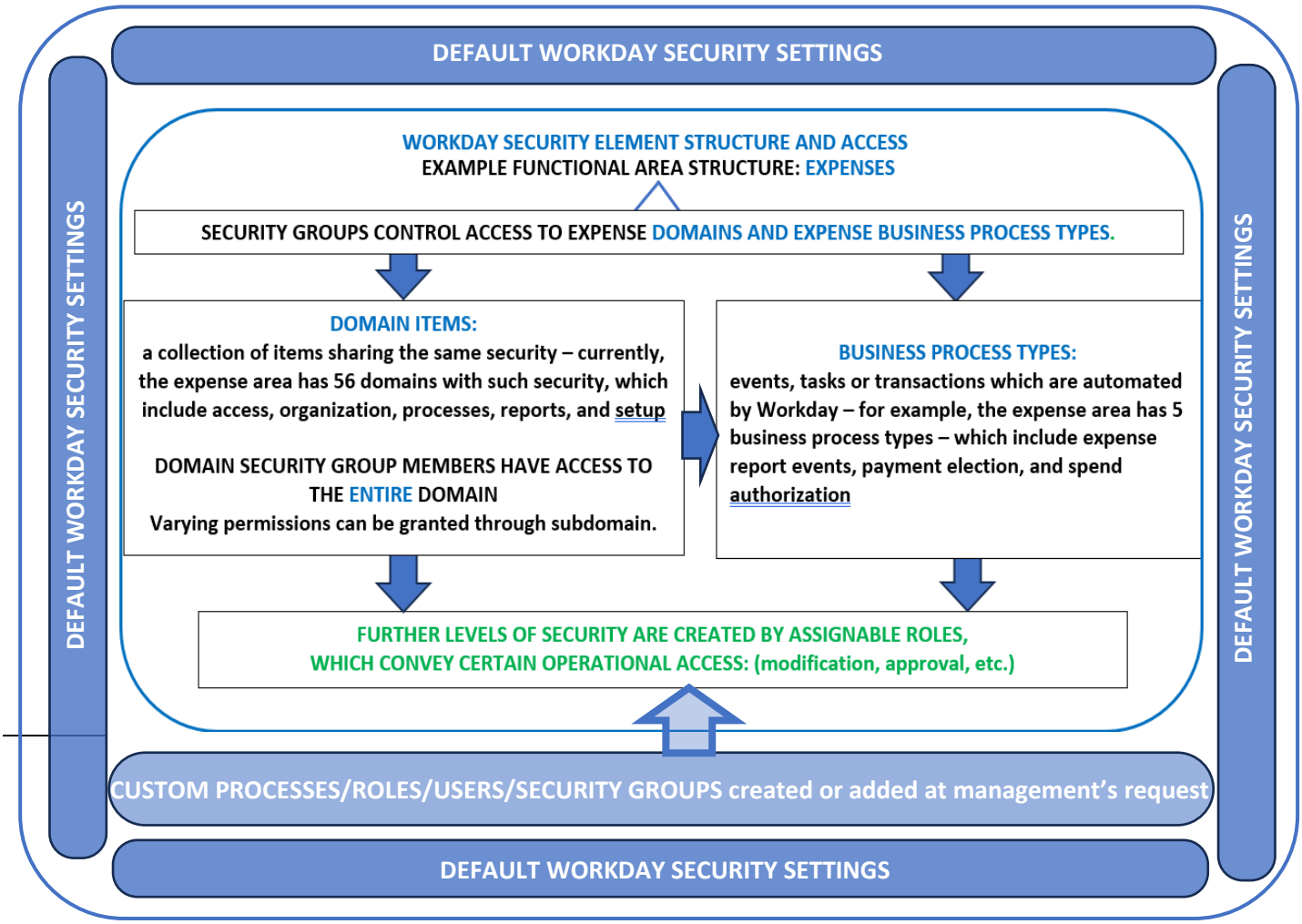
**The below tasks *within functions* should optimally be segregated. Management should *also consider limiting combinations of roles across processes and controls* – for example, separating accounts payable and receivable tasks from treasury functions, to prevent errors or manipulation of payments and receipts from being concealed in bank records/controls**



## WORKDAY SOFTWARE SECURITY STRUCTURE

The segregation control structure of Workday is embedded in separate areas *which intersect*. Workday comes with ***built in 'default' privileges, and also allows management to create additional 'custom' privileges***. All privileges exist in **security groups, domains, processes, roles, and user privileges**. These areas can overlap and may weaken segregation in ways that are difficult to identify; these overlaps are often referred to as 'toxic combinations' of access. Due to this complexity, **in depth analysis is frequently conducted to analyze Workday system segregation. Finance management plans to continue to conduct segregation analysis after implementation**. The below graphic is based on August 2023 Workday development Expense domain and business process information, and is provided to further illustrate these concepts.

### WORKDAY SECURITY OVERVIEW




- **IF A USER IS GRANTED ACCESS IN A SECURITY GROUP, IT CAN BE GRANTED AT *EITHER* THE DOMAIN *OR* THE BUSINESS PROCESS LEVEL.**
  - **DOMAIN LEVEL SCURITY GROUP ACCESS IS BROAD - it sets up *the same security profile for all items in a domain.* These can include access privileges, processes, reports, and the ability to setup processes. This *allows all domain members to have the same security privileges…. unless limited by a subdomain.***
- **DEFAULT SETTINGS AND ROLES *ARE THE FOUNDATION OF WORKDAY SECURITY, BUT***
- ***ANY ADDED CUSTOM CHANGES TO SECURITY GROUPS, DOMAINS, PROCESSES OR ROLES CAN EXPAND, LIMIT OR CONFLICT WITH WORKDAY DEFAULT SECURITY SETTINGS***
- ***SPECIFIC USER* (RATHER THAN ROLE) ACCESSES CAN BE GRANTED, *WHICH MAY ALSO CAUSE ACCESS CONFLICTS***

## CONTROLS *NOT* REQUIRING SEGREGATION – COMPENSATING AND MITIGATING CONTROLS

It's significant to consider that any gaps identified by management's upcoming segregation analysis may be addressed with multiple approaches**. Division of *all* tasks, processes, and access is usually not a practical response to segregation weaknesses, because such an approach would likely require staff levels beyond feasible budget limits. In those instances where duties cannot be fully segregated**, **mitigating or compensating controls should be evaluated and implemented where possible.** Below is summary 'high-level' information for management's consideration and reference as these types of controls are considered.

- **Compensating controls are *procedures or tasks added* when desired/optimal controls aren't feasible due to staffing, cost or system limitations.** For instance, if personnel recording transactions also perform a reconciliation process, a detailed independent review of the reconciliation could be performed and documented by a supervisor to provide additional control over incompatible functions. **Effective compensating controls should**:
  - Meet the intent of the original segregation control
  - Provide a similar level of assurance
  - Go beyond the original segregation control requirement

  For example, the above-mentioned reconciliation review would:
  - Meet the intent of ensuring bank account recordkeeping and reconciliation are accurate, timely and complete
  - Prove a similar level of assurance through reconciliation **review by an employee *separate*** from both transaction and reconciliation functions, preferably in supervisory role
  - Go beyond the segregation control gap, by including **independent, detailed verification of reconciliation** activity such as verifying the bank statement's balance, cash account balance, and the nature and resolution of any unusual or old reconciling items

- **Mitigating controls are *designed to reduce the risk* that *errors or irregularities can occur.*** An example would be relying on assurance provided by *actions performed in an earlier* phase of a process to *limit the depth/scope of review performed in later steps.*

The Auditor is available to discuss control structure, information and options with management, and encourages continued dialogue on control topics as the Workday system is implemented and refined.

## MANAGEMENT RESPONSE

Olathe Phase 3 Workday leads in conjunction with Olathe PMO and our AVAAP consultants completed ten weeks of end-to-end testing with Workday security roles assigned to testers. Over 230 scenarios with 1838 steps were tested over this time frame. These tests included negative testing for potential errors/process fails, and validation of controls (including approvals, thresholds, the inability to approve items that a tester entered even when authorized to approve). Significant work led by the Olathe Project Management Office and AVAAP Workday consultants was completed to test through a custom role to allow for view access of financial data in reports. Management believes this demonstrates the security of information in Workday is much more robust than what was available in the E1 legacy system. Prior to Workday 'go live', Security Access assignments will be reviewed and approved by the Executive team or designees to ensure appropriate access across the City.

**APPENDIX I**
**PROJECT SCOPE**

This project provided a limited review *of potential development phase segregation risks in the July – August 2023 timeframe*. Due to the development phase of the Workday Finance module in this timeframe, configurations reviewed are *preliminary, and may change as management further tests, evaluates and evolves the structure of Workday prior to planned January 2024 implementation.*

- **Workday tasks and privileges established by significant/higher risk roles were reviewed for 8 key Accounting/Finance personnel by:**
  - Judgmentally *selecting key personnel*
  - *Obtaining the security groups* which these personnel had membership in
  - *Selecting the significant 'assignable' roles within these security groups*
  - *Analyzing these key user significant roles* for the following capabilities, and potential segregation conflicts they may pose :
    - transaction initiation
    - transaction & process review and/or approval
    - transaction execution and/or recording
    - task and/or process setup, change and access privileges
    - security group membership and related accesses/privileges
    - access to integrations from/to other systems which can be used to change or add to Workday data (known as 'put' capability), and
    - transaction activity balancing/reconciliation

- **Audit provided details of this analysis to management** for reference in their upcoming segregation review efforts and Accounts Payable action plan development. This information also provides the requested Audit control consultation information. The data shared with management is viewed as a **starting point for their consideration in evaluating *potential* segregation gaps – *it is not considered by the Auditor to be substantive 'proof' of such gaps.***

- **Overall potential segregation risks and factors** were noted while performing the specific segregation procedures, and are ***listed in the Executive Summary of this report*.**