State of Wisconsin

DOA - DIVISION OF PERSONNEL MANAGEMENT

- OFFICE OF THE ADMINISTRATOR BULLETIN -

Date: January 31, 2019	**Subject:** Separation of Duties in PeopleSoft HCM
Locator No. DPM-0489-AO	

Separation of Duties (SOD) (also known as "Segregation of Duties") is a basic building block of sustainable risk management and internal controls for an organization. The principle of SOD is based on shared responsibilities of a key process that disperses the critical functions of that process to more than one person or department. SOD controls help reduce the risk of errors, misappropriations, and fraud. Employees should only be mapped to roles that are required for their job function(s). Separation of Duties in PeopleSoft HCM (HCM) is critical to effective internal control. It reduces the risk of both erroneous and inappropriate actions. In general, the payroll function, the time & labor function, and the HR specialist function should be separated among employees. When these functions cannot be separated, an internal control structure, such as a detailed supervisory review of related activities, is required.

Potential Risks Present in PeopleSoft HCM

There are six unique risks within the HCM system that must be considered when assigning Core User roles to an employee. One employee should **NOT** be able to perform all or some combinations of the following functions:

- Add an employee; and
- Enter, update, adjust timesheets or leave taken; and
- Update direct deposit; and
- Generate paychecks; and
- Process payroll

Risk 1:
Fictitious Employee is created and paid.

For a positive time reporter:

> The ability to establish an employee and to change the type of reporter should be separated from the ability to add and approve time or leave to employees' timesheets.
>
> If an agency with a small number of total staff is unable to separate these duties, a compensating control should be developed. For instance, if the number of employees is relatively small, a detailed review of the payroll register by a person not responsible for these duties, who would be aware of all current staff, could be performed. The review would need to be documented and maintained. The information reviewed would need to be a tested, canned query or report (not something that was provided by these same staff, which could then be manipulated).

For a negative exception reporter (typically referred to as an "exception time reporter"):

> The ability to set up an employee should be separated from the ability to set up the direct deposit and create and obtain the check.

Alternatively, because the number of exception reporters is expected to be limited at each agency, a compensating control could be created. For instance, a report showing all exception reporters could be reviewed by someone outside the payroll process. The review would be documented and maintained. The information reviewed would need to be a tested, canned query or report (not something provided by these same staff, which could have been manipulated).

Risk 2:
A terminated employee remains on payroll and continues to be paid.

For a positive time reporter:

The ability to update the employee record, such as updating the direct deposit or updating the type of reporter (change them to an exception reporter), should be separated from the ability to add and approve time.

If an agency with a small number of staff is unable to separate these duties, a compensating control should be developed. For instance, if the number of employees is relatively small, a detailed review of the payroll register by a person not responsible for these duties, who would be aware of all current staff, could be performed. The review would need to be documented and maintained. The information reviewed would need to be a tested, canned query or report (not something that was provided by these same staff, which could then be manipulated).

For a negative exception reporter:

The responsibility for terminations should be separated from the ability to set up the direct deposit and create and obtain the check.

Alternatively, because the number of exception reporters is expected to be limited at each agency, a compensating control could be created. For instance, a report that shows all exception reporters could be reviewed by someone outside the payroll process. The review would be documented and maintained. The information reviewed would need to be a tested, canned query or report (not something that was provided by these same staff, which could then be manipulated).

Risk 3:
An inappropriate one-time payment transaction is created and a check or a direct deposit is obtained by an unauthorized person.

For all staff, the ability to submit a one-time pay transaction should be separated from the ability to approve a one-time pay transaction.

Risk 4:
Adjustments are made to the system that create errors or fraudulent events.

Adjustments should be requested/reviewed by appropriate staff and completed by a small number of central staff. These adjustments include:

- Adjustments to payroll balances;
- Adjustments made using correction mode; and
- Mass base pay changes.

Documentation of all adjustments should be maintained, including who requested and reviewed them.

Risk 5:
An employee payment receipted by the agency related to an arrears or billing could be retained by the employee recording the receipt, and the account written off.

For all staff: the ability to write-off amounts should be separated from those who are receipting payments. If that is not possible, all write-offs should receive a secondary, manual review by management.

Assignment of Core User Roles for Agencies in PeopleSoft HCM

Requests for Core User security roles for HCM will occur directly in the system. Instructions for submitting security requests can be found here. All requests will be required to be approved at both the agency and central level. The fundamental premise of separation of duties is that no one person be able to control or perform all aspects of a business transaction or process. The combinations noted below should be avoided whenever possible. Agencies should review organizational structure and back-up responsibilities in order to identify where a separation of duties should exist. Agencies should grant "view-only" access whenever possible.

The role combinations that trigger a separation of duties violation are as follows:

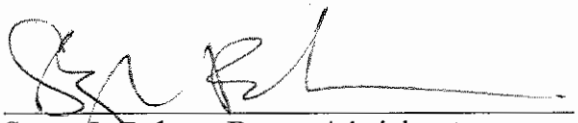
- HR Specialist and Payroll Specialist (PY_ADMIN) security roles
- HR Specialist and Time and Labor Specialist (TL_ADMIN) security roles
- HR Specialist and TL_SSO security roles
- HR Specialist and PY_SSO security roles
- HR Specialist and Central Payroll Time and Labor (TL_CORE_TIME_ADMIN) security roles
- HR_SSO and PY_SSO security roles
- HR_SSO and TL_SSO security roles
- HR Correction and Payroll Specialist (PY_ADMIN) security roles
- HR Correction and Time and Labor Specialist (TL_ADMIN) security roles
- HR Correction and TL_SSO security roles
- HR Correction and PY_SSO security roles
- HR Correction and Central Payroll Specialist (PY_ACCT_MANAGER) security roles
- HR Correction and Central Payroll Time and Labor (TL_CORE_TIME_ADMIN) security roles
- Payroll Specialist (PY_ADMIN) and Central Payroll Specialist (PY_ACCT_MANAGER) security roles
- Payroll Specialist (PY_ADMIN) and PY_SSO
- Courts Correction and Payroll Specialist (PY_ADMIN) security roles
- Courts Correction and Time and Labor Specialist (TL_ADMIN) security roles
- Courts Correction and TL_SSO security roles
- Courts Correction and PY_SSO security roles
- Courts Correction and Central Payroll Specialist (PY_ACCT_MANAGER) security roles
- Courts Correction and Central Payroll Time and Labor (TL_CORE_TIME_ADMIN) security roles
- Agency Benefits Specialist and any Accounts Receivable roles in FINANCE (this does not automatically trigger in the system and will require manual review)

Exceptions

Smaller agencies or those with remote locations often find it impractical to have meaningful separation of duties due to limited staff among which duties can be assigned. The Division of Personnel Management (DPM) enterprise staff and Central Payroll will provide routine monitoring of HCM transactions to identify potential SOD violations. Results will be provided to HR Managers, or the highest level of HR

leadership assigned to an agency, for explanation and additional internal control information where necessary. For permanent SOD exceptions, the agency should review the organizational structure, back-up responsibilities, and internal control structure on an annual basis to determine whether an SOD exception is still required or whether changes have occurred that would eliminate the need for an employee to have conflicting roles. Each year, agencies will resubmit a security request for individuals with an SOD exception which will include an explanation of the continuing need for the exception and set the expiration date to the following year. Each employee granted an SOD exception must complete the Separation of Duties Security Acknowledgement (DOA-15543), which will be placed in their official personnel file (P-File). For permanent SOD exceptions, the employee will only be required to submit a new acknowledgement form if the employee moves to a new position or is granted additional roles which creates new risks. For temporary requests, an explanation will be included in the security request along with an expiration date. If the need for an exception continues past the initial expiration date, a new request will be submitted for central approval and the employee will complete a new acknowledgement form.

Any security access granted to an employee outside the normal security request process in HCM which triggers a SOD risk requires an explanation, including expiration date, to be attached to the employee's acknowledgement form. The explanation will include an explanation of why the access was granted in a different manner than the HCM process and the necessity for such access.



Stacey L. Rolston, Deputy Administrator
Division of Personnel Management