Controls and Compliance Checklist

This checklist helps us to evaluate the current security controls in SafeInvest, using the simple "Yes" and "No" indicators (with "✓") to reflect the current state of controls, along with brief explanations to provide context and clarify any gaps.

The key question we ask for each control is: **Does SafeInvest currently have this control in place?**

Yes	No	Control	Explanation
	✓	**Least Privilege**	Many employees currently have unrestricted access to sensitive data. Enforcing strict, role-based access controls will help mitigate the risk of unauthorized exposure.
	✓	**Disaster Recovery Plans**	There are no formal disaster recovery plans presently, leaving the business unprepared for major disruptions. Setting up a clear, actionable plan in place is key to maintaining operations during and after an incident.
	✓	**Password Policies**	The current password requirements are minimal and do not meet industry best practices, increasing the risk of unauthorized access through weak or guessable passwords.
	✓	**Separation of Duties**	Key operational responsibilities are handled by the same employees without clear segregation, which can lead to accidental mistakes or increase the risk of misuse or fraud. Implementing proper task segregation would help reduce those risks.
✓		**Firewall**	The existing firewall is properly configured to block unwanted or malicious traffic according to defined security rules.
	✓	**Intrusion Detection System (IDS)**	The absence of an Intrusion Detection System (IDS) means suspicious activity may go undetected, limiting the organization’s ability to spot and respond to threats in real time.
	✓	**Backups**	Basic backup routines are in place, but there is no defined recovery strategy to guarantee that critical data can be quickly restored after a breach or system failure.
✓		**Antivirus Software**	Antivirus and endpoint protection tools are in place and monitored to identify known threats.
	✓	**Manual Monitoring & Maintenance for Legacy Systems**	Legacy systems are still in use, but they are not maintained regularly and lack clear support procedures, which increases their exposure to security vulnerabilities.

Yes	No	Control	Explanation
	✓	**Encryption**	Some areas, like cloud storage and transaction logs, still lack proper encryption, which exposes sensitive data to unnecessary risk.
	✓	**Password Management System**	Without a centralized password manager, users rely on manual resets and inconsistent practices, which can slow down operations and weaken password security.
✓		**Physical Locks**	Physical access to offices and sensitive areas is controlled through secure locking systems to prevent unauthorized entry.
✓		**CCTV Surveillance**	Surveillance cameras are placed in strategic locations to monitor physical access points and act as a deterrent to unauthorized activity.
✓		**Fire Detection & Prevention**	Fire alarms, sprinkler systems, and other fire detection measures are installed to protect physical assets and safeguard people and protect key assets in the event of an emergency.

This checklist evaluates SafeInvest's compliance with key cybersecurity frameworks: ISO 27001:2022, UAE Central Bank Regulations, PCI-DSS, and SOC 2. Each requirement is marked as either met (✓), unmet (❌), or partially met (⚠) with explanations and next steps.

ISO 27001:2022

Status	Best Practice	Explanation / Next Steps
❌	Maintain a comprehensive asset inventory and classification process.	The current asset inventory is missing key digital resources and lacks proper classification. A structured process is needed to document all assets and categorize them based on their criticality and compliance requirements.
❌	Enforce a robust access control policy (role-based access and least privilege).	Access privileges are not consistently enforced. Introduce a centralized access control solution to ensure that employees only have access to resources required for their roles, and a need-to-know can access critical systems.
⚠	Review and update the Information Security Policy regularly.	While there is a security policy in place, but has not been consistently updated to reflect new threats or changes in operations. To stay aligned with business and regulatory demands, a bi-annual review should be done to keep the policy relevant and aligned with current risks and compliance needs.

Status	Best Practice	Explanation / Next Steps
⚠	Provide ongoing security awareness training for all employees.	Employee security training happens only occasionally and does not cover key risk areas, a consistent training schedule, with phishing tests and real-world simulations would go a long way in boosting awareness and minimizing human error.
⚠	Regularly review and update the Incident Response and Business Continuity plans	While response plans are documented, they are not routinely tested. Running periodic tabletop exercises and simulations and using insights from those tests to update the plans will ensure the organization stays prepared for actual incidents.

UAE Central Bank Information Security Regulations

Status	Best Practice	Explanation / Next Steps
❌	Ensure compliance with data localization and retention requirements	The current data storage policies are not fully aligned with the UAE Central Bank regulatory requirements. Implement documented policies covering data localization, storage, and retention. These policies should be reviewed regularly to ensure they stay up to date with regulatory changes.
❌	Implement regular cybersecurity reporting to the board and regulatory authorities	Presently, there is no consistent reporting structure for cybersecurity. Setup a structured, quarterly reporting schedule, and provide detailed risk reports, incident summaries, and compliance updates to senior management and regulators.
⚠	Integrate a formal vendor and third-party risk management process	Currently, vendor assessment lack a structured approach, making it difficult to ensure consistent oversight. Introducing a formal vendor risk management program process with scheduled security assessments, due-diligence checks, well defined SLAs, and continuous monitoring of vendor performance.
❌	Perform periodic independent cybersecurity audits	At the moment, audits are only conducted internally. Engaging an external cybersecurity auditor on an annual basis can provide independent verification of our security controls, strengthen regulatory compliance, and highlight areas for improvement from a fresh perspective.

Payment Card Industry Data Security Standard (PCI DSS)

Status	Best Practice	Explanation / Next Steps
❌	Only authorized users have access to customers' credit card information	Access to sensitive cardholder data spans too many departments. To mitigate risk, adopt a strict role-based access model that ensures only authorized personnel, based on job function can access payment data.
⚠	Credit card data must be processed, transmitted, and stored in a secure environment	While some systems adhere to secure standards, the approach is inconsistent. Unify and enforce secure configurations across all payment channels, ensuring that data is transmitted over TLS/SSL and stored to comply with PCI-Standards.
❌	Implement robust data encryption for all payment channels and storage systems	Encryption controls are uneven across systems. Deploy end-to-end encryption protocols (both in transit and at rest) for all payment data, ensuring sensitive information is never stored in plaintext.
❌	Conduct regular vulnerability scans and penetration tests	No defined schedule exists for security testing. Implement quarterly vulnerability scans and conduct annual penetration tests to uncover and remediate security weaknesses before they are exploited.
⚠	Enforce network segmentation for payment processing systems	There is partial segregation between payment and other systems, but it needs to be more robust and consistently enforced. Strengthening segmentation will minimize the risk of lateral movement in the event of a breach.

SOC 2

Status	Best Practice	Explanation / Next Steps
❌	Establish and document a vendor risk management program	The current approach to evaluating third-party risk assessments varies and lacks structure. Implement a clear, documented process that includes thorough onboarding checks, regular security audits and contractual obligations to ensure third parties meet SOC 2 requirements and minimizes the risk introduced by external partnerships.
⚠	Maintain a rigorous change management process	Change management processes exist but vary across departments. It is important to develop a unified and well-documented change management process in place with clear approval paths, ensure updates are controlled, and minimize risks during system updates or new deployments.
❌	Conduct comprehensive internal audits and regular security training programs	Internal audits and employee security training are currently ad hoc and not part of a structured program. To strengthen compliance and security culture, implement a regular audit schedule and introduce continuous, role-specific training.

Status	Best Practice	Explanation / Next Steps
		This should include awareness workshops, phishing simulations, and a recurring security training program for all employees.
⚠	Implement robust monitoring and logging with proper retention policies	While monitoring tools are in place, audit logs are not retained or reviewed consistently. Set clear policies for log retention, periodic review, and integrate these logs into a centralized SIEM for improved visibility and incident response. This will enhance threat detection, improve response times, and provide a clear audit trail for compliance reviews.