Controls and compliance checklist

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.(meaning only those authorized)

A set of controls that would help if applied:

- Apply the principle of Least Privilege so that employees will be granted access to the data only if they need it to perform their tasks.
- Preparing Disaster recovery plans to be able to ensure the recovery phase of the NIST framework and get back the assets to normal state after being damaged .
- Implement Password policies that would at least be in line with the current minimum password complexity requirements which is at least 8 characters, a mix of letters and one number in minimum and a special character.
- Control access to the company's data while pertaining to separation of duties. And that's by granting access to different types of data to different types of employees so that the damage will be minimal in case of a data breach.

- Invest in new IDS/IPS to detect and prevent from threats.
- Maintain backups of data to restore it in case of a data breach.
- Maintaining a plan to manage legacy systems on a regular basis and document step–by-step intervention methods.
- Use string encryption ciphers to protect sensitive data and maintain data integrity.
- Set up a password management system to reduce password fatigue.

Compliance best practices to implement:: dfvgrgd

- Make sure only authorized users h ave : : : ::::re^fmg$^lgfdaccess to customer's sensitive data to meet the confidentiality principle of the CIA triad.
- Set up encryption to secure data and meet the data integrity policies.
- Enforce preventative password policies to reduce the prospect of account compromise through brute force attacks.
- Better handle assets management by creating assets

inventories through the identify process of the NIST CSF and then make sure assets are well classified and the impact of loss of each is documented and maintained.