Configuration Management checklist (section 3.5.2)
Server Security #5
June 1, 2011

The left column indicates whether the standard is listed in the Information Security Plan as a **M**ust or **S**hould. A justification must be written for any standard not followed in the department procedures. The justification must be approved by the IT Manager for items listed as a Should and also reviewed with the IT Security Office if the item was listed as a **M**ust. The IT manager must review, sign and date, all exceptions every six months to indicate that the exception is still necessary.

M/S	Item	Y/N
M	1. Server build configurations are documented (each server)	
S	2. Minimum documentation contents	
	a. Server name. b. Operating system and version (such as Windows Server 2008, SP3). c. Security patches. d. File system configuration. e. Group policies. f. Local accounts. g. Services running. h. Application software installed (with version). i. Network settings (including IP address, DNS settings, and so on). j. Domain information. k. Partitions/Shares with permissions. l. Physical system location. m. User information (as appropriate to rebuild/notify of changes). n. System model, speed, RAM and disk size, and available space. o. Hardware manufacturers (optional but recommended). p. System image information (for rebuilds).	
S	3. Disable AutoRun function for CD/DVD/USB devices	
M	4. Configure with appropriate redundancies, examples:	
S	a. RAID	
S	b. Dual power	
S	5. Monitor power usage & notify IT Manager of resource issues	
M	6. For servers behind FW, provide build to TSO 2 weeks prior to network connection	
M	7. For virtual servers behind FW, plans to TSO prior to build	
M	8. Document process to review server vulnerabilities (Foundstone, etc) at least after each modification (patches, upgrades, software changes)	
	1. If no formal change management needed (patches, accounts, etc.)	
	a. Modify server build document as applicable	
	b. Scan server for new vulnerabilities	
	2. If change affects a number of users/critical system, minimum documentation	
M	a. Description of change	

Configuration Management checklist (section 3.5.2)
Server Security #5
June 1, 2011

M/S	Item	Y/N
M	b. Reason for change	
M	c. Date and time of change	
M	d. Who made the change	
M	e. How the change was implemented	
M	f. How the change was tested/monitored	
M	g. Rollback process	
	h. Approval process	
M	i. Submit change to IT Manager	
M	ii. IT Manager assess impact	
M	iii. If multiple areas affected, communication of change	
M	iv. If denied, requestor refine and resubmit	
M	v. If PL1 involved, custodian Manager must approve	
	3. If change affects multiple departments/campus wide:	
S	a. Changes submitted to Configuration Management (CM) team	
	i. Use list in #2 for change request	
S	b. CM authorize change	
S	c. Implementation date set	
S	d. Upgrade announced prior to implementation	
S	e. Affected users have opportunity to comment	
S	f. Follow-up reminder sent before implementation	
S	g. Appropriate precautions (such as backups) completed	
S	h. Change completed	
S	i. Change tested	
S	j. If successful, access restored	
S	k. If unsuccessful, rollback process initiate	
S	l. Users notified of outcome (successful/rollback)	
S	m. File change documentation	