Security Self Assessment Questionnaire (CAIQ - Lite)

ACTIVENAV

Section Heading	Control Heading	Original ID	Question Text	Answer	Notes/Comment
Application & Interface Security	**Application Security**	AIS-01.2	Do you use an automated source code analysis tool to detect security defects in code prior to production?	Yes	Development of the ActiveNav Cloud product uses Veracode Static Analysis (SAST) for source code analysis and Veracode Software Composition Analysis (SCA) for third party component analysis. Veracode Pipeline Scans ensure that security issues are addressed prior to code being deployed to production.
		AIS-01.5	(SaaS only) Do you review your applications for security vulnerabilities and address any issues prior to deployment to production?	Yes	All ActiveNav Cloud code is peer reviewed by experienced engineers, with concerns being addressed before deployment. Veracode Pipeline Scans (static analysis) are used as a gate to deployment. We perform Threat Modelling as part of our development cycle. Veracode DAST is run weekly on the deployed production system.
	Customer Access Requirements	AIS-02.1	Are all identified security, contractual, and regulatory requirements for customer access contractually addressed and remediated prior to granting customers access to data, assets, and information systems?	Yes	We provide full details of this via our customer agreement and privacy policy
	Data Integrity	AIS-03.1	Does your data management policies and procedures require audits to verify data input and output integrity routines?	Yes	ActiveNav Cloud's APIs validate data inputs and sanitise API outputs. This is validated through extensive automated API and UI testing, combined with peer-review of all code changes, weekly DAST scans, and regular penetration tests. All data stores are backed-up using built-in Azure backup services.
Audit Assurance & Compliance	**Independent Audits**	AAC-02.1	Do you allow tenants to view your SOC2/ISO 27001 or similar third-party audit or certification reports?	Yes	ActiveNav maintains ISO 27001 certification. External audits are conducted annually by certified ISO 27001 auditors. Internal auditors follow a planned program at quarterly intervals overseen by our information security management team. Audit reports can be made available on a case-by-case basis.
		AAC-02.2	Do you conduct network penetration tests of your cloud service infrastructure at least annually?	Yes	ActiveNav Cloud is subject to regular Manual Penetration Tests via Veracode's Penetration Testing as a Service (PTaaS). This consists of a full annual test with quarterly checkpoint update tests. Penetration test reports can be made available on a case-by-case basis. ActiveNav Cloud is built on top of various Azure services. Details of cloud security testing and certifications held by Azure are available here: https://azure.microsoft.com/en-gb/explore/trusted-cloud/compliance/
		AAC-02.3	Do you conduct application penetration tests of your cloud infrastructure regularly as prescribed by industry best practices and guidance?	Yes	ActiveNav Cloud is subject to regular Manual Penetration Tests via Veracode's Penetration Testing as a Service (PTaaS). This consists of a full annual test with quarterly checkpoint update tests. Penetration test reports can be made available on a case-by-case basis. ActiveNav Cloud is built on top of various Azure services. Details of cloud security testing and certifications held by Azure are available here: https://azure.microsoft.com/en-gb/explore/trusted-cloud/compliance/
	Information System Regulatory Mapping	AAC-03.1	Do you have a program in place that includes the ability to monitor changes to the regulatory requirements in relevant jurisdictions, adjust your security program for changes to legal requirements, and ensure compliance with relevant regulatory requirements?	Yes	ActiveNav maintains ISO 27001 certification. As part of the ISO 27001 framework, adherence to relevant regulatory requirements and compliance is reviewed annually.
Business Continuity Management & Operational Resilience	**Business Continuity Testing**	BCR-02.1	Are business continuity plans subject to testing at planned intervals or upon significant organizational or environmental changes to ensure continuing effectiveness?	Yes	ActiveNav maintains ISO 27001 certification. As part of the ISO 27001 framework, all plans and policies are reviewed annually and tested as required.
	Policy	BCR-10.1	Are policies and procedures established and made available for all personnel to adequately support services operations' roles?	Yes	ActiveNav maintains ISO 27001 certification. As part of the ISO 27001 framework, all plans and policies are made available to all ActiveNav staff.
	Retention Policy	BCR-11.1	Do you have technical capabilities to enforce tenant data retention policies?	No	ActiveNav Cloud does not support setting of retention policies per-Tenant.
		BCR-11.3	Have you implemented backup or recovery mechanisms to ensure compliance with regulatory, statutory, contractual or business requirements?	Yes	All data stores used by ActiveNav Cloud are backed-up using built-in Azure backup services.
		BCR-11.7	Do you test your backup or redundancy mechanisms at least annually?	Yes	Backup and redundancy mechanisms used by the ActiveNav Cloud product are tested when introduced. The ActiveNav Cloud team are currently working on building a regular test plan for these.
Change Control & Configuration Management	**Unauthorized Software Installations**	CCC-04.1	Do you have controls in place to restrict and monitor the installation of unauthorized software onto your systems?	Yes	ActiveNav Cloud infrastructure is monitored by Microsoft Defender for Cloud (https://www.microsoft.com/en-ie/security/business/cloud-security/microsoft-defender-cloud).
Data Security & Information Lifecycle Management	**E-commerce Transactions**	DSI-03.1	Do you provide standardized (e.g. ISO/IEC) non-proprietary encryption algorithms (3DES, AES, etc.) to tenants in order for them to protect their data if it is required to move through public networks (e.g., the Internet)?	Yes	All communication between the end-user's browser and the ActiveNav Cloud service backend are routed through Azure Front Door, which enforces a minimum of TLS 1.2 and use of the following suite of secure ciphers: •TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 •TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 •TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 •TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
		DSI-03.2	Do you utilize open encryption methodologies any time your infrastructure components need to communicate with each other via public networks (e.g., Internet-based replication of data from one environment to another)?	Yes	All communication between backend services uses a minimum of TLS 1.2, with keys and ciphers managed by the Azure platform.
	Nonproduction Data	DSI-05.1	Do you have procedures in place to ensure production data shall not be replicated or used in non-production environments?	Yes	ActiveNav Cloud's development and production systems are managed in separate Azure subscriptions, with separate access controls. As a matter of policy, we do not use or replicate production data into the non-production environments.
	Secure Disposal	DSI-07.1	Do you support the secure deletion (e.g., degaussing/cryptographic wiping) of archived and backed-up data?	Yes	Management of the secure deletion of data and decommissioning of storage and compute resources is handled via the Microsoft Azure platform. All customer data is deleted as part of tenant deletion end of the account subscription lifecycle.
		DSI-07.2	Can you provide a published procedure for exiting the service arrangement, including assurance to sanitize all computing resources of tenant data once a customer has exited your environment or has vacated a resource?	Yes	Customers can terminate their subscription to ActiveNav Cloud according to the terms set out in the Service Subscription Agreement. All customer data is deleted as part of tenant deletion end of the subscription lifecycle.
Datacenter Security	**Asset Management**	DCS-01.2	Do you maintain a complete inventory of all of your critical assets located at all sites/ or geographical locations and their assigned ownership?	Yes	ActiveNav maintains ISO 27001 certification. As part of the ISO 27001 framework, we maintain a database of all critical company assets, including their location and owner.
	Controlled Access Points	DCS-02.1	Are physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks, and security patrols) implemented for all areas housing sensitive data and information systems?	Yes	ActiveNav does not maintain physical hosting infrastructure. All infrastructure involved in hosting the ActiveNav Cloud product is provided by Microsoft Azure. https://azure.microsoft.com/en-gb/explore/trusted-cloud/compliance/
	User Access	DCS-09.1	Do you restrict physical access to information assets and functions by users and support personnel?	Yes	ActiveNav does not maintain physical hosting infrastructure. All infrastructure involved in hosting the ActiveNav Cloud product is provided by Microsoft Azure. https://azure.microsoft.com/en-gb/explore/trusted-cloud/compliance/
Encryption & Key Management	**Key Generation**	EKM-02.1	Do you have a capability to allow creation of unique encryption keys per tenant?	Partially	Any customer-provided credentials are securely stored in a per-tenant Azure Key Vault. Search terms provided for Target Search are double encrypted using Azure Storage Client-Side Encryption with a tenant-specific key stored in the per-tenant Key Vault. Data held within shared databases is stored with Transparent Data Encryption but cannot be encrypted with tenant specific keys.
	Encryption	EKM-03.1	Do you encrypt tenant data at rest (on disk/storage) within your environment?	Yes	The service uses Microsoft Azure Storage Accounts with Transparent Data Encryption enabled and Azure Disk Encryption for any Virtual Machine disks. Azure SQL Transparent Data Encryption technology is used to protect all data in SQL databases, and the Azure platform ensures that the same level of encryption is used for all backups. All key management is handled via the Microsoft Azure platform, with keys stored in Azure Key Vaults. All data at rest is secured using 256-bit AES encryption.
Governance and Risk Management	**Baseline Requirements**	GRM-01.1	Do you have documented information security baselines for every component of your infrastructure (e.g., hypervisors, operating systems, routers, DNS servers, etc.)?	Yes	All such infrastructure involved in hosting the ActiveNav Cloud product is provided by Microsoft Azure. All of the infrastructure provisioning and configuration is automated via Azure Pipelines and ARM Templates, which are maintained as source code (Infrastructure as Code), undergoing review and approval for any changes.

Section Heading	Control Heading	Original ID	Question Text	Answer	Notes/Comment
	Policy	GRM-06.1	Are your information security policies and procedures made available to all impacted personnel and business partners, authorized by accountable business role/function and supported by the information security management program as per industry best practices (e.g. ISO 27001, SOC 2)?	Yes	ActiveNav maintains ISO 27001 certification. As part of the ISO 27001 framework, all plans and policies are made available to all ActiveNav staff.
	Policy Enforcement	GRM-07.1	Is a formal disciplinary or sanction policy established for employees who have violated security policies and procedures?	Yes	Confidentiality agreements and/or NDAs are maintained for all staff. Any violations of information security policies or procedures would be considered as misconduct under their employment contracts, to be managed via internal disciplinary procedures.
	Policy Reviews	GRM-09.1	Do you notify your tenants when you make material changes to your information security and/or privacy policies?	Yes	All changes to information security and/or privacy policies that have a material impact on ActiveNav's customers are notified to the customers in advance via the Customer Success Team.
		GRM-09.2	Do you perform, at minimum, annual reviews to your privacy and security policies?	Yes	ActiveNav maintains ISO 27001 certification. As part of the ISO 27001 framework, all plans and policies are reviewed and audited annually.
Human Resources	**Asset Returns**	HRS-01.1	Upon termination of contract or business relationship, are employees and business partners adequately informed of their obligations for returning organizationally-owned assets?	Yes	It is standard ActiveNav policy to require the return of company owned assets on termination of contracts of employment or other relationships.
	Background Screening	HRS-02.1	Pursuant to local laws, regulations, ethics, and contractual constraints, are all employment candidates, contractors, and involved third parties subject to background verification?	Yes	Pursuant to local laws, regulations, ethics, and contractual constraints, all employees are subject to 10-year background checks, inclusive of federal, state, municipality criminal checks, sexual predator lists, SSN verification, education search, employment verifications, global watchlist search, and professional licenses verification. Confidentiality agreements and/or NDAs are maintained for all staff.
	Employment Agreements	HRS-03.1	Do your employment agreements incorporate provisions and/or terms in adherence to established information governance and security policies?	Yes	Confidentiality agreements and/or NDAs are maintained for all ActiveNav staff. Any violations of information security policies or procedures would be considered as misconduct under their employment contracts, to be managed via internal disciplinary procedures.
	Employment Termination	HRS-04.1	Are documented policies, procedures, and guidelines in place to govern change in employment and/or termination?	Yes	ActiveNav's information security policies and staff handbooks include clear procedures for dealing with changes to, or termination of, contracts of employment for ActiveNav staff.
	Training / Awareness	HRS-09.5	Are personnel trained and provided with awareness programs at least once a year?	Yes	All ActiveNav staff new staff undertake information security awareness training. All staff are required to repeat this training annually.
Identity & Access Management	**Audit Tools Access**	IAM-01.1	Do you restrict, log, and monitor access to your information security management systems (e.g., hypervisors, firewalls, vulnerability scanners, network sniffers, APIs, etc.)?	Yes	Access to all aspects of the service environment is controlled by ActiveNav's AzureAD and Azure RBAC. The ActiveNav Cloud DevOps team use Microsoft Defender for Cloud and SQL including Advanced Threat Protection to automatically monitor, detect and alert suspicious activities and unusual access patterns. The Microsoft Azure platform maintains an auditable activity log for management operations against all deployed resources.
		IAM-01.2	Do you monitor and log privileged access (e.g., administrator level) to information security management systems?	Yes	The ActiveNav Cloud DevOps team use Microsoft Defender for Cloud and SQL including Advanced Threat Protection to automatically monitor, detect and alert suspicious activities and unusual access patterns. he Microsoft Azure platform maintains an auditable activity log for management operations against all deployed resources.
	User Access Policy	IAM-02.1	Do you have controls in place ensuring timely removal of systems access that is no longer required for business purposes?	Yes	Access to all aspects of the service environment is controlled by ActiveNav's AzureAD and Azure RBAC. Any role or temporary access granted for a specific activity is removed at completion of that activity.
	Policies and Procedures	IAM-04.1	Do you manage and store the identity of all personnel who have access to the IT infrastructure, including their level of access?	Yes	Access to all aspects ActiveNav's IT environment is controlled by ActiveNav's AzureAD and Azure RBAC. Role assignment is regularly reviewed by engineering and security management.
	Source Code Access Restriction	IAM-06.1	Are controls in place to prevent unauthorized access to your application, program, or object source code, and assure it is restricted to authorized personnel only?	Yes	Access to all aspects of the environment used to develop and host ActiveNav Cloud are controlled by ActiveNav's AzureAD and Azure RBAC. Role assignment is regularly reviewed by engineering and security management.
		IAM-06.2	Are controls in place to prevent unauthorized access to tenant application, program, or object source code, and assure it is restricted to authorized personnel only?	Yes	Access to all aspects of the environment used to develop and host ActiveNav Cloud are controlled by ActiveNav's AzureAD and Azure RBAC. Role assignment is regularly reviewed by engineering and security management.
	User Access Restriction / Authorization	IAM-08.1	Do you document how you grant, approve and enforce access restrictions to tenant/customer credentials following the rules of least privilege?	Yes	Customer credentials for system access are managed independently in Azure AD B2C. Credentials provided to the Cloud platform for repository access are securely stored in a per-tenant Azure Key Vault, and cannot subsequently be retrieved through the user interface. Roles are assigned to user accounts to control the level of privilege that individuals have within the platform.
	User Access Reviews	IAM-10.1	Do you require a periodical authorization and validation (e.g. at least annually) of the entitlements for all system users and administrators (exclusive of users maintained by your tenants), based on the rule of least privilege, by business leadership or other accountable business role or function?	Yes	ActiveNav maintains ISO 27001 certification. As part of the ISO 27001 framework, all security roles in the business are reviewed and audited annually.
	User Access Revocation	IAM-11.1	Is timely deprovisioning, revocation, or modification of user access to the organizations systems, information assets, and data implemented upon any change in status of employees, contractors, customers, business partners, or involved third parties?	Yes	ActiveNav's information security policies and staff handbooks include clear procedures for dealing with changes to, or termination of, contracts of employment for ActiveNav staff, and other business relationships. This includes revocation of access to ActiveNav systems and assets.
Infrastructure & Virtualization Security	**Audit Logging / Intrusion Detection**	IVS-01.1	Are file integrity (host) and network intrusion detection (IDS) tools implemented to help facilitate timely detection, investigation by root cause analysis, and response to incidents?	Yes	Microsoft Defender for Cloud and SQL including Advanced Threat Protection is used to automatically monitor, detect and alert suspicious activities and unusual access patterns.
		IVS-01.2	Is physical and logical user access to audit logs restricted to authorized personnel?	Yes	Access to all aspects of the service environment is controlled by ActiveNav's AzureAD and Azure RBAC. Role assignment is regularly reviewed by engineering and security management.
		IVS-01.5	Are audit logs reviewed on a regular basis for security events (e.g., with automated tools)?	Yes	Microsoft Defender for Cloud and SQL including Advanced Threat Protection is used to automatically monitor, detect and alert suspicious activities and unusual access patterns.
	Clock Synchronization	IVS-03.1	Do you use a synchronized time-service protocol (e.g., NTP) to ensure all systems have a common time reference?	Yes	Time synchronization of our Azure infrastructure is handled by the Azure cloud services.
	OS Hardening and Base Controls	IVS-07.1	Are operating systems hardened to provide only the necessary ports, protocols, and services to meet business needs using technical controls (e.g., antivirus, file integrity monitoring, and logging) as part of their baseline build standard or template?	Yes	Where we have a small number of VMs in our hosting infrastructure, their operating systems only enable the minimum services required for their specific purpose, have Endpoint Protection installed, and are hardened according to recommendations from Microsoft Defender for Cloud.
	Production / Non-Production Environments	IVS-08.1	For your SaaS or PaaS offering, do you provide tenants with separate environments for production and test processes?	Not Applicable	This is not applicable to the nature & purpose of the ActiveNav Cloud product.
		IVS-08.3	Do you logically and physically segregate production and non-production environments?	Yes	Production and non-production environments are logically separated within our Azure subscriptions and hosted in physically different regions.
	Segmentation	IVS-09.1	Are system and network environments protected by a firewall or virtual firewall to ensure business and customer security requirements?	Yes	The ActiveNav Cloud product makes use of Azure Front Door to provide WAF and reverse proxy capabilities to segregate the backend from the open Internet. All backend services make use of Network Security groups to restrict access to only those services that require it.
	VMM Security - Hypervisor Hardening	IVS-11.1	Do you restrict personnel access to all hypervisor management functions or administrative consoles for systems hosting virtualized systems based on the principle of least privilege and supported through technical controls (e.g., two-factor authentication, audit trails, IP address filtering, firewalls and TLS-encapsulated communications to the administrative consoles)?	Yes	All infrastructure involved in hosting the ActiveNav Cloud product is provided by Microsoft Azure, and hence ActiveNav staff do not have direct access to hypervisor management functions. Access to all other aspects of the environment used to develop and host ActiveNav Cloud are controlled by ActiveNav's AzureAD and Azure RBAC. Role assignment is regularly reviewed by engineering and security management.
	Wireless Security	IVS-12.1	Are policies and procedures established and mechanisms configured and implemented to protect the wireless network environment perimeter and to restrict unauthorized wireless traffic?	Not Applicable	No part of the ActiveNav Cloud product makes use of wireless networks. All operational or administrative access requires two factor authentication over securely encrypted HTTPS connections.
		IVS-12.2	Are policies and procedures established and mechanisms implemented to ensure wireless security settings are enabled with strong encryption for authentication and transmission, replacing vendor default settings (e.g., encryption keys, passwords, SNMP community strings)?	Not Applicable	No part of the ActiveNav Cloud product makes use of wireless networks. All operational or administrative access requires two factor authentication over securely encrypted HTTPS connections.
		IVS-12.3	Are policies and procedures established and mechanisms implemented to protect wireless network environments and detect the presence of unauthorized (rogue) network devices for a timely disconnect from the network?	Not Applicable	No part of the ActiveNav Cloud product makes use of wireless networks. All operational or administrative access requires two factor authentication over securely encrypted HTTPS connections.
Interoperability & Portability	**APIs**	IPY-01.1	Do you publish a list of all APIs available in the service and indicate which are standard and which are customized?	Not Applicable	ActiveNav Cloud does not currently offer API access to customers
Mobile Security	**Approved Applications**	MOS-03.1	Do you have a policy enforcement capability (e.g., XACML) to ensure that only approved applications and those from approved application stores can be loaded onto a mobile device?	Not Applicable	ActiveNav does not provide mobile devices or produce mobile applications.

Section Heading	Control Heading	Original ID	Question Text	Answer	Notes/Comment
Security Incident Management, E-Discovery, & Cloud Forensics	**Incident Management**	SEF-02.1	Do you have a documented security incident response plan?	Yes	The ActiveNav Global Information Security Manual details the full Information Security Incident Response Process.
		SEF-02.4	Have you tested your security incident response plans in the last year?	Yes	The ActiveNav Information Security Team serves as the primary contract for security incident response, as well as provide overall direction for incident prevention, identification, investigation and resolution. Our CTO/CISO defines roles and responsibilities for the IST and the IST must comply with the policies in place about detecting events and timely corrective actions. These are defined by the incident type such as validating that an incident has occurred, communicating with the broader IST and notification with relevant parties, preserving evidence, documenting an incident itself and related response activities, containing the incident, eradicating the incident, escalating the incident if necessary and conducting a retrospective after eradication for lessons learned.
	Incident Reporting	SEF-03.1	Are workforce personnel and external business relationships adequately informed of their responsibility, and, if required, consent and/or contractually required to report all information security events in a timely manner?	Yes	The ActiveNav Global Information Security Manual, available to all staff, details the full Information Security Incident Response Process. All staff are trained on the content of the ISM.
		SEF-03.2	Do you have predefined communication channels for workforce personnel and external business partners to report incidents in a timely manner adhering to applicable legal, statutory, or regulatory compliance obligations?	Yes	The ActiveNav Global Information Security Manual, available to all staff, details the full Information Security Incident Response Process. All staff are trained on the content of the ISM.
	Incident Response Legal Preparation	SEF-04.4	Do you enforce and attest to tenant data separation when producing data in response to legal subpoenas?	Yes	Any legally enforceable data production event is handled formally through ActiveNav's global incident response process which manages, among other things, collection, separation, verification, integrity and chain of custody.
Supply Chain Management, Transparency, and Accountability	**Incident Reporting**	STA-02.1	Do you make security incident information available to all affected customers and providers periodically through electronic methods (e.g., portals)?	Yes	ActiveNav informs all customers of relevant security incidents via our Support Team.
	Network / Infrastructure Services	STA-03.1	Do you collect capacity and use data for all relevant components of your cloud service offering?	Yes	The ActiveNav Cloud DevOps team use Azure Monitor and Azure Application Insights and other reporting tools to collect and monitor usage and capacity of the cloud infrastructure and application services.
	Third Party Agreements	STA-05.4	Do third-party agreements include provision for the security and protection of information and assets?	Yes	ActiveNav performs information security reviews for all third party suppliers during contract negotiation and onboarding. All such third-party agreements are required to include provisions for security and protection of information and assets.
		STA-05.5	Do you have the capability to recover data for a specific customer in the case of a failure or data loss?	No	The ActiveNav Cloud product is multi-tenant in nature with disaster recovery implemented for the complete cloud instance. We have robust systems in place, using services provided by the Microsoft Azure hosting platform, to backup and restore all critical customer data in the event of failure or data loss. Recovery of specific tenants in isolation is not supported.
	Supply Chain Metrics	STA-07.4	Do you provide tenants with ongoing visibility and reporting of your operational Service Level Agreement (SLA) performance?	No	ActiveNav doesn't currently offer live reporting against SLAs. However, we do inform all customers of service disruptions or any other impacts to service via our Support Team.
	Third Party Audits	STA-09.1	Do you mandate annual information security reviews and audits of your third party providers to ensure that all agreed upon security requirements are met?	No	ActiveNav performs information security reviews for all third party suppliers during contract negotiation and onboarding. Further reviews are triggered if there is a material change to the service or its terms of business.
Threat and Vulnerability Management	**Antivirus / Malicious Software**	TVM-01.1	Do you have anti-malware programs that support or connect to your cloud service offerings installed on all of your IT infrastructure network and systems components?	Yes	All infrastructure involved in hosting the ActiveNav Cloud product is provided by Microsoft Azure, who are responsible for anti-malware provision on the servers underlying the PaaS services we use. Where we have a small number of VMs in this infrastructure, these have Endpoint Protection installed, as recommended by Microsoft Defender for Cloud. All laptops used by ActiveNav staff have Bitdefender Endpoint Security installed.
	Vulnerability / Patch Management	TVM-02.5	Do you have a capability to patch vulnerabilities across all of your computing devices, applications, and systems?	Yes	Where we have a small number of VMs in our hosting infrastructure, these have Microsoft's Update Management tooling installed, as recommended by Microsoft Defender for Cloud. All laptops used by ActiveNav staff have automatic update managed via Group Policy.
	Mobile Code	TVM-03.1	Is mobile code authorized before its installation and use, and the code configuration checked, to ensure that the authorized mobile code operates according to a clearly defined security policy?	Not Applicable	ActiveNav does not provide mobile devices or produce mobile applications.