Function	**Objective**	**Risks**	**Test & Mitigation Steps**		**Expected Results**
Function	**Objective**	**Risk**	**Test & Mitigation Steps**		
Web site security	To make sure the website is not at risk, for certain attacks such as cross site scripting XSS, man in the middle or SQL injection.	Web application attacks can lead to customer data being exposed to hackers.	Utilize pentesting tools to make sure the website is secure from hackers. Complete identification and validation. Make sure the unsecured port 80 is closed, per CIS control 5 standard.		Testing will confirm if site is vulnerable for an attac, via a poorly written code.
WebLogic servers	To make sure Weblogic and other servers are patched correctly and encrypt all data, to prevent hackers from reading data from jsp and html applications.	Unpatched servers can lead to vulnerability to be exploited, by an attacker with network access via HTM to compromise Oracle Weblogic.	Check server configuration, Patch management(ask for patch history for all servers, test patches), perform a penetration test and harden patches based on test findings. Per CIS control standard 5.		For the weblogic server to have complete process and transactions and no explotis.
Database security	To make sure all servers are ACID-compliant and meets Atomicity, Consistency, Isolation and Durability.	ACID requirements will maintain integrity and make sure all transactions on the web application are processed and accurate.	All databases and servers must be tested per ACID compliance. Atomicity- Test by performing a checkout on the website, with a item and without an item. Consistency-make sure data is valid to prevent attacks. Isolation-to make sure only services such as paying for the missed toll and ordering a new tag are available. Durability-stress test databases and servers to make sure they are durable. This can be done by a load test/ stress test to test data being sent.		To make sure exploits sent at the database are not successful and easy flow of transactions.

Transaction processing	Data validation and controls are in place: Range, Completeness, Duplicate, Validity, Reasonableness and Existence check. These controls will make sure transactions run smoothly.	Financial issues and data breaches can occur for customers and client, if data controls are not in place.	Test website data for accuracy. Perform a exception test. Exception learning.		Outcome is to see in accurate data to not beable to be entered or rejected.
Remote access security	To prevent use of vendors sharing accounts and checks in balances in place for logging and monitoring to track vendor use.	For to make sure everyone is being made accountable and tranparency.	Shared user accounts have to be removed, review which accounts are being shared amoungst vendors, review hours of operation of vendors. Configure vendor accounts per CIS control standards and make special access for high rated accounts, for access of certain vendors. Make account have MFA access.		Outcome is to reduce and/or eliminate shared accounts and to pinpoint logins per vendor.
Proper separation of the PROD, DEV and TEST environments	The Test, Dev and Prod environemtns are seperated, to maintain seperation of duties.	If not properly seperated each sector can be impacted via unauthorized and/or unapproved changes.	Review operating procedures. Review network control to make sure VLAN/Firewall are in place for a seperate environment. Find out if developers used accounts to build the application . Separate stages of development so that SoD is informed and maintained.		All changes will follow the change control policy. Change requestors can not approve initiated changes.
Logging and monitoring	Logs are configured properly and the splunk tool is used in an effective way. Logs are stored in a secure area.	Improper logging and monitoring of logs can prevent a valid investigation, if an attack is done on the system.	Check splunk configuration, to make sure the tool is working properly and capturing data. Make sure login attempts are monitored, even failed attempts.		Outcome to have higher quality logs for accountability, transparency and proper logging. This will allow a better investigation, if needed.