Table 8. Risk Definitions

Rating	Definition of Risk Rating
High	Exploitation of the technical or procedural vulnerability will cause substantial harm to CMS business processes. Significant political, financial, and legal damage is likely to result
Moderate	Exploitation of the technical or procedural vulnerability will significantly impact the confidentiality, integrity and/or availability of the system or data. Exploitation of the vulnerability may cause moderate financial loss or public embarrassment to CMS
Low	Exploitation of the technical or procedural vulnerability will cause minimal impact to CMS operations. The confidentiality, integrity and availability of sensitive information are not at risk of compromise. Exploitation of the vulnerability may cause slight financial loss or public embarrassment

4.1.4 CMSR Security Control Family and Reference

The CMSR security control family and control number that is affected by the vulnerability is identified in the CMSR Security Control Family and the Reference columns.

4.1.5 Affected Systems

The systems, URLs, IP addresses, etc., affected by the weakness, are identified in the Affected Systems column.

4.1.6 Ease-of-Fix

Each finding is assigned an Ease-of-Fix rating described as Easy, Moderately Difficult, Very Difficult, or No Known Fix. The ease with which the Business Risk can be reduced or eliminated is described using the guidelines in Table 9.

Table 9. Definition of Ease-of-Fix Rating

Rating	Definition of Ease-of Fix Rating
Easy	The corrective action(s) can be completed quickly with minimal resources and without causing disruption to the system or data
Moderately Difficult	Remediation efforts will likely cause a noticeable service disruption: • A vendor patch or major configuration change may be required to close the vulnerability • An upgrade to a different version of the software may be required to address the impact severity • The system may require a reconfiguration to mitigate the threat exposure • Corrective action may require construction or significant alterations to the manner in which business is undertaken
Very Difficult	The high risk of substantial service disruption makes it impractical to complete the corrective action for mission critical systems without careful scheduling: • An obscure, hard-to-find vendor patch may be required to close the vulnerability • Significant, time-consuming configuration changes may be required to address the threat exposure or impact severity • Corrective action requires major construction or redesign of an entire business process
No Known Fix	No known solution to the problem currently exists. The Risk may require the Business Owner to: • Discontinue use of the software or protocol • Isolate the information system within the enterprise, thereby eliminating reliance on the system In some cases, the vulnerability is due to a design-level flaw that cannot be resolved through the application of vendor patches or the reconfiguration of the system. If the system is critical and must be used to support on-going business functions, no less than quarterly monitoring shall be