assessment checklist

| **Administrative Controls** | | | |
| --- | --- | --- | --- |
| **Control name** | **Control type and explanation** | **Needs to be implemented**  **(X)**  **Already implemented ( )** | **Priority** |
| Password policies | Preventative; establish password strength rules to improve security/reduce likelihood of account compromise through brute force or dictionary attack techniques |  |  |
| Manual Monitoring for legacy systems | Preventive; Refers to the process of actively overseeing old systems |  |  |
| Disaster Recovery Plan | Corrective; A strategy that outlines how recover from a disruptive event |  |  |
| Least Privilage | Preventive; A policy-driven practice that ensures only the needed access will be granted to authorized people. |  |  |
| Separation of Duties | Preventive; Distributes access in a way that avoids the centralization of power in one individual |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Technical Controls** | | | |
| **Control Name** | **Control type and explanation** | **Needs to be implemented**  **(X)**  **Already implemented ( )** | **Priority** |
| Intrusion Detection System (IDS) | Detective; allows IT team to identify possible intrusions (i.e., anomalous traffic) quickly |  |  |
| Encryption | Deterrent; makes confidential information/data more secure (i.e., website payment transactions) |  |  |
| Network Firewall | Preventive; Protects a network from unauthorized acces by monitoring and controlling network traffic. |  |  |
| Antivírus Software | Preventive, Detective and Corrective; Software used to prevent, detect and eliminate malware and viruses. |  |  |
| Backup | Corrective control; Prevent permanent data loss by saving copies. |  |  |
| Password management system | Preventive; A tool that helps protect, acess and manage passwords |  |  |
| Disabling unused ports | Before an incident occurs, to prevent malicious  actors from entering the network through the  open port. Can be used after an incident to  prevent future attacks from happening  through unused open ports |  |  |
| Multifactor authentication (MFA) | Can help protect against brute force attacks  and similar security events. MFA can be  implemented at any time, and is mostly a  technique that is set up once then maintained. |  |  |
| Network log analysis | Can be configured to alert the security team  when there is abnormal traffic on the network.  This can be used either before an incident  occurs, during to track network traffic, and can  be configured in the response of a  cybersecurity attack. A common tool used for  analyzing network logs is a SIEM. |  |  |
| Patch updates | Patch updates often contain fixes to security  problems. It is important to keep systems up to  date with the latest security patches because  attackers will be alerted to the security  vulnerability when patches are released. |  |  |
| Penetration test (pen test) | Pen tests are used to protect and prevent  against potential attacks. |  |  |
| Port filtering | Port filtering is used to control network traffic  and can prevent potential attackers from  entering a private network. |  |  |
|  |  |  |  |
|  |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Physical Controls** | | | |
| **Control Name** | **Control type and explanation** | **Needs to be implemented**  **(X)**  **Already implemented ( )** | **Priority** |
| Closed-circuit television (CCTV) surveillance | Preventative/detective; can reduce risk of certain events; can be used after event for investigation |  |  |
| Locks | Preventative; physical and digital assets are more secure |  |  |
| Fire Dectetion | Preventive; Provides early warnings of fire hazards that could disrupt or damage assets |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Compliance Checklist** | | | |
| **Compliance Name** | **Explanation** | **Needs to be implemented**  **(X)**  **Already implemented ( )** | **Priority** |
| Payment Card Industry Data Security Standards (PCI DSS) | A set of security standards designed to ensure the correct handling of credit card information and payment data |  |  |
| General Data Protection Regulation (GDPR) | Privacy and data regulation implemented by the European Union. |  |  |
| System and Organizations Controls (SOC Type1, SOC Type 2) | Developed by American Institute of Certified Public Accountants, they are used to evaluate internal controls and pratices of organizations providing services to third parties. |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |