Control Identifier	Control Name	Fullfilled Y/N	Requirements	Item	Details	Comment
1	**Risk Accessment**	N	At least one subitem, preference and priority as the order from 1.1 to 1.4	1.1	Latest Security Compliance certificate such as ISO 27001, SOC2, software development	No ISO/SOC2, pen test/VA, or risk/privacy analysis provided in Bizkit architecture.
				1.2	Latest Red Team/Pen-test/VA San result with remediations completed for all Highs and Mediums	
				1.3	Risk/Privacy Impact Analysis with controls desgined, implemented or with schedules (new project)	
				1.4	Successful incidident dectections in MITRE categories and related security control implemented	
2	**Information Classification & Controls**	N	All subitems	2.1	Soluction Architecture Diagrams (SAD), Refer Worksheet 2	Architecture diagram present but no Information Classification Diagram (ICD); control requires both.
				2.2	Information Classification Diagram (ICD), Refer Worksheet 2	
3	**Data in Use, At Rest and In Transit**	Y	Internal or above	3A	Access Control - Authentication (accounts) and Authourization (roles and permissions)	Meets data protections: HTTPS/TLS 1.2+, Azure AD/Managed Identity for access, SQL TDE at rest.
			Confidential or above	3B	Least information shown, Masking, Tokenization and Encyption	
				3.1	In use - 3A & 3B used in solution interface (GUI)	
				3.2	At rest - 3A & 3B, especiall for files exported & database Encrypted	
				3.3	In trasit - 3A & 3B, especially transfer between different security zones/networks	
4	**Key Management**	N			Key Generation, Distribution, Storage, Usage, Rotation, Revocation and Destruction	Key Vault/TDE noted but no key audit trails or quarterly key review evidence.
				4.1	Audit Trials is enabled and logged	
				4.2	4.1 is reviewed at least quarterly	
				4.3	The master encryption key should not leave the security storage through its service life	
5	**Account Management**	N	All subitems	5.1	Solution default user account roles and capabilities (system function an be performed)	No roles list, password policy, or MFA posture for users/privileged/service accounts.
			Refer Worksheet 5	5.2	Password for privilege accounts, service accounts and user accounts comply with policy	
				5.3	MFA for all users if solution is public facing. Otherwise, MFA at least to privilege accounts	
6	**Unsuccessful Logon Attemps**	N		6.1	Lockout and timeout comply with policy	No lockout/timeout configuration or monitoring evidence for unsuccessful logons.
				6.2	Privilege account lockout being monitored and handled such as notification and remediation records. Exmaples inlcude system records, emails, signed reports, etc	
7	**Privilege Account Review**	N	All subitems			No privileged RBAC listing, periodic access review, or change approvals provided.
				7.1	System pre-built RBAC AND/OR Permissions	
				7.2	Customized RBAC AND/OR Permissions	
				7.3	List of user accounts with roles assigned and owners	
				7.4	Account access review record	
				7.5	Change requests and approval records for account created, changed, disabled and deleted.	
8	**User Account Review**	N	All subitems			No user/role listings or periodic access review records provided.
				8.1	System pre-built RBAC AND/OR Permissions	
				8.2	Customized RBAC AND/OR Permissions	
				8.3	List of user accounts with roles assigned and owners	
				8.4	Account access review record	
				8.5	Change requests and approval records for account created, changed, disabled and deleted.	
9	**Remote Access**	N				No evidence of MFA/2FA for public-facing services or confirmation admin module is non-public.
				9.1	2FA for public facing services	
				9.2	No public facing for admin module	
10	**System Hardening**	N				No hardening baseline/benchmark (e.g., CIS) evidence for App Service/SQL/OS.
				10	Industry standard or least JEC hardening guideline	
11	**Security Control Assessment**	N	At least 11.1 to 11.3			No patch schedule/execution logs, vulnerability scan results, or pen-test with remediation.
				11.1	Regular patching records such as schedules, exectuion, patch applied	
				11.2	Regular vulnerability scanning and remediation records	
				11.3	Latest pen-test and remediation records	
				11.4	Records of configuration scanning and misconfiguration remediated	
12	**System Documentation and User Manuals**	Y	Necessary 12.1			System architecture/security design is provided; user manuals not supplied (12.1 satisfied).
				12.1	Latest system documentation set (system and user)	
				12.2	Access controls and access records of system documenation, program source codes and related resources	
13	**Training & Records**	N				No security awareness/training records included.
				13.1	Any security awareness related training to user such as accounts managements, security risk in systems (1.1) and risk handling such as incidents reporting.	
				13.2	Training records	
14	**Data Backup**	N	All subitems			Backups every 24h, 7-day retention stated; missing execution logs, access control, and offline copy.
				14.1	Screen capture of regular backup schedule	
				14.2	Logs or reports of backup execution records	
				14.3	Backup retained in required period	
				14.4	Access control of backup acccess and restoration	
				14.5	Offline backup available, at least when request	
15	**Restore Drill**	N	At least 15.1			No backup restore drill/test evidence.
				15.1	Provide supporting that back up and resotration working properly, such as in UAT or Production	
				15.2	If critical system, provide latest annual restore drill plan, result and reviewed record	
16	**BCP/DR Drills**	N	All subitems if critical			No DR drill plan, result, remediation, or review evidence.
				16.1	Latest DR drill plan	
				16.2	Latest DR drill result	
				16.3	Latest DR drill remediation	
				16.4	Latet DR drill review record	

17	**3rd Party / Vendor Management**	N			No supplier due diligence/compliance attestations or exit strategy evidence.
			17.1	Evulation results of vendor selection	
			17.2	Vendor complience certificate	
			17.3	Vendor's third party compliance certificates used in the soltuion or service provided.	
			17.4	Exit strategy in contract completion or termination	