

**OCFO Business Systems User Access Review**  
**Risk Based Review - Categories, Criteria and Review Cycle**

4/10/2015

<b>Risk Group</b>	<b>Review Cycle/ Risk Criteria</b>
<b>1 - Very Sensitive Roles</b>	<i>Review every 6 months</i>
	Sys and application admin roles with broad permissions
	Security management roles
	Roles with Correction Mode
	Roles with potential COI: eg, Print AP checks; apply cash receipts; manage Lab bank accounts
	Functional roles with broad permissions with potential for COI
	<b>Roles that previously had no users assigned</b>
<b>2 - Sensitive Roles</b>	<i>Review every 12 months</i>
	Application module specific admin and configuration
	IT system tools and infrastructure management
	Manages user setup: Signature auth; credit cards
	Manages vendor setup
	Manages personal identify information (PII) or Read Only roles that have access to PII or confidential intellectual property
	Create new financial transactions: PO's; cost transfers; journal entries; create WFO or misc. invoices; invoice vouchers
	Transaction approval - sensitive transactions: controlled materials or services; high value or broad approval authority (non-dynamic roles)
	DOE proposal approvals
	Payroll staff specific roles: Payroll system; LDRS; LETS
	Roles related to special batch process agent operators
<b>3 - Restricted Roles</b>	<i>Review every 2 years</i>
	Central Office functional staff specific roles - limited permissions; low or no COI potential
	Read-only access to sensitive information (eg, PII)
<b>4 - Limited Roles</b>	<i>Review every 3 years</i>
	Division user roles with limited permissions
	Transaction approval - non-sensitive transactions: construction; furniture; telephone purchases
	Transaction reviewer roles - purchase requisitions
<b>5 - No Risk Roles</b>	<i>No formal review required</i>
	Public roles - assigned to all employees and guests regardless of responsibilities
	Dynamic roles - assigned based on external criteria
	Read only roles - access to non-sensitive information
	Process error and warning notifications