Finance Duty Segregation Guidelines

Finance Module(s)	Segregation of Duty Scenarios	Business Impact/Risk	Segregation Recommendations
CM (Cash Management) Central Office Only	Individuals who can load bank files and reconcile cash.	The risk increases that a single user can bypass cash management controls.	Segregate Load BAI File from Cash Management.
	Access to setup information should be limited and restricted.	Granting inappropriate users access to maintain setup data could result in erroneous or unintentional changes.	Limit access to CM Setup.
GL (General Ledger) Central Office Only	Access to approve journals should be limited and segregated.	Granting a single user the ability to enter, post and approve their own journals increases the risk that a single user can bypass journal processing controls.	Segregate GL Specialist from GL Administrator.
	Individuals intended to have inquiry-only access should only be granted inquiry-only responsibilities.	Unintentionally granting modify access to an inquiry-only individual increases the risk of unauthorized entries.	Limit those individuals to GL Inquiry only. All other GL responsibilities should not be granted.
	Access to setup and master information should be limited and restricted.	Granting inappropriate users access to maintain setup data could result in erroneous or unintentional changes.	Limit access to GL Setup.
	Access to run journal import should be restricted and limited. In addition, other journal activities (e.g., posting) should not be granted to those individuals with journal import access.	Segregation of journal import functionality is recommended to limit a single user's ability to import journals and perform journal activities (e.g., posting).	Limit access to IS Processing. Segregate IS Processing from GL Specialist and GL Administrator.
AP/PO - Campus (Accounts Payable / Purchasing)	Access to central office responsibilities should be restricted to central office personnel only.	Granting campus users access to central office responsibilities increases the risk of unauthorized or unintentional modifications to data.	Grant campus users only campus-level responsibilities for AP/PO.
	Access to create/ modify supplier information should be segregated from the following processes: • Generate a purchase order • Create an invoice • Make a payment (central office only)	Granting a single user the ability to create a new supplier (or modify an existing supplier) and to perform purchasing, invoice and/or payment functions increases the risks that purchase-to-pay controls may be circumvented and payments made to inappropriate or erroneous suppliers.	Limit access to Campus Supplier Update. Segregate AP Administrator from Campus Supplier Update. Segregate AP Administrator from Purchasing Administrator, Purchasing Specialist and Purchasing Buyer. Segregate Campus Supplier Update from Purchasing Administrator, Purchasing Specialist and Purchasing Buyer.

	Individuals intended to have inquiry-only access should only be granted inquiry-only responsibilities.	Unintentionally granting modify access to an inquiry-only individual increases the risk of unauthorized entries.	Limit those individuals to AP Inquiry and PO Inquiry only. All other AP and PO responsibilities should not be granted.
	Access to generate and approve a PO should be segregated from the ability to create an invoice.	Granting a single user the ability to generate and approve a PO and process an invoice may increase the risks that purchase-to-pay controls may be circumvented and payments made for inappropriate or erroneous purchases.	Segregate AP Administrator from Purchasing Administrator, Purchasing Specialist and Purchasing Buyer.
	Access to create and modify receiving information should be segregated from the ability to generate a PO and invoice.	Granting a single user the ability to generate a requisition, approve a PO, apply the receipt and create an invoice increases the risks that purchase-to-pay controls may be circumvented.	Segregate Central Receiving from AP Administrator, Purchasing Administrator, Purchasing Specialist and Purchasing Buyer.
AP/PO – Central Central Office Only	Access to setup and master information should be limited and restricted.	Granting inappropriate users access to maintain setup data could result in erroneous, unauthorized or unintentional changes.	Limit access to AP Setup and Purchasing Setup. Segregate access to AP Setup and Purchasing Setup.
	Access to create/ modify supplier information should be segregated from the following purchase-to-pay processes: - Generate a PO - Create an Invoice - Make a Payment (Central Office only)	Granting a single user the ability to create a new supplier (or modify an existing supplier) as well as perform PO, invoice and payment functions increases the risks that purchase-to-pay controls may be circumvented and payments made to inappropriate or erroneous suppliers.	Limit access to Central Office Supplier Update. Segregate Central Office AP Administrator from Central Office Supplier Update. Segregate Central Office AP Administrator from Purchasing Administrator, Purchasing Specialist and Purchasing Buyer. Segregate Central Office Supplier Update from Purchasing Administrator, Purchasing Specialist and Purchasing Buyer.
	Access to run payment batches should be restricted and limited. In addition, other invoice and payment activities should not be granted to those individuals with running payment batch access.	Segregation of running payment batch processes is recommended to limit a single user's ability to perform invoice and payment activity and run the batch process.	Limit access to IS Processing. Segregate IS Processing from Central Office AP Administrator and Central Office Supplier Update.
	Individuals intended to have inquiry-only access should be granted inquiry-only responsibilities.	Unintentionally granting modify access to an inquiry-only individual increases the risk of unauthorized entries.	Limit those individuals to AP Inquiry only. All other AP and PO Responsibilities should not be granted.

Back to [Guidelines for Segregating User Duties](#)