Section Heading	Control Heading	Original ID	Question Text	Answer	Notes/Comment
Security Certifications		1	Which of the following is your company compliant with?	[1]	
		1.1	Please upload the document, if applicable and appropriate	[2]	
		2	Is there an information security management program that has been approved by management, communicated to appropriate constituents and an owner to maintain and review the program?		
		2.1	Does it include a risk management program? Please explain the risk assessment methodology followed in your organization.		
		2.1.1	Has a risk assessment been conducted during the last 12 months? Are findings tracked and remedied?		
		3	Do you have a third party/vendor management program in place?		
		3.1	Does it include risk management and ongoing oversight?		
		3.1.1	Please upload the document, if applicable and appropriate	[3]	
		4	Do you require third parties to sign Non-Disclosure Agreements (NDA)?		
		4.1	Please upload the document, if applicable and appropriate	[4]	
		5	Do you require third parties to sign Service Level Agreement (SLA)?		
		5.1	Please upload the document, if applicable and appropriate	[5]	
Information Security Policy		6	Please select all topics covered by company policies	[6]	
		6.1	Please upload all relevant policies for review. The [Your company] Information Security team may reach out to you for further discussion..	[7]	
		7	Are the policies reviewed and approved at least annually?		
		8	Is there an information security function/personnel responsible for security initiatives?		
		9	Is information classified based on its level of sensitivity?		
Data Handling		10	Are encryption mechanisms maintained for sensitive [Your company] data both in transit and at rest? Please describe.		
		11	Is [Your company] Data sent or received via physical media?		
		12	Is all media containing [Your company] systems and data securely disposed of to prevent recovery?		
		13	Is data segmentation and separation capability between clients provided?		
		14	Are backups of [Your company] Systems and Data performed? What is the retention period?		
		14.1	Are backups stored onsite or offsite?	[8]	
		14.1.1	For offsite, please provide the name of the subcontractor used.		
		14.1.2	For offsite, do you have a contract in place with the subcontractor?		
Human Resource Security		15	Are background checks performed for all employees and third parties?		
		16	Is there a disciplinary process for non-compliance to security policies, does it include termination or change of status process?		
		17	Is security awareness training provided to all employees at new hire and every year thereafter?		
Physical Security		18	Is there a physical security program? Please provide details.		
		19	Are physical security and environmental controls in place at the data center and office buildings?		
		20	Is there a visitor access process or procedure to allow visitors into the building?		
		21	Are visitors required to sign in and their IDs checked prior to permitting them to the building?		
		22	Are visitors required to be escorted at all times during their visit to the building?		
		23	Are data centers, Main Distribution Frame closets (MDFs) and other sensitive areas marked appropriately and access limited to only authorized users?		
Change Management		24	Is there an operational change management/change control program and process that has been approved by management, communicated to appropriate constituents and an owner to maintain and review the program?		
		24.1	Please upload the document, if applicable and appropriate	[9]	
		25	Is there a formal process to ensure clients are notified prior to changes being made which may impact their service?		
Identity & Access Management		26	Are user's credentials unique and is strong authentication such as Multifactor (MFA) required for remote access or access to sensitive information? Please explain		
		27	Do you enforce password (e.g., minimum length, age, history, complexity) and account lockout (e.g., lockout threshold, lockout duration) for all computing devices?		
		28	Is there a process which allows [Your company] to specifically list who from the provider will have access to their [Your company] Systems and Data?		
		29	Is there a process to de-provision users logical and physical access after employee termination?		
		30	Are user accounts (applications, Operating systems, computing devices, networking devices, privilege accounts) reviewed at-least quarterly?		
Infrastructure Security		31	Is there an anti-malware/Endpoint Security policy or program in place?		
		32	Is there a vulnerability management policy or program in place? Are all assets in scope scanned and at what frequency? Please explain		
		33	Are vulnerability scans performed on all internet-facing applications at least monthly and after significant changes?		
		34	Are network and application penetration tests performed?		
		34.1	What is the frequency?		
		35	Is there a patch management process for applications, systems, devices? Describe the patch management process.		
		35.1	Does the program define the timeline for patch deployment based on patch criticality?		
		36	Are default hardened base images applied to all operating systems?		
		37	Is there a threat management system in place? Please provide details.		
		38	Is there a Data loss prevention system in place? Does it cover Email and network etc.? Please explain		
		39	Is there an Intrusion detection and/or Intrusion Prevention system in place? Please name the tool.		
		40	While connecting remotely to the company network, does the system require a company approved and authorized Virtual Private Network (VPN) tool to connect?		
		40.1	Does the Virtual Private Network (VPN) tool require Multi Factor Authentication (MFA) for logging into the company network?		
Secure Software Development		41	Do you maintain a formal Software Development Lifecycle (SDLC)?		
		42	Are development, test, and staging environments separated?		
		43	Are change control procedures required for all application changes to the production environment?		
		44	Are [Your company] systems and data ever used in the development, test, or QA environments?		
		45	Are code reviews conducted for all software builds?		

		46	Are applications analyzed on a regular basis to determine their vulnerability against recent attacks?		
		47	Are vulnerability scans and penetration tests conducted on all production builds?		
		48	Are mobile applications developed for [Your company]?		
Endpoint Security		49	For endpoints, are security configuration and hardening standards documented?		
		50	For all endpoints, are sufficient details contained in Operating System and application logs to support incident investigation, including successful and failed login attempts and changes to sensitive configuration settings and files?		
		50.1	Are these logs protected against modification, deletion, and/or inappropriate access?		
		51	Are unauthorized external media devices (including mass storage devices) prohibited from connecting to the end points, servers and other computing devices?		
		52	Are exceptions documented, approved by senior management, and logged for audit purposes?		
		53	Is encryption required on authorized removable media?		
Network Security		54	Are security and hardening standards maintained for network devices, including Firewalls, Switches, Routers and Wireless Access Points (baseline configuration, patching, passwords, access control)?		
		55	Are logical and/or physical controls used to isolate critical and sensitive systems into network segments separate from network segments with less sensitive systems?		
		56	Are Intrusion Detection/Prevention Systems employed in all sensitive network zones and wherever firewalls are implemented?		
		57	Is information transmitted over public networks to the production infrastructure sent over cryptographically sound encrypted connections? (TLS, VPN, IPSEC, etc)?		
Fourth Party Security		58	Do agreements with fourth parties who have access or potential access to [Your company] Data, address confidentiality, audit, security, and privacy, including but not limited to incident response, ongoing monitoring, data sharing and secure disposal of [Your company]?		
		59	Is there a documented privacy policy or procedures for the protection of information transmitted, processed, or maintained on behalf of [Your company]?		
Incident Response		60	Is there an Incident Response Program that has been approved by management and communicated to constituents?		
		61	Is there a formal Incident Response Plan? Please provide details		
		61.1	Please upload the document, if applicable and appropriate	[10]	
		62	Is there a 24x7x365 staffed phone number available to [Your company] to report security incidents?		
Business Continuity and Disaster Recovery		63	Are formal business continuity procedures developed and maintained?		
		64	Is there a periodic (at least annual) review of your Business Continuity Program?		
		65	Is there a formal, documented exercise and testing program in place?		
		66	Are all suppliers of critical hardware, network services and facility services involved in annual continuity and recovery tests?		
		67	Is there a formal Disaster recovery plan and is the plan reviewed and tested annually? Please provide details		
		68	Are site failover tests performed at least annually?		
		69	Do contracts with Critical Service Providers include a penalty or remediation clause for breach of availability and continuity SLAs?		
		70	Is there sufficient redundancy capacity to ensure services are not impacted in multi-tenancy environments during peak usage and above?		
Compliance		71	Are client audits and assessments permitted?		
		72	Is there an internal audit, risk management, or compliance department, or similar management oversight unit with responsibility for assessing, identifying and tracking resolution of outstanding regulatory issues?		
		73	Are there policies and procedures to ensure compliance with applicable legislative, regulatory and contractual requirements including intellectual property rights on business processes or information technology software products?		
		74	Is there a records retention policy covering paper and electronic records, including email in support of applicable regulations, standards and contractual requirements?		

[1] Separate Options with semi-colon.

Options:
- F. SOC 3 (type 1, 2)
- G. HITRUST
- B. PCI DSS
- I. Privacy Shield
- A. ISO 2700x
- D. SOC 1
- H. SOX
- E. SOC 2
- C. SSAE 16
- Not Applicable

[2] You will be able to upload a file for this question through Whistic after importing.

[3] You will be able to upload a file for this question through Whistic after importing.

[4] You will be able to upload a file for this question through Whistic after importing.

[5] You will be able to upload a file for this question through Whistic after importing.

[6] Separate Options with semi-colon.

Options:
- B. Business Continuity
- N. Information Classification
- K. Remote access
- G. Communication
- C. Acceptable use
- A. Risk Management
- R. Security Awareness
- O. Encryption
- D. Access control
- J. Security incident & privacy event management
- L. Vulnerability management
- Q. e-commerce
- M. Mobile computing
- E. System and data handling
- I. Physical security
- H. Network security
- F. Disaster recovery
- P. Cloud computing
- Not Applicable

[7] You will be able to upload a file for this question through Whistic after importing.

[8] Separate Options with semi-colon.

Options:
- A. Offsite
- B. Onsite
- Not Applicable

[9] You will be able to upload a file for this question through Whistic after importing.

[10] You will be able to upload a file for this question through Whistic after importing.