Cloud Security, Infrastructure and Data Protection Assurance

The following schedules have been prepared by streamGo to demonstrate our information security standards relating to our platform, infrastructure and organisation.

The 3 areas we cover are the security of our cloud based event platform, our internal infrastructure and our accountability, transparency and the organisational and technical measures we deploy to protect personal data.

Cloud Security

Based on the 14 principles of Cloud Security, as determined by the National Cyber Security Centre, demonstrates how we configure and safely deploy our Cloud based event platform.

ISO 27001

streamGo has been awarded ISO 27001 in November 2021. All elements of the framework are implemented in the business.

GDPR Compliance

We commission an external, independent annual assessment of our GDPR credentials. Our latest audit was completed in Sept 2021. Enclosed are the details of our latest audit which shows the overarching Risk Areas assessed and the standards we adopt associated with each Key Risk Area. This is a comprehensive evidence based audit.

Cloud Security Questionnaire

	Principle	Approach	streamGo deployed security
	1. Data in transit protection		
1	User data transiting networks are adequately protected against tampering and eavesdropping. Network protection - denying an attacker the ability to intercept data Encryption - denying your attacker the ability to read data	Private WAN service	All services remain with in a single VPC
		Legacy SSL and TLS	N/A
		TLS	TLS 1.2
		IPsec or TLS VPN gateway	N/A
		Bonded fibre optic connections	N/A
	2. Asset Protection and Resilience		
2.1	Physical location and legal jurisdiction		
	We understand in which locations our data is stored, processed and managed. We understand how data-handling controls within the service are enforced, relative to UK legislation.	Unknown processing and storage locations	N/A
		Known locations for storage only	N/A
		Known locations for storage, processing and management	United Kingdom
2.2	Data centre security		
	Locations used to provide cloud services have physical protection against unauthorised access, tampering, theft or reconfiguration of systems.	Unknown	N/A
		Known controls	AWS approved employee time-bound access
		Conformance with a recognised standard	Yes - ISO 27001
2.3	Data at rest protection		
	To ensure data is not available to unauthorised parties with physical access to infrastructure, user data held within the service is protected regardless of the storage media on which it's held.	Physical access control	N/A
		Infeasibility of finding a specific customer's data on physical media	N/A
		Encryption of all physical media	Encryption at rest using KMS

2.4	Data sanitisation		
	The process of provisioning, migrating and de-provisioning resources does not result in unauthorised access to user data. We are sufficiently confident that: 1. Our data is erased when resources are moved or re-provisioned, when they leave the service or when we request it to be erased	None/unknown	N/A
		Assurances media can't be directly addressed	Data is no longer served
		Explicit overwriting of storage before reallocation	N/A
Equipment disposal			
2.5	Once equipment used to deliver a service reaches the end of its useful life, it is disposed of in a way which does not compromise the security of the service, or user data stored in the service.	Unknown or proprietary techniques used	N/A
		A recognised standard for equipment disposal is followed	Conforms to NIST 800- 88 guidelines
		A third party destruction service is used	N/A
2.6	Physical resilience and availability		
	Services have varying levels of resilience, which will affect their ability to operate normally in the event of failures, incidents or attacks. A service without guarantees of availability may become unavailable, potentially for prolonged periods, regardless of the impact on your business.	Publicised Service Level Agreement (SLA)	Yes
		Historical data relating to service availability	N/A
		System design to demonstrate service resilience	Multi-zone availability served through load balancer with regular health checks
3. Separation between users			
	No malicious or compromised user of the service can affect the service or data of another.	Virtualisation technologies (e.g. a hypervisor) provide separation between users	N/A
		Other software provides separation between users	User policies prevent writing of data
4. Governance framework			
	We have a security governance framework which coordinates and directs management of our service and information within it. 1. A clearly identified, and named, board owner 2. A documented framework for security governance, with policies governing key aspects of	Assertion that the goals are met	Yes
		Conformance with a recognised standard	Yes - ISO 27001

	information security relevant to the service. 3. Security and information security are part of our financial and operational risk reporting mechanisms, which are reportable to the board 4. We have documented processes to identify and ensure compliance with applicable legal and regula tory requirements.		
5. Operational security			
	The service is operated and managed securely to impede, detect or prevent attacks.		
	Configuration and change management We have an accurate picture of the assets which make up the service, along with their configurations and dependencies.	Assertion that the goals are met	Yes, all assets, configuration and dependencies are documented
		Conformance with a recognised standard	Yes - ISO 27001
	Vulnerability management We have a vulnerability management process which enables us to know what vulnerabilities are present within our IT estate on a regular basis.	Conformance with a recognised standard	Yes - ISO 27001
	Protective Monitoring We effectively monitor for attack, misuse and mal function	Assertion that the goals are met	Yes, platform access is continuously monitored and logged
		Conformance with a recognised standard	Yes - ISO 27001
	Incident management 1. Incident management processes are in place for the service and are actively deployed in response to security incidents 2. Pre-planned incident management processes are in place 3. A defined process and contact route exists for reporting of security incidents by consumers and external entities 4. Security incidents are reported in acceptable timescales and formats	Assertion that the goals are met	Internal processes in place for handling of all incident types. Direct contacts in place for reports from external sources.
		Conformance with a recognised standard	Yes - ISO 27001
6. Personnel security			

	1. Only authorised employees have access to personal data and systems. 2. We thoroughly and regularly screen and adequately train our staff.	Personnel screening not performed	N/A
		Personnel screening performed but does not conform with BS7858:2012	Only trained and authorised personnel given access
		Personnel screening per formed which conforms to BS7858:2012	N/A
7. Secure development			
	Services are designed and developed to identify and mitigate threats to system security.	Engineering approaches consider security as an important factor	Yes
		Engineering approach adheres to a secure development standard or recognised good practice	SDLC incorporates industry best practices and conforms to ISO 27001.
		Independent reviews of engineering approach is undertaken against recognised secure development standards	Yes as part of ISO 27001
8. Supply chain security			
	We ensure our supply chain satisfactorily supports all of our security principles.	Our security commitments transit through our suppliers	Yes
		Assessed through application of an appropriate standard	N/A
9. Secure user management			
	Management interfaces and procedures in place to prevent unauthorised access and alteration of our resources, applications and data.	Authentication of users takes place to the management interfaces and support channels	Yes
		Strong authentication in place	Yes
		Strong authentication is in place, which is subject to regular exercising	Yes

		Separation and access control exist within management interfaces	Yes
		No digital service management interface for users to administer their service	N/A
		Access control implemented in software	N/A
		Access control implemented in software, subject to regular testing	Yes
	10. Identity and authentication		
	All access to the service interfaces are constrained to authenticate and authorised individuals. Authentication occurs over secure channels.	Two factor authentication	N/A
		TLS client certificate	Yes
		Identity federation with your existing identity provider	N/A
		Limited access over dedicated link, enterprise or community network	N/A
		Username and password access	Yes
	11. External interface protection		
	All external or less trusted interfaces of the service are identified and appropriately defended.	Internet	Yes
		Community network	N/A
		Private network	Yes
	12. Secure service administration		
	The design, implementation and management of administration systems follow enterprise good practice, whilst recognising their high value to attackers.	Unknown service management architecture	
		Known service management architecture	
		Other	SDLC incorporates industry best practices and regular reviews/testing
	13. Audit information for users		
	Audit to monitor access to our service and the	None	Yes

	data held within it are available upon request	Data made available by negotiation	
		Data made available	
14. Secure use of the service			
	We have full knowledge of the configuration or state of devices accessing the service.	Enterprise managed devices	Yes
		Partner managed devices	N/A
		Unknown devices	N/A

Criteria	Approach	streamGo deployed security
Office Firewalls and Internet Gateways Software or hardware which provides technical protection between our systems and the outside world. Questions in this section relate to Hardware Firewall devices, Routers, Computers and Laptops only.	We have firewalls at the boundaries between our organisation's internal networks and the internet	Firewall in place within the office and Amazon Web Services (AWS)
	Has the password that's set up prior to installation of your internet router been changed for installation	Changed upon initial set up
	Is the new password on all your internet routers or hardware firewall devices are at least 8 characters in length and are difficult to guess	Yes
	Do you change the password whenever we suspect it may have been compromised	Yes
	Do you have any services enabled that are accessible externally from your internet routers or hardware firewall devices for which you do not have a documented business case	No
	If you do have services enabled on your firewall, do you have a process to ensure they are disa bled in a timely manner when they are no longer required? Describe the process.	N/A
	Have you configured your internet routers or hardware firewall devices so that they block all other services from being advertised to the internet?	Yes
	Are your internet routers or hardware firewalls configured to allow access to their configuration settings over the internet?	No

	If yes, is there a documented business requirement for this access?	N/A
	If yes, is the access to the settings protected by either two-factor authentication or by only allowing trusted IP addresses to access the settings? List which option is used.	N/A
	Do you have software firewalls enabled on all of your computers and laptops?	Yes
	If not, is this because software firewalls are not commonly available for the operating system you are using? Please list the operating systems.	N/A
Secure Configuration Computers are often not secure upon default installation. An 'out-of-the-box' set-up can often include an administrative account with a standard, publicly known default password, one or more unnecessary user accounts enabled (sometimes with special access privileges) and pre-installed but unnecessary applications or services. All of these present security risks. Questions in this section apply to: Servers, Computers, Laptops, Tablets and Mobile Phones	When you are able to do so, have you removed or disabled all the software that you do not use on your laptops, computers, servers, tablets and mobile phones? Describe how you achieve this.	Yes, we have done this on a main system and then all machines are cloned from the main system once a year.
	Have you ensured that all your laptops, computers, servers, tablets and mobile devices only contain necessary user accounts that are regularly used in the course of your business?	Yes – using jumpcloud by department
	Have you changed the default password for all user and administrator accounts on all your laptops, computers, servers, tablets and smartphones to a non-guessable password of 8 characters or more?	Yes
	Do all your users and administrators use pass words of at least 8 characters?	Yes
	Do you run software that provides sensitive or critical information (that shouldn't be made public) to external users across the internet?	Yes, our platform
	If yes, do you ensure all users of these services use a password of at least 8 characters and that your systems do not restrict the length of the password?	Yes
	If yes, do you ensure that you change passwords if you believe that they have been compromised?	Yes
	If yes, are your systems set to lockout after ten or fewer unsuccessful login attempts, or limit the number of login attempts to no more than ten within five minutes?	No

	If yes, do you have a password policy that guides all your users?	Not formally but passwords have to be over 8 digits, containing capitals and symbols. It prevents any that don't match this requirement
	Is "auto-run" or "auto-play" disabled on all of your systems?	Yes
Software Patching To protect your organisation, you should ensure that your software is always up-to-date with the latest patches. If, on any of your in-scope devices, you are using an operating system which is no longer supported, (e.g. Microsoft Windows XP/ Vista/2003 or macOS El Capitan, Ubuntu 17.10), and you are not being provided with updates from another reliable source, then you will not be awarded certification. Mobile phones and tablets are in scope and must also use an operating system that is still supported by the manufacturer. Questions in this section apply to: Servers, Computers, Laptops, Tablets, Mobile Phones, Routers and Firewalls.	Are all operating systems and firmware on your devices supported by a supplier that produces regular fixes for any security problems?	Yes
	Are all applications on your devices supported by a supplier that produces regular fixes for any security problems?	Yes
	Is all software licensed in accordance with the publisher's recommendations?	Yes
	Are all high-risk or critical security updates for operating systems and firmware installed within 14 days of release? Describe how you achieve this.	Yes, they auto update in the background
	Are all high-risk or critical security updates for applications (including any associated files and any plugins such as Adobe Flash) installed within 14 days of release? Describe how you achieve this.	Yes, auto installed
	Have you removed any applications on your devices that are no longer supported and no longer receive regular fixes for security problems?	N/A
User Accounts It is important to only give users access to the resources and data necessary for their roles, and no more. All users need to have unique accounts and should not be carrying out day-to-day tasks such as invoicing or dealing with e-mail whilst logged on as a user with administrator privileges which allow significant changes to the way your computer systems work. Questions in this section apply to: Servers, Computers, Laptops, Tablets and Mobile Phones.	Are users only provided with user accounts after a process has been followed to approve their creation? Describe the process.	Approved by Production Director
	Can you only access laptops, computers and servers in your organisation (and the applications they contain) by entering a unique username and password?	Yes
	How do you ensure you have deleted, or disa bled, any accounts for staff who are no longer with your organisation?	They are deleted as soon as they leave the business. We have a list of accounts to disable at this point.

	Do you ensure that staff only have the privileges that they need to do their current job? How do you do this?	Yes. Regular review takes place
Administrative Accounts User accounts with special access privileges (e.g. administrative accounts) typically have the greatest level of access to information, applications and computers. When these privileged accounts are accessed by attackers they can cause the most amount of damage because they can usually perform actions such as install malicious software and make changes. Special access includes privileges over and above those of normal users. It is not acceptable to work on a day-to-day basis in a privileged "administrator" mode. Questions in this section apply to: Servers, Computers, Laptops, Tablets and Mobile Phones.	Do you have a formal process for giving someone access to systems at an "administrator" level? Describe the process.	No
	How do you ensure that staff only use administrator accounts to carry out administrative activities (such as installing software or making configuration changes)?	The main user account is not admin – they must enter admin password and request this to allow it.
	How do you ensure that administrator accounts are not used for accessing email or web browsing?	They can't login as admin
	Do you formally track which users have administrator accounts in your organisation?	Yes - Jumpcloud
	Do you review who should have administrative access on a regular basis?	Yes
	Have you enabled two-factor authentication for access to all administrative accounts?	No
	If no, is this because two-factor authentication is not available for some or all of your devices or systems? List the devices or systems that do not allow two-factor authentication.	Jumpcloud
Malware protection Malware (such as computer viruses) is generally used to steal or damage information. Malware is often used in conjunction with other kinds of attack such as 'phishing' (obtaining information by confidence trickery) and social network sites (which can be mined for information useful to a hacker) to provide a focussed attack on an organisation. Anti-malware solutions (including anti-virus) are available from commercial suppliers, some free, but usually as complete software and support packages. Malware are continually evolving, so it is important that the supplier includes both malware signatures and heuristic detection facilities which are updated as frequently as possible. Anti-malware products can also help confirm whether websites	Are all of your computers, laptops, tablets and mobile phones protected from malware by either; A - having anti-malware software installed, B - limiting installation of applications to an approved set (i.e. using an App Store and a list of approved applications) or, C - application sandboxing (i.e. by using a virtual machine)?	Yes
	If Option A: Where you have anti-malware software installed, is it set to update daily and scan files automatically upon access? If Option A: Where you have anti-malware software installed, is it set to scan web pages you visit and warn you about accessing malicious websites?	Yes Yes

you visit are malicious. Questions in this section apply to: Computers, Laptops, Tablets and Mobile Phones.	If Option B: Where you use an app-store or application signing, are users restricted from installing unsigned applications?	Yes
	If Option B: Where you use an app-store or application signing, do you ensure that users only install applications that have been approved by your organisation and do you document this list of approved applications?	Yes
	If Option C: Where you use application sandboxing, do you ensure that applications within the sandbox are unable to access data stores, sensitive peripherals and your local network? Describe how you achieve this.	N/A

GDPR Compliance

Risk Area	Key Risk Area	streamGo status
Our People Our People are adequately trained and aware of the requirements of the new Privacy legislation and the risks this brings.	All staff receive formal Data Privacy and Protection training every year and are tested regularly	Yes. Last completed July 2021
	Staff have all read the appropriate Privacy, Protection, Acceptable Use and Cyber Security policies annually	Yes. Annual review July 2021
	Quarterly department audits/spot checks via a 'Business Healthcheck'	Audit completed June 2021. Reviewed quarterly
	Consideration has been given to the appointment of a DPO / Privacy sponsor	Data Lead - Product Director
	There are regular updates from key stakeholders about the importance of Privacy eg team meetings, comms schedules, emails	Ad hoc in team meetings
Policy and Governance Our governance, policies and processes are available, understood and robust enough in order to fully comply with the legislation.	We understand what data we hold by completing 'records of processing' for all processing activities including a lawful basis for each activity	Records of Processing updated July 2021 (Controller and Processor)
	There is a published policies, standards and controls for Privacy/Protection, Acceptable Use and Cyber/Infosec	Data Protection, Acceptable Use of IT Systems and Information and Cyber Security policies last updated June 2021
	We have documented and published processes/ standards for dealing with each of the DS Subject rights & change to data use	Processes are in place for managing Data Subject Rights
	We deploy appropriate technological solutions to protect our data	See Cyber Security and Cloud Security Questionnaire
	Privacy 'Horizon Scanning' activity Undertaken	Ad hoc horizon scanning
	2nd Line audit for adherence & compliance	To be scheduled
Sharing data We fully understand who we share data with and have sufficiently satisfied ourselves that they are compliant.	We hold a full list of Data Processors and Sub Processors (RoP)	Records of Processing updated June 2021 (Controller and Processor)

	Each Processor has a Data Processing Agreement in place (or equivalent) that includes what to do in the event of a breach	DPAs are in place for Processors
	Each Processor has been subject to a due diligence audit (at least every 3 years	Formal Process in place for all new processors
	All staff who manage 3rd parties have been trained	Yes. Last completed July 2021
	Any transfer of data to a 3rd country is identified and the appropriate safeguards are sought	Recorded in Records of Processing
	Board sign off all exceptions	Non required to date
Breach Reporting & Control Our breach reporting processes are adequate.	We have a documented process for dealing with Data Breach and Privacy complaints	Yes
	All staff are aware of and adhere to the same	Yes
	We log all breaches (reportable/non reportable) and action plan underlying issues	Yes
	We review breach log for trends and instigate improvement plans	Yes, quarterly
	All staff are trained in how to spot a breach	Yes
Applying the Principles We understand, limit and use our data in accordance with the regulations.	A compliant Privacy notice is available for Staff and Customers explaining how we use data etc	Yes, published on website
	Our Processing activity is recorded and a Lawful basis established for all processing activity	Yes, in RoP and Privacy Notice
	Data capture is limited to only bare minimum	Yes, restricted to only required data to set up an account/ register for an event
	Data is kept up to date and accurate	Reliance on Data Subject to notify or any inaccuracies
	Dtaa is only stored for as long as necessary	Deleted upon close of client account or upon request if earlier

	We have process for dealing with subject rights	Yes
	Registration with the ICO complete	Yes
Physical Environment Our physical environment is sufficiently robust to protect the data in our possession.	All visitors sign in and are accompanied at all times	Yes
	All staff to read the Physical Security policy	Included in the Information and Cyber Security Policy
	'Clear Desk' review is completed monthly	Minimal/ no hard copy data is available on desks. Locking down of computers when away from desk is detailed in the Information & Security Policy and monitored on an ad hoc basis
	Secure areas are kept locked and checked regularly	Yes
Privacy by Design We have a Privacy Plan to help create a Privacy culture and deal with change effectively.	We have an ongoing Privacy Plan aimed at supporting our culture	Yes, Data Privacy Risk Register and associated action plan last updated July 2021
	Our plan is sponsored by the Board and is regularly reviewed	Yes, Richard Lee, Product Director
	'We have procedures for change and Managers understand and have been trained in the Data Protection Impact Assessments (DPIA)	Yes
	We have a DPIA reporting mechanism	All staff are trained to complete a DPIA and forward to a Director for sign off
	There is a central cascade of key messages periodically	Ad hoc cascade of messages takes place