Function or Functional Area	Objective	Risk(s)	Reference	Test Steps	Expected Result
Web site security	-Identify vulnerabilities related to cross-site scripting (XSS)	-Risk of data compromise	-OWASP Application Security Verification Standard(ASVS)	-Conduct an internal security test. -Run an automated web scan using the Acunetix vulnerability scanner. -Manually review the source code of the website.	-A report identifying any vulnerabilities related to XSS. -All identified vulnerabilities should be mitigated or fixed.
WebLogic servers	-Evaluate the effectiveness of patch management process	-Risk of unauthorized access, data compromise, loss or destruction	-NIST SP 800-53	-Conduct an internal security test -Run a load test. -Review the configuration data and applications stored in clear text on the file system. -Examine WebLogic Server authentication and authorization	-A report identifying any vulnerabilities in WebLogic Server authentication and authorization. -A recommendation to improve the configuration and hardening of WebLogic servers, if necessary.
Remote access security	-Identify weaknesses in vendor access controls	-Risk of unauthorized access, data compromise, loss or destruction	-NIST SP 800-46 Rev. 2	-Conduct an external security test. -Review vendor access policies and procedures. -Review the usage of vendor accounts. -Attempt to gain unauthorized access using vendor accounts	-A report identifying any weaknesses in vendor access controls. -A recommendation to improve vendor access controls, if necessary.
Proper separation of PROD, DEV, and TEST environments	-Confirm the separation of environments and identify any unauthorized changes	-Risk of data compromise, loss or destruction	-ISO 27001:2022 A 8.31	-Conduct an internal security test. -Review the environment separation policies and procedures. -Review accessany unauthorized changes.	-A report confirming the separation of environments and identifying any unauthorized changes. -A recommendation to improve the separation of environments, if necessary.
Logging and monitoring	-Evaluate the effectiveness of logging and monitoring for security purposes	-Risk of data compromise, loss or destruction	-CIS Control 8,13	-Conduct an internal security test. -Review the configuration of Splunk. -Review the logs for security events. -Review logging and monitoring policies and procedures.	-A report identifying any weaknesses in logging and monitoring for security purposes. -A recommendation to improve logging and monitoring for security purposes, if necessary.