University of Connecticut

Information Security Office

Risk Management Exception Template

Revision History

Revision Date	Revised By	Summary of Revisions	Section(s) / Page(s) Revised
6/01/2013	ISO	Initial Release	All

Approvals

Review Date	Reviewed By	Name/Title	Action (Reviewed or Approved)
6/01/2013	CISO	Jason Pufahl, CISO	Approved
6/01/2013	RMAC	Risk Management Advisory Council	Reviewed

University of Connecticut

Risk Management Exception Template

Please check one of the following:

__ Risk Management Exception Request

__ Risk Management Issue Report

__ Risk Management Vulnerability Report

Requester: ________________________________

Date of request: ___________________________

Date of RMAC Review: _____________________

Close Date: ________________________________

Service\Application Name	
CVE	CVE-
CVSS	
Description *(from scan report, if applicable)*	
Host(s)	
Vulnerability / Issue Overview *(plain description of vulnerability)*	
Risk statement *(Describe likelihood of exploitation)*	
Risk statement *(Describe the business impact if realized)*	
Population Affected *(Department(s), # people, affiliations)*	
Service / Application owner	
Current In-Place Risk Mitigation Controls	
Remediation Road Blocks *(justification for an exception or other remediation road blocks that would need to be addressed)*	
Remediation Options *(include cost, resource, & time estimates)*	
RMAC recommendation(s)	
Resolution details:	

Instructions:

1. Please indicate what type of request/report you are submitting.
   a. You are requesting an exception to remediate an identified vulnerability.
   b. You are reporting an issue that might translate to risk for the University but does not show up as vulnerability on scanning reports.
   c. You are reporting a vulnerability with a server or application that is not currently being scanned and the vulnerability warrants attention from the security office.
2. Please see notes below for field by field information.

Service\Application Name	Required
CVE	CVE- if the vulnerability is noted in a scanning report
CVSS	If the vulnerability is noted in a scanning report
Description *(from scan report, if applicable)*	If there is a description in a scan report, please use that, otherwise provide your description
Host(s)	Host name(s), required.
Vulnerability / Issue Overview *(plain description of vulnerability or issue)*	Required
Risk statement *(Describe likelihood of exploitation)*	Required
Risk statement *(Describe the business impact if realized)*	Required, this field must be provided even if the likelihood is almost non-existent.
Population Affected *(Department(s), # people, affiliations)*	Required
Service / Application owner	Required
Current In-Place Risk Mitigation Controls	If none, please say "none"
Remediation Road Blocks *(justification for an exception or other remediation road blocks that would need to be addressed)*	If applicable. If this submission is for a vulnerability remediation exception, then this is a required field.
Remediation Options *(include cost, resource, & time estimates)*	Required
RMAC recommendation(s)	To be provided back to the requester by RMAC.
Resolution details:	Reflects the decision of disposition of the request until and including when request is closed.