PORTFOLIO ACTIVITY
SECURITY AUDIT:
CONTROLS AND COMPLIANCE CHECKLIST FOR BOTIUM TOYS

PART ONE: CONTROL ASSESSMENT CHECKLIST

CONTROL	YES/NO	EXPLANATION/COMMENTS
1. Least privilege	No	Currently all employees have access to sensitive data including customer data.
2. Separation of duties	No	No separation of duties for critical roles, ensuring data handling is limited to authorized personnel
3. Multi factor authentication	No	Multi factor authentication is not implemented on critical accounts
4. Encryption	No	Encryption is not currently implemented, to ensure confidentiality of customer's data including credit card information
5. Password policy	No	Employee password requirement are minimal and lacks complexity which would give a threat actor easy access to data or other assets
6. Password management system	No	No system to enforce password policy or handle resets securely
7. Intrusion Detection System (IDS)	No	No IDS in the place, leaving the network vulnerable to undetected breaches
8. Firewall	Yes	The firewall rules are appropriately defined and maintained
9. Antivirus protection	Yes	Antivirus is installed and monitored regularly
10. Legacy system	No	Legacy system are monitored

monitoring		but lack regular maintenance
11. Data backup and Recovery	No	No disaster recovery plan or data backup in place
12. Physical security	Yes	CCTV Fire detection and physical access controls are sufficient

RECOMMENDATION TO CONTROL ASSESSMENT CHECKLIST

CONTROL	RECOMMENDATION
1. Least privilege	Ensure employees only have access to data and systems essential to their roles, minimizing exposure to sensitive data
2. Separation of duties	Divide responsibilities among multiple employees to prevent conflict of interest, unauthorized access or data misuse
3. Intrusion Detection System (IDS)	Deploy all IDS to monitor network traffic and detect potential breaches on time
4. Encryption	Encryption to all sensitive data both in transit and at rest to prevent unauthorized access
5. Password policy	Enforce a strong password policy requiring a mix of uppercase, lowercase, numbers, special characters and regular change
6. Password management system	Implement a centralized password manager to enforce policies, simplify password resets and reduce downtime
7. Disaster Recovery plan	Develop and regularly test a data recovery plan to ensure business continuity and data recovery in the event of a breach or system failure
8. Legacy system management	Establish a regular monitoring and maintenance schedule for legacy system, with clear intervention protocols to mitigate vulnerabilities

COMPLIANCE ASSESSMENT CHECKLIST

Compliance Best practices in line with GDPR AND PCI DSS

GDPR - General Data Protection Regulation

PCI DSS - Payment Card Industry Data Security Standard

COMPLIANCE REQUIREMENT	YES/NO	BEST PRACTICES
1. PCI DSS- Data Encryption	No	Customer payment data is unencrypted. Data encryption should be implemented for both data in transit and data at rest
2. PCI DSS- Access controls	No	No role based access control, implement least privilege and restrict sensitive data access
3. PCI DSS- Vulnerability scanning	No	No schedule vulnerability scans. Quarterly scanning should be conducted and annual penetration testing should be done
4. PCI DSS- Password management policies	No	Password policies are nomimal and no password management system is currently in place. Secure password and management policies should be adopted
5. GDPR- Breach notification(72 hours)	Yes	E.U breach notification on plan exists, but staff needs additional training on response actions
6. GDPR- Data Access/Erasure Requests(DSAR)	No	No defined process for handling access or erasure requests. A streamlined DSAR workflow should be created
7. GDPR- Data protection Impact Access (DPIA)	No	Data protection impact assessment not conducted. A process should be implemented to access risks to data privacy
8. GDPR- Data minimization	No	Excessive data is collected without clear purpose. Limit data collection to essential information only
9. GDPR- Data Encryption	No	E.U personal data remains unencrypted. Ensure encryption on all stored and transmitted personally identifiable information (PII) .

COMPLIANCE CHECKLIST RECOMMENDATIONS

1. Conduct a Data Protection Impact Assessment (DPIA) : Regularly evaluate and mitigate data privacy risks, ensuring GDPR compliance

2. Define a data access/erasure process: Build a clear documented DSAR process to handle customer data access and deletion requests efficiently

3. Achieve PCI DSS compliance: Encrypt cardholder data, restrict access, and implement routine vulnerability scans to safeguard financial transactions

4. Implement Data minimization: only collect essential customer data, avoid storing unnecessary sensitive information to reduce exposure

5. Strengthen GDPR compliance: Ensure E.U data is fully encrypted, refine breach notification plans and conduct regular Data Protection Impact Assessment(DPIA) to stay compliant