MUSC Information Security Risk Analysis Worksheet

Compliance Process Step: Identify and Analyze Potential Issues

Instructions

Please refer to MUSC' *Risk Management Guidelines* for complete information on the purpose and scope of the *Risk Assessment Worksheet* document. The *Risk Management Guidelines* are published on the Web at http://www.musc.edu/security/guidelines.

The *Risk Analysis Worksheet* should be completed by your risk assessment team. Collectively, the members of your team must have knowledge of your System, knowledge of the organization, understanding of applicable security policies and standards, and understanding of the organization's security architecture and plans, that is sufficient to enable them to identify relevant threats, vulnerabilities, and other security issues, to assess risks, to analyze potential security controls, to specify an optimal set of controls, and to communicate their findings to the appropriate management.

In the Security Issue column, your team should record a brief statement of the security issue or area of concern that they have identified. Issues are identified by considering threat-vulnerability pairs that potentially affect the System, or by considering the System's known information security policy compliance gaps. Any requirement on your Compliance Checklist that achieved a score lower than 3 must be recorded here as a security issue.

For threat-vulnerability pairs, use the Likelihood and Impact columns to record the estimated likelihood of this particular issue occurring (Low, Medium or High), and its potential impact (Low, Medium or High). See the *Guidelines* for more information. Ignore these two columns for any security issue that derives from known policy compliance gaps, because you will just arbitrarily assign that issue a High risk level in the next column. See the *Guidelines* for more information.

In the Risk Level column, record the risk level (Low, Medium, or High) for this issue. The risk level follows either from the product of the Likelihood and Impact ratings, or from the fact that this particular security issue derives from a known compliance gap, in which case the Risk level must arbitrarily be rated as High. See the *Guidelines* for more information.

In the next two columns, list the specific security control(s) that your risk assessment team is recommending to address this particular issue, and the overall relative priority of each recommended control. Strategies for analyzing and selecting controls are explained in the *Guidelines*.

MUSC Information Security Risk Analysis Worksheet

Compliance Process Step: Identify and Analyze Potential Issues

Instructions

Use the Comments column to record any other information that is considered relevant to the security risk management decision-making process for this particular security issue.

The *Risk Analysis Worksheet* should be presented to management at the appropriate level. Management may request changes to the assessment team's recommended control selections and priorities. Once it has been finalized after management review, the *Risk Analysis Worksheet* should be used to guide the development of your System's security plan.

Your risk assessment team, and the members of management who review your Risk Analysis Worksheet, should ensure that all proposed security controls are consistent with MUSC's overall information security architecture and plans. The Information Security Office in the Office of the CIO can assist in this regard. Contact information on the Web at http://www.musc.edu/security.

MUSC Information Security Risk Analysis Worksheet

System Name: **Prepared By:**

System Owner: **Date:**

Security Issue (Threat-Vulnerability Pair or Compliance Issue)	Likelihood	Impact	Risk Level	Recommended Security Controls	Control Priorities	Comments