Tavio IT Security Questionnaire

Section Heading	Question	Answer	Notes
Audit Reports	Is your organization certified against ISO 27001?	No	
	Does your organization have a SOC 2 report?	Yes	
Security Policy	Is there an Information Security Policy that has been approved by management, published and communicated to personnel?	Yes	
	Do all policies get assigned to an owner who is responsible for periodic review and approval?	Yes	
	Have all policies and standards been reviewed in the last 12 months?	Yes	
Cloud Hosting	Does Tavio use a Cloud Hosting Provider?	Yes	Tavio platform is hosted on AWS.
	Does the Cloud Hosting Provider provide independent audit reports for their cloud hosting services (e.g., Service Operational Control - SOC)?	Yes	
	Is the Cloud Service Provider certified by an independent third party for compliance with,domestic or international control standards e.g., the National Institute of Standards and Technology - NIST, the International Organization for Standardization - ISO?	Yes	
	Are default hardened base virtual images applied to virtualized operating systems?	Yes	
Server Security	Are Servers used for transmitting, processing or storing Client data?	Yes	
	Are server security configuration standards documented and based on external industry or vendor guidance?	Yes	
	Are server security configuration reviews performed regularly to validate compliance with documented standards?	Yes	
	Are all servers configured according to security standards as part of the build process?	Yes	
	Are all unnecessary/unused services uninstalled or disabled on all servers?	Yes	
	Are vendor default passwords removed, disabled or changed prior to placing any device or system into production?	Yes	
	Is sufficient detail contained in operating system and application logs to support security incident investigations (at a minimum, successful and failed login attempts, and changes to sensitive , configuration settings and files)?	Yes	
	Are all systems and applications patched regularly?	Yes	
	Are there any Operating System versions in use within the Client Services that no longer have patches released?	No	
	Are Windows servers used as part of the Client Services?	No	
	Is Unix or Linux used as part of the Client services?	Yes	
	Are users required to 'su' or 'sudo' into root?	Yes	
Network Security	Is there a policy that defines Network Security requirements that is approved by management, communicated to personnel and has an owner to maintain and review?	Yes	
	Do network devices deny all access by default?	Yes	
	Do the firewalls have any rules that permit 'any' network, sub network, host, protocol or port on any of the firewalls (internal or external)?	No	
	Is there a policy that defines the requirements for remote access from external networks to networks containing Client Systems and Data that has been approved by management and communicated to personnel?	Yes	
	Are encrypted communications required for all remote network connections from external networks to networks containing Client Systems and Data?	Yes	
	Is remote administration of organizational assets approved, logged, and performed in a manner that prevents unauthorized access for personnel?	Yes	
	Are encrypted communications required for all remote system access?	Yes	
	Are Network Intrusion Detection capabilities employed?	Yes	
	Is there a DMZ environment within the network that transmits, processes or stores Client Systems and Data?	Yes	
	Are wireless networking devices connected to networks containing Client Systems and Data?	No	
Threat Management	Is there an anti-malware policy or program that has been approved by management, communicated to appropriate personnel and an owner to maintain and review the policy?	Yes	
	Does the anti-malware policy or program include defined operating systems that require antivirus?	Yes	
	Is there a Vulnerability Management Policy that has been approved by management, communicated to appropriate constituent and an owner assigned to maintain and review the policy?	Yes	
	Are network vulnerability scans performed against internal networks and systems?	Yes	
	Are network vulnerability scans performed against internet-facing networks and systems?	Yes	
	Do network vulnerability scans occur at least quarterly?	Yes	
	Do you deliver software, firmware, and/or BIOS updates to clients through automatic downloads (e.g., Windows Update, LiveUpdate)?	Yes	
End User Device Security	Are end user devices (desktops, laptops, tablets, smartphones) used for transmitting, processing or storing Client Data?	No	
	Are end user device security configuration standards documented?	Yes	
	Are defined procedures in place to identify and correct systems without anti-virus at least weekly for all end user devices	Yes	
	Are personnel allowed to utilize mobile devices within your environment?	No	
	Can personnel access corporate e-mail using mobile devices?	Yes	
	Are personal computers (PCs) used to transmit, process or store Client Systems and Data.	No	
	Are non-company managed PCs used to connect to the company network?	Yes	- MFA is enforced on all user accounts - An access request is needed to get permissions to connect - Connecting to any production instance triggers an alert
	Is there an Access Control program that has been approved by management, communicated to personnel and an owner to maintain and review the program?	Yes	
	Are personnel able to access Client Data?	Yes	- As a managed integration service, our support personnel are authorized to access Client data - The Services Team can temporarily have access to data during the implementation phase
	Are clients allowed to manage access to their own systems and data?	Yes	Clients can have full control over their own environment
	Are unique IDs required for authentication to applications, operating systems, databases and network devices?	Yes	
	Is there a process to request and receive approval for access to systems transmitting, processing or storing Client Systems and Data?	Yes	
	Is access to applications, operating systems, databases, and network devices provisioned, according to the principle of least privilege?	Yes	
	Is there segregation of duties for granting access and approving access to Client Systems and Data?	Yes	

Access Control	Is there segregation of duties for approving and implementing access requests for Client Systems and Data?	Yes	
	Is access to systems that store or process Client data limited?	Yes	
	Is there a Password policy for systems that transmit, process or store Client systems and data that has been approved by management, communicated to personnel, and enforced on all platforms and network devices?	Yes	
	Does the Password policy define specific length and complexity requirements for passwords?	Yes	
	Are complex passwords required on systems transmitting, processing, or storing Client data e.g. mix of upper-case letters, lower case letters, numbers, and special characters?	Yes	
	Does the Password policy define requirements for provisioning and resetting passwords?	Yes	
	Does the Password policy require keeping passwords confidential?	Yes	
	Does the Password policy prohibit users from sharing passwords?	Yes	
	Are user IDs and passwords communicated/distributed via a secure process?	Yes	Sensitive information is shared via a secret management platform
	Is Multi-factor Authentication deployed?	Yes	
	Does system policy require terminating or securing active sessions when finished?	Yes	
	Does system policy require logoff from terminals, PC or servers when the session is finished?	Yes	
	Is there a process for reviewing access?	Yes	
	Are user access rights reviewed periodically?	Yes	
	Are privileged user access rights reviewed at least quarterly?	Yes	
	Are access rights reviewed when a constituent's role changes?	Yes	
	Are inactive Constituent user IDs disabled and deleted after defined periods of inactivity?	Yes	
Risk Management	Is there a formalized risk governance plan that defines the Enterprise Risk Management program requirements?	Yes	
	Does the risk governance plan include risk management policies, procedures, and internal controls?	Yes	
	Does the risk governance plan include range of assets to include: people, processes, data and technology?	Yes	
	Is there a formalized Risk Assessment process that identifies, quantifies, and prioritizes risks based on the risk acceptance levels relevant to the organization?	Yes	
	Is there a process to identify and manage the risk response and treatment of risks?	Yes	
	Do vendors have access to Client systems and data or processing facilities?	Yes	AWS hosts our infrastructure but has no access to Client data.
Asset and Information Management	Is there an Asset Management program approved by management, communicated to personnel and an owner to maintain and review?	Yes	
	Is there an asset Inventory list or configuration management Database (CMDB)?	Yes	
	Is there an Acceptable Use policy for information and associated assets that has been approved by management, communicated to appropriate personnel, and assigned an owner to maintain and periodically review the policy?	Yes	
	Is there a process to verify return of personnel assets (computers, cell phones, access cards, tokens, smart cards, keys, etc.) upon termination?	Yes	
	Is Information classified according to legal or regulatory requirements, business value, and sensitivity to unauthorized disclosure or modification?	Yes	
	Is an owner assigned to all Information Assets?	Yes	
	Are owners responsible to approve and periodically review access to Information Assets?	Yes	
	Is there a policy or procedure for Information Handling (storing, processing, and communicating) consistent with its classification that has been approved by management, communicated to appropriate personnel and assigned an owner to maintain and periodically review?	Yes	
	Does the policy or procedure for Information Handling include encryption requirements?	Yes	
	Is Client Data sent or received electronically?	Yes	
	Is all Client Data sent or received electronically encrypted in transit while outside the network?	Yes	
	Do scans performed on incoming and outgoing email include phishing prevention?	Yes	
	Are Client systems or data stored or transferred in cloud-based public file sharing solutions?	No	
	Is regulated or confidential Client Data stored in a database?	Yes	Configurations and credentials are stored in a database
	Is regulated or confidential Client Data stored in files?	Yes	Data files are encrypted and stored in a private bucket associated to the customer environment
	Is data encrypted at rest?	Yes	AES256 Volume Encryption
	Is data encrypted in transit?	Yes	TLS 1.2 or higher. SFTP FIPS compliant ciphers.
	Are encryption keys managed and maintained for Client Data?	Yes	
	Are encryption keys generated in a manner consistent with key management industry standards?	Yes	
Human Resource Security	Are Human Resource policies approved by management, communicated to personnel and an Security owner to maintain and review?	Yes	
	Do Human Resource policies include Constituent background screening criteria?	Yes	
	Does Constituent background screening criteria include Criminal screening?	Yes	
	Are personnel required to attend security awareness training?	Yes	
	Does the security awareness training program include an explanation of personnel' security roles and responsibilities?	Yes	
	Does the security awareness training program include new hire and annual participation?	Yes	
	Does the Human Resource policy include a disciplinary process for non-compliance?	Yes	
	Does the Human Resource policy include Termination and/or change of status processes?	Yes	
	Is electronic access to systems containing Client data removed within 24 hours for terminated personnel?	Yes	
IT Operations Management	Are management approved operating procedures utilized?	Yes	
	Do changes to the production environment including network, systems, application updates, and code changes subject to the change control process?	Yes	
	Does the change control process include a formal process to ensure clients are notified prior to changes being made which may impact their service?	Yes	
	Does the change control process include a scheduled maintenance window?	Yes	
	Does the change control process include a scheduled maintenance window which results in client downtime?	-	Routine maintenance of the integration platform typically does not impact customer integration processes. In the event that downtime is anticipated, advance notification will be provided.
	Are Information security requirements specified and implemented when new systems are introduced, upgraded, or enhanced?	Yes	Utilizing an Infrastructure as Code (IaC) process ensures that our baseline security configuration is automatically applied whenever an infrastructure component is upgraded or added.
	Are new, upgraded or enhanced systems required to include a determination of security requirements based on the sensitivity of the data?	Yes	
	Do systems and network devices utilize a common time synchronization service?	Yes	
	Are applications used to transmit, process or store Client Data?	Yes	
	Are outside development resources utilized?	No	

Application Security	Are web applications configured to follow best practices or security guidelines (e.g., OWASP)?	Yes	
	Are Client Systems and Data used in the test, development, or QA environments?	No	
	Does the application change management/change control process include change control procedures required for all changes to the production environment?	Yes	
	Does the application change management/change control process include testing prior to deployment?	Yes	
	Does the application change management/change control process include stakeholder communication and/or approvals?	Yes	
	Does the application change management/change control process include documentation for all system changes?	Yes	
	Does the application change management/change control process include logging of all Change Requests?	Yes	
	Are applications evaluated from a security perspective prior to promotion to production?	Yes	
	Is open source software or libraries used to transmit, process or store Client Data?	Yes	
	Are identified security vulnerabilities remediated prior to promotion to production?	Yes	
	Is a web site supported, hosted or maintained that has access to Client Systems and Data?	No	
	Are Web Servers used for transmitting, processing or storing Client Data?	Yes	
	Do you have Logical or Physical segregation between web, application and database components? (i.e., Internet, DMZ, Database)?	Yes	
	Are reviews performed to validate compliance with documented web server software security standards	Yes	This area is covered by our established patch management and vulnerability scanning practices.
	Are sample applications and scripts removed from web servers?	Yes	
	Are available critical web server software security patches applied and verified at least monthly?	Yes	
	Are web server software versions that no longer have security patches released prohibited?	Yes	
	Is sufficient detail contained in Web Server and application logs to support incident investigation, including successful and failed login attempts and changes to sensitive configuration settings and files?	Yes	
	Are Web Server and application logs relevant to supporting incident investigation protected against modification, deletion, and/or inappropriate access?	Yes	
	Is an Application Programming Interface (API) available to clients?	Yes	
	Are mobile applications that access Client Systems and Data developed?	No	
Incident Event & Communication Management	Is there an established Incident Management program that has been approved by management, communicated to appropriate personnel and an owner to maintain and review the program?	Yes	
	Is there a formal Incident Response Plan?	Yes	
	Does the Incident Response Plan include actions to be taken in the event of an information security event?	Yes	
	Are events on Client Systems or systems containing Client Data relevant to supporting incident investigation regularly reviewed using a specific methodology to uncover potential incidents?	Yes	
	Does regular security monitoring include malware activity alerts such as suspicious activity?	Yes	
Business Resiliency	Is there an established Business Resiliency program that has been approved by management, communicated to appropriate personnel, and an owner to maintain and review the program?	Yes	
	Does the Business Resiliency program include a formal annual (or more frequent) executive management review of business continuity scope, key performance indicators, accomplishments, and risks?	Yes	
	Do the products and/or services specified in the scope of this assessment fall within the scope of the Business Resiliency program?	Yes	
	Are formal Business Continuity procedures developed and documented?	Yes	
	Has senior management assigned the responsibility for the overall management of critical response and recovery efforts?	Yes	
	Is there an annual review of your Business Resiliency procedures?	Yes	
	Is there a formal documented information technology Disaster Recovery exercise and testing program in place?	Yes	
	Is there an annual schedule of planned disaster recovery exercises and tests?	Yes	
	Are backups of Client systems and data performed?	Yes	
	Is there a policy or process for the backup of production data?	Yes	
	Are backup integrity and related restoration procedures tested at least annually?	Yes	
	Are backup and replication errors reviewed and resolved as required?	Yes	
	Is Client data backed up and stored offsite?	Yes	
	Are backups containing Client data stored in an environment where the security controls protecting them are equivalent to production environment security controls?	Yes	