Controls and compliance

Controls assessment

Administrative Controls			
Control name	**Control type and explanation**	**Needs to be implemented (Y / N) - Purpose**	**Priority**
Least Privilege	Preventative, *All Botium Toys employees have access to internally stored data and customers' PII/SPII.*	Y - Reduce risk and overall impact of malicious insider	High
Disaster recovery plans	Corrective, No disaster recovery plans currently in place, Also doesn't have backups of critical data.	Y - for business continuity	High
Password policies	Preventative, No centralized password management system, which sometimes affects the productivity	Y - don't make easy access secure data / other assets by threat actor	High
Separation of duties	Preventative, not implemented	Y - Reduce risk and overall impact of malicious insider	High

Technical Controls			
Firewall	Preventative,The IT department has a firewall that blocks traffic based on an appropriately defined set of security rules.	**No**	
IDS/IPS	Detective, Not installed an intrusion detection system	Y - To detect and prevent anomalous traffic	High
Encryption	Deterrent, not currently used to ensure confidentiality of customers' credit card information that is accepted, processed, transmitted, and stored locally in the company's internal database.	Y - Provide confidentiality to sensitive information	High
Backups	Corrective company does not have backups of critical data.	Y - Restore/recover from an event	High
Password management	Preventative, no password management system currently in place;	Y - Reduce password fatigue	High
Antivirus (AV) software	Preventative, Antivirus software is installed and monitored regularly by the IT department.	**No**	
Manual monitoring, maintenance, and intervention	Preventative, maintained, there is no regular the schedule in place for these tasks and intervention methods are unclear.	Y - Necessary to identify and manage threats, risks, vulnerabilities to out-of-date systems	High

Physical/Operational Controls		
(CCTV) surveillance	Preventative/Detective, the store has up-to-date (CCTV) surveillance,	**No**
Locks	Deterrent/Preventative,Store has main offices, store front, and warehouse of products, has sufficient locks	**No**
Fire detection/prevention	Detective/Preventative, as well as functioning fire detection and preventing system	**No**