# Delightfully Dipped Controls and compliance Audit

**Controls assessment checklist**

| **Yes** | **No** | **Control** |
| --- | --- | --- |
|  |  | Least privilege |
|  |  | Disaster recovery plans |
|  |  | Password policies |
|  |  | Separation of duties |
|  |  | Firewall |
|  |  | Intrusion detection system (IDS) |
|  |  | Backups |
|  |  | Antivirus software |
|  |  | Manual monitoring, maintenance, and intervention for legacy systems |
|  |  | Encryption |
|  |  | Password management system |
|  |  | Locks (offices, storefront, warehouse) |
|  |  | Closed-circuit television (CCTV) surveillance |
|  |  | Fire detection/prevention (fire alarm, sprinkler system, etc.) |

**Compliance checklist**

Payment Card Industry Data Security Standard (PCI DSS)

| **Yes** | **No** | **Best practice** |
| --- | --- | --- |
|  |  | Only authorized users have access to customers’ credit card information. |
|  |  | Credit card information is stored, accepted, processed, and transmitted internally, in a secure environment. |
|  |  | Implement data encryption procedures to better secure credit card transaction touchpoints and data. |
|  |  | Adopt secure password management policies. |

General Data Protection Regulation (GDPR)

| **Yes** | **No** | **Best practice** |
| --- | --- | --- |
|  |  | E.U. customers’ data is kept private/secured. |
|  |  | There is a plan in place to notify E.U. customers within 72 hours if their data is compromised/there is a breach. |
|  |  | Ensure data is properly classified and inventoried. |
|  |  | Enforce privacy policies, procedures, and processes to properly document and maintain data. |

System and Organizations Controls (SOC type 1, SOC type 2)

| **Yes** | **No** | **Best practice** |
| --- | --- | --- |
|  |  | User access policies are established. |
|  |  | Sensitive data (PII/SPII) is confidential/private. |
|  |  | Data integrity ensures the data is consistent, complete, accurate, and has been validated. |
|  |  | Data is available to individuals authorized to access it. |

### **Recommendations**

### **Controls Assessment Recommendations**

Ensure all users have minimum necessary access, regularly update permissions, and implement comprehensive disaster recovery plans. Enforce robust password policies and multi-factor authentication. Establish clear separation of duties, configure and update firewalls, and deploy an intrusion detection system. Implement regular backups, deploy up-to-date antivirus software, and manually monitor legacy systems. Use encryption for sensitive data and a password management system, and maintain physical security measures including locks, CCTV surveillance, and fire detection systems.

### **Compliance Recommendations**

Authorize only necessary access to credit card information, secure storage and processing environments, and implement data encryption for PCI DSS compliance. Enforce secure password management and ensure E.U. customer data privacy with a breach notification plan as per GDPR. Classify and inventory data accurately, and enforce comprehensive privacy policies. Establish user access policies, ensure data confidentiality and integrity, and maintain data availability to comply with SOC standards.