## Control and compliance assessment

* **Controls**

|  |  |  |
| --- | --- | --- |
| Name | Explanation/Type | Have |
| Least Privilege | all employees have access to customer data.  privileges need to be limited to reduce the risk of a breach. | **X** |
| Disaster recovery plans | no disaster recovery plans in place. These need to  be implemented to ensure business continuity. | **X** |
| Password policies | Need to establish password strength rules to improve security. | **X** |
| Separation of duties | Needs to be implemented to reduce the possibility of  fraud/access to critical data, since the company CEO  currently runs day-to-day operations and manages the  payroll. | **X** |
| Firewall | Already in place to block traffic based on appropriately defined set of security rules | **O** |
| Intrusion detection system (IDS) | Needs an IDS in place to help identify possible intrusions by threat actors | **X** |
| Backups | Needs to have backups of critical data to supports ongoing productivity in the case of an event | **X** |
| Antivirus software | Detect and quarantine known threats | **X** |
| Manual monitoring, maintenance, and intervention for legacy  systems | Required for legacy systems to identify and mitigate potential threats, risks, and vulnerabilities | **X** |
| Encryption | Needs to provide greater confidentiality of sensitive information. | **X** |
| Password management system | Needs to improve IT department employee productivity in the case of password issues.  Password recovery, reset. | **X** |
| Locks (offices, storefront, warehouse) | Already have physical locks for company’s offices, store front, and warehouse. | **O** |
| Closed-circuit television (CCTV) surveillance | CCTV is installed at the physical location | **O** |
| Fire detection/prevention | Already have a functioning fire detection and prevention system | **O** |
|  |  |  |

* **Compliance**

|  |  |  |
| --- | --- | --- |
| Name | Explanation/Type | Adhere |
| PCI DSS | All employees have access to the company’s internal data such as credit card information.  Company does not use encryption.  Password policies are nominal and have no management. | **X** |
| GDPR | Does not use encryption to better ensure the confidentiality of customers’ financial information.  Data is not classified and inventoried. | **X** |
| SOC type 1  SOC type 2 | Controls of Least Privilege and separation of duties are not in place.  Encryption is not used ensure PII/SPII.  Data is not available to individuals authorized to access it. | **X** |