Scans of web applications, systems, services, operating systems, and devices with regulatory and compliance requirements (*e.g.*

5.3. Critical and High vulnerabilities must be patched as soon as possible, according to the timelines detailed in the *Software Patch Management Information Security Standard*. ServiceNow tickets will not be closed until remediation and clean rescans are completed, or until mitigating controls have been established, documented, tested/validated, and an exception request has been approved by the CIO.

5.4. In some instances, the CIO will approve the network quarantine of an IT Resource with Critical or High vulnerability if Information Security Services assesses the risk and lack of remediation. In such cases, a notice will be sent to the system owner prior to the quarantine.

6. Exceptions Review. In the event that vulnerability remediation (patching, updating, or establishing mitigating controls) cannot follow the stated schedule, an exception request must be made that details why postponement or deferral is needed. The CIO or authorized designee must grant remediation exception request approvals, which will be submitted through the ServiceNow system. Exceptions may include:

Production system freeze or change blackout periods

request