Function	Objective	Risks	CIS Top 20	Test Steps	Results
Website security	The web application is not susceptible to common attacks such as Cross Site Scripting (XSS) or SQL injection, and is running at minimum TLS 1.2.	Web application attacks can disclose sensitive information	Control 7, Control 16	Use pentesting tools and close vulnerable ports.	
WebLogic servers	Servers are properly patched them and have encryption enabled to prevent any data from being stored in plain text.	If an attacker gains access to a server, they can view confidential information in plain text.	Control 3, Control 13	Each item must be tested individually: Atomicity - Test the site by executing actions such as going to the checkout page without having any items in the cart. Consistency - ensure there is proper field data validation in order to counter SQL injection attacks. Isolation - ensure that one	The completeness and accuracy of transactions is confirmed. Exploits launched against them do not succeed.
Database security	The servers are ACID-compliant and meet all four of its criteria: Atomicity, Consistency, Isolation and Durability	Meeting the ACID Requirements will help ensure transaction integrity, maximize uptime, and ensure that all transactions are processed completely and accurately.	Control 3	Each item must be tested individually: Atomicity - Test the site by executing actions such as going to the checkout page without having any items in the cart. Consistency - ensure there is proper field data validation in order to counter SQL injection attacks. Isolation - ensure that one	The completeness and accuracy of transactions is confirmed. Exploits launched against them do not succeed.
Transaction processing	Data validation and controls are in place: Range check, Completeness check, Validity check, Duplicate check, Reasonableness check, Logical Relationship check and Existence check to ensure data being input	Lack of data validation controls can impact accuracy and completeness of transactions, which could ave severe financial implications.	PCI DSS	In a test environment, test the website for invalid data inputs.	We should expect to see invalid data inputs rejected or flagged.
Remote access security	Shared accounts are not used, and proper logging and monitoring are in place to ensure and track users logging in at odd hours.	Shared accounts make it difficult to tie activities to an individual (accountability).	Control 1, Control 5	Configure accounts so that permissions are separate and high level accounts have MFA enabled to help prevent account takeover.	We should see a reduction in shared account activity and be able to pinpoint responsibility for actions performed by accounts.
Proper separation of the PROD, DEV and TEST environments	The Test, Dev and Prod environments are separated such that proper Separation of Duties (SoD) is enforced and maintained.	Improperly isolated Test, Dev and Prod environments can negatively impact the production environment in the form of unauthorized/unapproved changes.		Review standard operating procedures when it comes to creating new products and migrating them to the production environment. Clearly separate the stages of development so that proper SoD is enforced and maintained.	All changes follow the change control policy. Change requestors cannot approve their own changes. Developers cannot make changes to production. All changes are authorized and approved prior to migration to production.
Logging and monitoring	Logs are properly configured to capture relevant information and store it in a secure location.	A lack of proper logging and monitoring impairs the ability to reconstruct attacks or events for investigative and troubleshooting purposes.	Control 6, Control 13	Check Splunk configuration to ensure it captures logs on system changes to ensure we can trace actions to the proper user and capture relevant data to perform proper forensics.	Higher quality logs that provide much greater insight into user actions performed on our systems. Ability to reconstruct a series of events for investigative purposes.