

## User Account Management for FISMA and ISO 27001 Audit

Objectives:	Procedures	Status	Notes
The organization manages information system accounts, including authorizing, establishing, activating, modifying, reviewing, disabling, and removing accounts;	Examine access control policy, account management procedures, security plan, or other relevant documents; reviewing for the measures to be employed to manage information system accounts, including authorizing, establishing, activating, modifying, reviewing, disabling, and removing accounts.		
The organization defines in the security plan, explicitly or by reference, the frequency of information system account reviews and the frequency is at least annually;	Examine an agreed-upon representative sample of records of account maintenance actions for an agreed-upon representative sample of active system accounts, along with the name of the individual associated with each account; reviewing for evidence that the measures related to active accounts		
The organization reviews information system accounts in accordance with organization-defined frequency; and	Examine records of account disabling or removal actions for accounts associated with an agreed-upon representative sample of recently transferred, separated, or terminated employees; reviewing for evidence that the measures related to disabling or removing accounts		
The organization initiates required actions on information system accounts based on the review.	Interview an agreed-upon representative sample of organizational personnel with account management responsibilities;		
	Examine the security plan; reviewing for the frequency (to be at least annually) of information system account reviews.		
	Examine an agreed-upon representative sample of records of information system account reviews;		
	Interview an agreed-upon representative sample of organizational personnel with account management responsibilities; conducting focused discussions for evidence that the organization initiates required actions on information system accounts based on the periodic account reviews.		

Objectives:	Procedures	Status	Notes
The organization employs automated mechanisms to audit account creation, modification, disabling, and termination actions; and	Examine security plan, information system design documentation, or other relevant documents; reviewing for the automated mechanisms and their configuration settings to be employed to audit account creation, modification, disabling, and termination actions.		
The organization employs automated mechanisms to notify, as required, appropriate individuals.	Examine documentation describing the current configuration settings		
	Test an agreed-upon representative sample of the automated mechanisms; conducting generalized testing for evidence that these mechanisms operate as intended.		
	Examine account management policy, procedures addressing account management, security plan, or other relevant documents; reviewing for the notifications deemed required by the organization with regard to account management actions and for the individuals deemed appropriate by the organization to receive these notifications.		

	Note to assessor: The identification of when notification is required and to whom the notification should be provided need only be specific enough to enable determination of whether the organizational intent is being achieved; for example, the individuals need not be called out by name but may be defined by the positions or roles that need to receive the notification.		
	Examine the security plan, information system design documentation; reviewing for the automated mechanisms and their configuration settings		
	Examine documentation describing the current configuration settings		
	Test an agreed-upon representative sample of the automated mechanisms implementing account management functions; conducting generalized testing for evidence that these mechanisms operate as intended.		