Function	Objective	Risk	Test & Mitigation Steps	Expected Results
Web site security	Ensure our web application is not subceptable to common attacks such as Cross Scripting (XSS) or SQL injections and ensure we are running at minimin TLS 1.2 and not longer utulize SSL because it is no longer secure.	Our website can subsentable to XSS attacks and can give threats a launching off points to more sensitive systems.	We will utulize a suite of pentesting tools to ensure our website are not easily exploitable by attackers and close of uncesessary ports as descrive in the CIS control. Ensure unsecurte ports are closed such as port 80.	From testing we should be able to determine wehter we have poorly written code that can leave our site open to attacks.
WebLogic servers	Secure our servers by properly patching them and ensure we have encryption enable to prevent any data from being stored in plain text.	Last year a lack of patching allowed on of our server to be attacked with a coinminer attack, if we are not properly patching our servers they can again be exploited and even cause a data leak and impact our avilibility on OLTP services.	First we must check our servers configurations and that our servers are properly patched, also test those patches to ensure they do not negative impact our production enviroment. Following that we should some penetration test to ensure that our servers are not easily exploitable and hardened our servers based on the findings on the pen test.	We should expect to see a few missing patches but we can remidiate that and patch them to prevent any threat from attacking and gaining access to them.
Database security	We will ensure our servers are ACID complient and meet all four of its critiria, Atomacity, Consistency, Isolation and Duralbility	Meeting the ACID Requirements will ensure we are not making transactions for prodcts we do not have, maintain stable uptime and ensure all transactions are processed properly, data validity, and prevent unhappy cstomers.	We must test each item idividually: Atomicity - we will test our site that we cannot skip steps such as going to checkcout page without having any items in your kart. Consistency - we must ensure that we cannot input unvalidated data values, to prevent attacks such as an SQL injection. Isolation - ensure that we cannot sell an item we are lacking and proper inventory is maintained at all times. Durability - stresstest our servers to ensure that data is process and stored properly	We should see that our database is propely secure and it functions and store data properly properly, and not easily supseptible to attacks.
Transaction processing	We will address some Data validation and controls: Range check, Completeness check, Validity check, Duplicate check, Reasonableness check, Logical Relationship check and Existence check to ensure data being input meets proper critiar when making a transaction.	Not having these controls will create imperfect data that can hurt our avility to make decisions with faulty data.	In a test enviroment test that our website does not accept invalid data inputs to prevent scripting attacks.	We should expect to see rejects of invalid data inputs.
Remote access security	Prevent shared accounts from bing used and ensure and maintain proper logs to ensure the autheticity of users logging in at odd hours.	Shared accounts make it difficult to pin resposibility on anyone person for changes made specially changes that negatively impact us.	Configure accounts so that permissions are seperate and high level accounts have MFA enabled to prevent account sharing.	We should see a ruduction in shared account activity and be able to pin point resposibility from actions performed on accounts.

Proper separation of the PROD, DEV and TEST environments	Validate that our DEV enviromet is seperate and isolated from our Production enviromet	Not having properly isolated developing and testing enviroment can negatively impact our production enviroment by causing unapproved changes and upto deletion of data to our production enviroments	First we must review our standard operating procedures pipeline when it comes to creating new products and pushing them to our production enviroment. We must cearly seperate the stages of product and prevent them from overlapping and pushing out unrefined products.	we should see a reduction in impact to our production enviroment from our test and development enviroments.
Logging and monitoring	Properly maintain logs with relevant information and ensure it is stored in a safe location	Most of Splunk logs are focused on performance, and without proper logs we can not perform proper forensics if we are attacked because we will not be able to see and trace how attackers got into our systems.	Check Splunk configuration to properly more than performance data and captures logs on system changes to ensure we can trace actions to the proper user and capture relevant data for to perform proper forensics.	we should have higher qualirt logs that provide much greater insight into our users actions performed on our systems. We should also have a lot more data to work with should our systems ever become comprimised.