

Policy		Checklist Item	Written into Policy?	Written Comments	Enforced?	Enforcement Comments	Status
Security Risk Management Policy	Purpose	The purpose of the policy is clearly stated.	Yes		N/A		Done!
	Scope	The scope of the policy is clearly stated.	No	Define to whom and to what systems this policy applies. List the employees required to comply or simply indicate "all" if all must comply. Also indicate any exclusions or exceptions that are out of scope, i.e. those people, elements, or situations that are not covered by this policy or where special consideration may be made.	N/A		Write
	Governing Laws, Regulations, and Standards	Governing laws and regulations requiring a risk management program are specified.	No	If applicable, list any laws or regulations that govern the policy or with which the policy must comply. Confirm with the legal department that the list is full and accurate. If there are no pertinent governing laws or regulations, mark cell F37 of this tool as N/A.	N/A		Write
	Review	State frequency of reviewing the policy.	Yes				
		State frequency of reviewing the assessment procedures.	Yes				
	Risk Assessment	Conduct risk assessment on information system data handling, access, and disruption.	Yes				
		Document, maintain and review risk assessment results. State who will be notified of results.	No	Add this statement into the policy and customize it to your organization.			Write
	Vulnerability Scanning	State that vulnerability scanning in information system and hosted applications will occur during a defined time period, and that vulnerabilities will be remediated in accordance with an organizational assessment of risk.	No	Add this statement into the policy and customize it to your organization.			Write