Access Control

PeopleSoft

Audit Report # 19-100

August 29, 2019

The University of Texas at El Paso

Office of Auditing and Consulting

"Committed to Service, Independence and Quality"

The University of Texas at El Paso
Office of Auditing and Consulting Services

500 West University Ave.
El Paso, Texas 79968
915-747-5191
WWW.UTEP.EDU

August 29, 2019

Dr. Heather Wilson
President, The University of Texas at El Paso
Administration Building, Suite 500
El Paso, Texas 79968

Dear Dr. Wilson:

The Office of Auditing and Consulting Services has completed a limited scope audit of Access Control-PeopleSoft. During the audit, we identified opportunities for improvement and offered the corresponding recommendations in the audit report. The recommendations are intended to assist the departments in strengthening controls and help ensure that the University's mission, goals and objectives are achieved.

We appreciate the cooperation and assistance provided by: Office of Research and Sponsored Projects (including Contracts and Grants Accounting), Enterprise Computing, System Integration (PeopleSoft), Accounts Payable, and Accounting and Financial Reporting during our audit.

Sincerely,

Lori Wertz

Lori Wertz
Chief Audit Executive

Report Distribution:

University of Texas at El Paso:
Mr. Richard Adauto III, Executive Vice President
Dr. Roberto Osegueda, Vice President Research
Ms. Guadalupe Gomez, Director, Contracts and Grants Accounting
Dr. Stephen Riter, Vice President Information Resources
Ms. Iris R. Niestas, Assistant Vice President, PeopleSoft
Mr. Luis Hernandez, Assistant Vice President and Director, Enterprise Computing
Ms. Mary Solis, Director and Chief Compliance and Ethics Officer

University of Texas System (UT System):
System Audit Office

External:
Governor's Office of Budget, Planning and Policy
Legislative Budget Board
Internal Audit Coordinator, State Auditor's Office
Sunset Advisory Commission

Audit Committee Members:
Mr. Joe R. Saucedo
Mr. Fernando Ortega
Dr. Gary Edens
Mr. Benjamin Gonzalez
Mr. Mark McGurk
Dr. John Wiebe

Auditors Assigned to the Audit:
Victoria Morrison
Luis Carrera

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The Office of Auditing and Consulting Services has completed a limited scope audit of Access Control-PeopleSoft for individuals under the Office of Research and Sponsored Projects organizational chart in Appendix A: ORSP Organizational Chart. PeopleSoft is the University of Texas at El Paso's (UTEP) Enterprise Resource Planning (ERP) software used for Finance and Human Resources systems.

During the audit, we noted the following:

- PeopleSoft user(s) have greater access than is required to perform their job duties.
- Access was granted to a PeopleSoft security role without approval from an authorized approver.
- PeopleSoft user(s) have access to multiple security roles causing possible segregation of duties (SOD) conflicts.

We also performed a review of SOD conflicts at the most granular security level (page level). Although SOD conflicts existed in the PeopleSoft Finance system, mitigating controls were in place and operating effectively to reduce the risk of an employee perpetrating and concealing an unauthorized activity without collusion with another person.

BACKGROUND

In May of 2014, the University of Texas at El Paso (UTEP) along with other UT System institutions converted to a shared instance of PeopleSoft Enterprise Resource Planning (ERP) software for their Finance and Human Resources systems. PeopleSoft is hosted and maintained at the UT System "Shared Information Services" Department (UTSIS).

PeopleSoft security architecture is set up with multiple levels of security. UTSIS security, in partnership with functional committees (i.e. subject matter experts) from the institutions, developed PeopleSoft's user security, based on the needs of the institutions. User security is controlled through permission lists and roles.

Each UT System institution has an Information Security Administrator (ISA), who performs PeopleSoft access control processes (i.e. granting access after it has been approved, etc.), but cannot modify and/or create security roles. The responsibility for modifying and/or creating security roles rests with UTSIS Security.

Due to the complexity of the PeopleSoft security architecture, it is possible for users to be granted access to security roles aligned with their job responsibilities, but when paired with another security role, it may cause segregation of duties (SOD) conflicts (i.e. creating and approving a journal entry). Mitigating controls exist, such as PeopleSoft approval workflow and user preferences, to minimize the risk of SOD conflicts.

In addition, depending on the security role and the functional area, some of the security roles may grant users access more elevated than others (i.e. access to various processes). This may cause users to have more access than necessary to perform their job responsibilities.

Since PeopleSoft went live, the Office of Auditing and Consulting Services has not conducted an access control audit specifically related to PeopleSoft. Therefore, this audit will focus on segregation of duties conflicts and access to elevated access security roles.

AUDIT OBJECTIVES

The objective of this audit was to determine if PeopleSoft access is properly segregated, elevated access privileges are limited and controlled and access is approved and reviewed.

SCOPE AND METHODOLOGY

The scope of the audit covers PeopleSoft access privileges from April 30, 2018 to April 29, 2019, and is limited to individuals under the Office of Research and Sponsored Projects (ORSP) organizational chart in Appendix A: ORSP Organizational Chart.

The audit was conducted in accordance with the *International Standards for the Professional Practice of Internal Auditing* and the authoritative guidelines of the *International Professional Practice Framework* issued by the Institute of Internal Auditors.

The criteria for the audit included (See Appendix B: Criteria):

- Texas Department of Information Resources (DIR) *Security Control Standards Catalog Version 1.3*
- UT System Policy (UTS 165) Information Resources Use and Security Policy
- UTEP Information Resources Use and Security Policy

Audit procedures included:

- interviewing and requesting information from key personnel
- reviewing applicable laws, regulations, policies and procedures
- running queries on PeopleSoft to extract data
- testing data using data analytics software
- limited testing, where appropriate

RANKING CRITERIA

All findings in this report are ranked based on an assessment of applicable qualitative, operational control and quantitative risk factors, as well as the probability of a negative outcome occurring if the risk is not adequately mitigated. The criteria for the rankings are as follows:

Priority - an issue identified by an internal audit that, if not addressed timely, could directly impact achievement of a strategic or important operational objective of a UT institution or the UT System as a whole.

High – A finding identified by internal audit that is considered to have a medium to high probability of adverse effects to the UT institution either as a whole or to a significant college/school/unit level.

Medium – A finding identified by internal audit that is considered to have a low to medium probability of adverse effects to the UT institution either as a whole or to a college/school/unit level.

Low – A finding identified by internal audit that is considered to have minimal probability of adverse effects to the UT institution either as a whole or to a college/school/unit level.

AUDIT RESULTS

A. Elevated Access Granted in PeopleSoft

A.1. PeopleSoft user(s) have greater access than required to perform job duties

Staff members from the ORSP IT and Research functions have greater PeopleSoft access than required to perform their job duties.

a) ORSP IT function: Four (4) staff members have access to security roles with the ability to create/change transactions; their job duties only require read-only access to retrieve data from PeopleSoft.

b) ORSP Research function: Staff members have access to security roles previously granted on a temporary basis, but never removed.

   a. Three (3) staff members have access to three (3) security roles with elevated access.
   b. Four (4) staff members have access to two (2) front-office security roles (limited access).

Policies and Standards require reviewing, removing, and/or disabling accounts to reflect current user needs or changes to user roles or employment status. In addition, access must be based on an employee's "need to know" as established by their official duties.

Recommendation:

In partnership with System Integration (PeopleSoft) and Enterprise Computing Departments, ORSP should:

- *Use the principle of least privilege and remove/modify access not required to perform a users' job duties.*
- *Where needed, replace current access with read-only access, allowing ORSP IT and Research function staff members to continue performing their job duties.*
- *Perform a periodic review of PeopleSoft access to verify if access is adequate. User accounts access privileges should be updated to reflect current user needs and/or changes due to user roles or employment status.*

Level: This finding is considered **HIGH** because having greater access than required to perform job duties could lead to intentional or unintentional changes to transactions. Without proper oversight, these transactions could go undetected for extended periods.

Management Response:

The security roles for the four individuals will be modified to the module read-only roles and we will remove any roles no longer needed.

Responsible Party:

Iris Niestas, Assistant Vice President, System Integration.

Implementation Date:

September 13, 2019

A.2. Access was granted to a PeopleSoft security role without approval from an authorized approver

One of 11 user accounts tested from a population of 26 was missing approval support from an authorized approver (i.e. subject matter expert). A PeopleSoft request form, which automatically routes an access approval request to the authorized approver, was not used.

Policies and Standards state access to an information resource may not be granted by another user without the permission of the Owner or the Owner's delegated custodian of the information resource.

Recommendation:

Access to PeopleSoft security roles should only be granted after approval has been received from authorized approver(s). The use of PeopleSoft request forms reduces the risk of unauthorized access being granted, as request for access approvals are automatically routed to authorized approvers.

Level: This finding is considered **HIGH** because access was granted to a security role without approval from an authorized approver, increasing the risk of unauthorized changes to information resources.

Management Response:

The Project Costing module is owned by both the General Ledger team (approver – Laura Gutierrez) and the Contracts and Grants team (approver – Lupe Gomez). We should update our owner list and conduct a periodic review to ensure we have the correct approver list.

In addition, we should try to use the backoffice access request form consistently for changes to security role assignments.

Responsible Party:

Iris Niestas, Assistant Vice President, System Integration.

Implementation Date:

September 30, 2019

A.3. PeopleSoft user(s) have access to multiple security roles, causing possible segregation of duties conflicts

Eighteen (18) Contracts and Grants Accounting staff members including an Accounting Specialist II, Accountants I/II/III, an Assistant Manager, Managers, and a Director have access to up to 11 PeopleSoft security roles with elevated access (depending on the user). When taken separately, the roles might not represent a risk, but when combined, they might cause possible SOD conflicts.

These roles give users access to:

- Grants Management Module - accounts receivable activities; billing; setup ability for contracts, grants, and sponsored projects
- Review and update vendor data
- Post vouchers and payments, and create manual payments
- Capital projects accounts receivable activities

Policies and standards state the lack of segregation of duties may result in unauthorized or unintentional modification or misuse of the organization's information assets. In addition, access must be based on an employee's "need to know" as established by their official duties.

Recommendation:

In partnership with the System Integration (PeopleSoft) and Enterprise Computing Departments, Contracts and Grants Accounting should:

- *Identify the job duties of Contracts and Grants Accounting staff members and map them to the necessary PeopleSoft security roles. Only those security roles required to perform their job duties should be granted. Minimizing the risk of possible SOD conflicts should also be part of this process.*
- *Where needed, replace current access to read-only access, allowing Contracts and Grants Accounting staff members to continue performing their job duties.*

Level: This finding is considered **HIGH** because unauthorized or unintentional modification or misuse of the University's information assets could occur. Without proper oversight, these transactions could go undetected for extended periods.

Management Response:

We will work with the Contracts and Grants team to determine the level of access required in order to identify security role changes that can be made without impacting their ability to perform daily job duties.

Responsible Party:

Iris Niestas, Assistant Vice President, System Integration.

Implementation Date:

December 13, 2019

B. Segregation of Duties (SOD) in PeopleSoft

B.1. Identified SOD conflicts are mitigated by controls in place

SOD refers to the practice of dividing responsibilities between different staff members so that no single individual can control a transaction from beginning to end, increasing the risk of unauthorized activity going undetected.

We identified SOD conflicts within the PeopleSoft Finance system. Mitigating controls in place, such as the PeopleSoft approval workflow and user preferences, are operating effectively to reduce the risk of an employee perpetrating and concealing an unauthorized activity without collusion with another person.

CONCLUSION

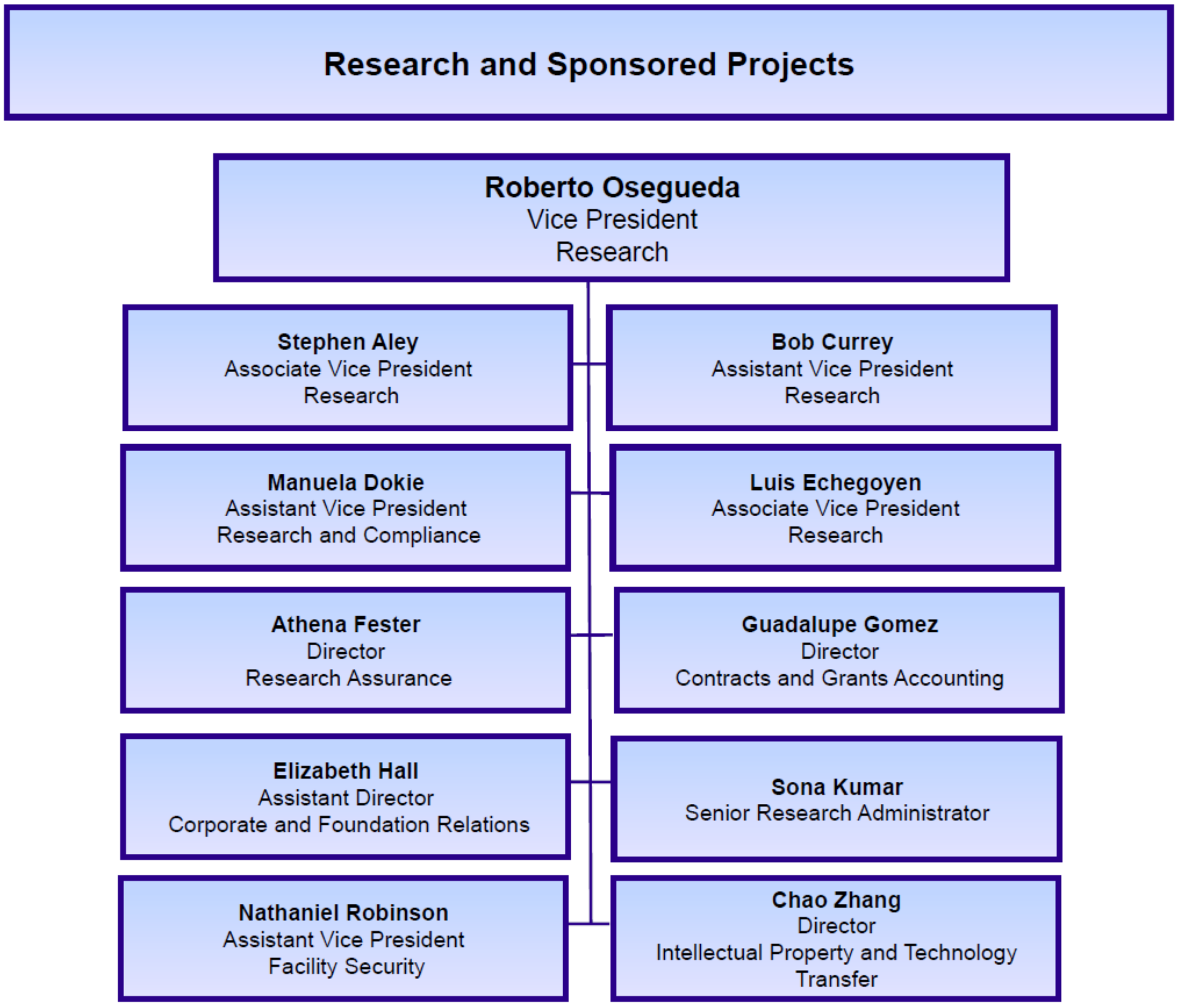
Based on the results of audit procedures performed, we conclude the Office of Research and Sponsored Projects can strengthen existing access controls by implementing the recommendations detailed in this report.

We wish to thank the management and staff of the Office of Research and Sponsored Projects (including Contracts and Grants Accounting), Enterprise Computing, System Integration (PeopleSoft), Accounts Payable, and Accounting and Financial Reporting for their assistance and cooperation provided throughout the audit.

APPENDIX A: ORSP ORGANIZATIONAL CHART

Office of Research and Sponsored Projects Organizational Chart

Reference: UTEP website, About > Organizational Charts > Research and Sponsored Projects


Research and Sponsored Projects
Roberto Osegueda Vice President Research
Stephen Aley Associate Vice President Research
Bob Currey Assistant Vice President Research
Manuela Dokie Assistant Vice President Research and Compliance
Luis Echegoyen Associate Vice President Research
Athena Fester Director Research Assurance
Guadalupe Gomez Director Contracts and Grants Accounting
Elizabeth Hall Assistant Director Corporate and Foundation Relations
Sona Kumar Senior Research Administrator
Nathaniel Robinson Assistant Vice President Facility Security
Chao Zhang Director Intellectual Property and Technology Transfer

Return *EXECUTIVE SUMMARY*
Return *SCOPE AND METHODOLOGY*

APPENDIX B: CRITERIA

Texas Department of Information Resource-Security Control Standards Catalog Version 1.3 (TAC 202.76)

AC-2 Account Management

RISK STATEMENT

To prevent unauthorized access to information systems.

CONTROL DESCRIPTION

The organization:

…

c. Establishes conditions for group and role membership;

d. Specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account;

e. Requires approvals by [Assignment: organization-defined personnel or roles] for requests to create information system accounts;

f. Creates, enables, modifies, disables, and removes information system accounts in accordance with [Assignment: organization-defined procedures or conditions];

g. Monitors the use of, information system accounts;

h. Notifies account managers:

1. *When accounts are no longer required;*
2. *When users are terminated or transferred; and*
3. *When individual information system usage or need-to-know changes;*

i. Authorizes access to the information system based on:

1. *A valid access authorization;*
2. *Intended system usage; and*
3. *Other attributes as required by the organization or associated missions/business functions;*

j. Reviews accounts for compliance with account management requirements [Assignment: organization-defined frequency]; and

k. Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.

IMPLEMENTATION

STATE

Confidential information shall be accessible only to authorized users. An information file or record containing any confidential information shall be identified, documented, and protected in its entirety. Information resources assigned from one state organization to another or from a state organization to a contractor or other third party, at a minimum, shall be protected in accordance with the conditions imposed by the providing state organization.

STATE ORGANIZATION: [To be determined]

COMPARTMENT: [To be determined]

EXAMPLE(S)

The organization has:

a. Implemented role-based access to help in identifying and selecting only those accounts that enable organization mission/ business function.

b. Formulated process flow for approval of access request to information systems.

c. Defined policies and procedures for creating, modifying, disabling and removing user accounts in the system.

AC-3 Access Enforcement

RISK STATEMENT

Misconfigured access controls provide unauthorized access to information held in application systems.

CONTROL DESCRIPTION

The organization enforces approved authorizations for logical access to the system in accordance with applicable policy.

IMPLEMENTATION

STATE

1. Access to state information resources shall be appropriately managed.

2. Each user of information resources shall be assigned a unique identifier except for situations where risk analysis demonstrates no need for individual accountability of users. User identification shall be authenticated before the information resources system may grant that user access.

STATE ORGANIZATION: [To be determined]

COMPARTMENT: [To be determined]

EXAMPLE(S)

The organization has implemented role-based access control to determine how users may have access strictly to those functions that are described in job responsibilities.

AC-4 Information Flow Enforcement

RISK STATEMENT

Users gain access to information that is beyond their appropriate level of privilege.

CONTROL DESCRIPTION

The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies].

…

AC-5 Separation of Duties

RISK STATEMENT

The lack of user segregation of duties may result in unauthorized or unintentional modification or misuse of the organization's information assets.

CONTROL DESCRIPTION

The organization:

a. Separates [Assignment: organization-defined duties of individuals];
b. Documents separation of duties of individuals; and
c. Defines information system access authorizations to support separation of duties.

IMPLEMENTATION

STATE

State organizations shall ensure adequate controls and separation of duties for tasks that are susceptible to fraudulent or other unauthorized activity.

…

AC-6 Least Privilege

RISK STATEMENT

Information in applications is accessed by users and other personnel outside of defined business requirements.

CONTROL DESCRIPTION

The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.

…

EXAMPLE

Only authorized users have authorized accounts to establish system accounts, configure access authorizations, filter firewall rules, manage cryptographic keys, and access control lists.

UTS 165 Information Resources Use and Security Policy

UTS 165 Standard 4: Access Management

…

4.1 Access Management Requirement.

(a) All Institutions must adopt Access Management processes to ensure that access to Information Resources is restricted to authorized Users.

…

4.2 Access Management Process: An Access Management Process must incorporate Procedures for:

…

(d) reviewing, removing and/or disabling accounts at least quarterly, or more often if warranted by Risk, to reflect current User needs or changes of User role or employment status;

…

4.5 Data Access Control Requirement. All Owners and Custodians must control and monitor access to Data within their scope of responsibility based on Data sensitivity and Risk, and through use of appropriate administrative, physical, and technical safeguards including the following:

(a) Owners must limit access to records containing Confidential Data to those employees who need access for the performance of the employees' job responsibilities. An employee may not access Confidential Data if it is not necessary and relevant to the employee's job function.

(b) Owners and Custodians must monitor access to records containing Confidential Data by the use of appropriate measures as determined by applicable Policies, Standards, Procedures, and regulatory requirements.

…

UTEP Information Resources Use and Security Policy

UTEP Standard 4: Access Management (January 10, 2019)

…

4.1 Access Management Requirement. Information Resource accounts are the means used to grant access to UTEP's Information Resources. These processes ensure that access to Information Resources are restricted to authorized Users.

Authorized users of University Information Resources are:

i. University students who are limited to the use of those Information Resources specifically assigned to serve educational purposes;

ii. University employees who are provided access to those Information Resources required for the performance of their duties in the conduct of official business. Access to any particular administrative data file/system must be based on an employee's "need to know" as established by their official duties and reflected in the advance provision of specific authorization codes, passwords or other access-enabling means to the employee; and

…

(b) Access to an Information Resource may not be granted by another user without the permission of the Owner or the Owner's delegated custodian of the Information Resource.

4.2 Access Management Process.

…

(d) Data/System Owners, System Administrators, and/or other authorized personnel are responsible for reviewing, removing and/or disabling accounts in a timely manner, or more often if warranted by risk, to reflect current User needs or changes to User roles or employment status. Unless otherwise documented and approved by the ISO, please follow the guidelines established below:

…

v. documenting a process to modify a user account to accommodate situations such as name changes, status or role change, accounting changes and permission changes to reflect their current status;

vi. documenting a process for reviewing existing accounts for validity at least annually and for reflecting their current status;

…

viii. are subject to independent audit review;

…

4.5 Data Access Control Requirements. All Owners and Custodians must control and monitor access to Data within their scope of responsibility based on Data sensitivity and risk and through use of appropriate administrative, physical, and technical safeguards including the following:

(a) Owners must limit access to records containing Confidential Data to those employees who need access for the performance of the employees' job responsibilities.

i. an employee may not access Confidential Data if it is not necessary and relevant to the employee's job function.

(b) Owners and Custodians must monitor access to records containing Confidential Data by the use of appropriate measures as determined by applicable policies, standards, procedures, and regulatory requirements. Access must be properly documented, authorized, and controlled.

(c) Owners and custodians must follow log capture and review processes based on risk and applicable policies, standards, procedures, and regulatory requirements (See 17.4). Such processes must include the:

i. data elements to be captured in logs;

ii. time interval for custodial review of the logs; and

iii. appropriate retention period for logs.

…

Return *SCOPE AND METHODOLOGY*

APPENDIX C: DEFINITIONS

	TERMS	DEFINITIONS
	Information Security Administrator (ISA)	The designated administrator is assigned perform access control/management of the information resource. *Reference: UTEP Standard 1: Information Resources Security Requirements and Accountability*
	OSRP IT Function	Personnel (including programmer analysts) under the Office of Research and Sponsored Projects (ORSP), who carry out IT related activities, including extracting data from PeopleSoft, maintaining the Project Information Center web application (PIC tool), and creating reports for ORSP.
	PeopleSoft Financials (FI) Module	PeopleSoft module that handle all financial related activities.
	PeopleSoft Human Capital Management (HR) Module	PeopleSoft module that handle human resources related activities.
	Elevated Access Roles	PeopleSoft roles that have permissions to create/update/delete/approve a transaction (within same security role), including roles that are classified as super users.
	System Integration (formerly known as "PeopleSoft")	The System Integration office is responsible for oversight of the University's Enterprise Resource Planning (ERP) system used for both financial and employee transactions. They coordinate with departments across campus to integrate large-scale systems where integration leads to increased efficiency in support of teaching and learning. *Reference: UTEP website*
	PeopleSoft Permission Lists	A collection of several pages that grants access to various functions. They are the foundation of security authorizations. In addition, they ultimately control what a user can and cannot access.
	PeopleSoft Roles	A logical collection of one or more permissions lists that authorize access to specific system functions (i.e. permission lists related to the management of multiple time and expense-related activities).
	Principle of Least Privilege	The principle that users and programs should only have the necessary privileges to complete their tasks. *Reference: National Institute of Standards and Technology (NIST)*