Controls and compliance checklist

Scenario: Perform a controls and compliance assessment for the fictitious Company X.

Scope: The scope of this audit is defined as the entire security program at Company X. This includes their assets like employee equipment and devices, their internal network, and their systems.

Company X's Security Posture:

- Currently, all Company X employees have access to internally stored data and may be able to access cardholder data and customers' PII/SPII.
- Encryption is 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.
- Access controls pertaining to least privilege and separation of duties have not been implemented.
- The IT department has ensured availability and integrated controls to ensure data integrity.
- The IT department has a firewall that blocks traffic based on an appropriately defined set of security rules.
- Antivirus software is installed and monitored regularly by the IT department.
- The IT department has not installed an intrusion detection system (IDS).
- There are no disaster recovery plans currently in place, and the company does not have backups of critical data.
- The IT department has established a plan to notify E.U. customers within 72 hours if there is a security breach. Additionally, privacy policies, procedures, and processes have been developed and are enforced among IT department members/other employees, to properly document and maintain data.
- Although a password policy exists, its requirements are nominal and not in line with current minimum password complexity requirements (e.g., at least eight characters, a combination of letters and at least one number; special characters).

- There is no centralized password management system that enforces the password policy's minimum requirements, which sometimes affects productivity when employees/vendors submit a ticket to the IT department to recover or reset a password.
- While legacy systems are monitored and maintained, there is no regular schedule in place for these tasks and intervention methods are unclear.
- The store's physical location, which includes Company X's main offices, store front, and warehouse of products, has sufficient locks, up-to-date closed-circuit television (CCTV) surveillance, as well as functioning fire detection and prevention systems.

Controls assessment checklist

Yes	No	Control
	X	Least Privilege
	X	Disaster recovery plans
	X	Password policies
	X	Separation of duties
✓		Firewall
	X	Intrusion detection system (IDS)
	X	Backups
✓		Antivirus software
	X	Manual monitoring, maintenance, and intervention for legacy systems
	X	Encryption
	X	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
	X	Only authorized users have access to customers' credit card information.
	X	Credit card information is stored, accepted, processed, and transmitted internally, in a secure environment.
	X	Implement data encryption procedures to better secure credit card transaction touchpoints and data.
	X	Adopt secure password management policies.

General Data Protection Regulation (GDPR)

Yes	No	Best practice
	X	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.
	X	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
	X	User access policies are established.
	X	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.

Risk score:

The risk score for Company X is a 7, out of 10. This score results from the absence of critical security controls and not adhering to compliance best practices.

Recommendations:

- Password policies exist but are insufficient and must be updated to provide desired protections.
- Monitoring and maintenance of legacy systems needs to be conducted according to an established schedule.
- The intervention process when dealing with legacy systems needs to be clearly defined.
- Sensitive data (PII & SPII) needs to be restricted to only those who need it to perform their job/tasks.
- Encryption should be implemented for data in-use and at-rest to ensure confidentiality.
- Other controls that need to be implemented include least Privilege, disaster recovery plans, separation of duties, an IDS, legacy system management, and a password management system.