Jama Information Security FAQ

General Information

This questionnaire is based on the Shared Assessments Standardized Information Gathering (SIG) Questionnaire and is intended to provide an overview of controls related to cybersecurity, IT, privacy, data security and business resiliency.

Section 1

A. GENERAL INFORMATION	
How many people are employed at this site?	Approximately 200
How many people are employed by the parent company?	Same as above
How long has this site been in operation?	12+ years
How long has the parent company been in operation?	Same as above
What other types of business are conducted at this site?	None
Number of buildings/facilities	2
Approximate total square footage of facilities	30,000
Approximate annual sales	Not provided to 3rd parties
Please provide a general list of services provided or products manufactured.	Jama Software provides the leading platform for requirements, risk and test management.

Section 2

RISK ASSESSMENT AND TREATMENT	Yes	No	N/A	Notes or Comments
Is there a risk assessment program that has been approved by management, communicated to appropriate constituents and an owner to maintain and review the program?	☐	☐ **X**	☐	Jama does not currently have a formally documented risk management policy, however Jama's leadership team and Finance organization own the oversight of identification, assessment, and treatment of risks.

SECURITY POLICY	Yes	No	N/A	Notes or Comments
Is there an information security policy that has been approved by management, communicated to appropriate constituents and an owner to maintain and review the policy?	☐ X	☐	☐	Yes. Jama's Information Security Program is based on ISO 27001. A high-level overview of the program can be found here: https://www.jamasoftware.com/trust/
Have the policies been reviewed in the last 12 months?	☐ X	☐	☐	
Is there a vendor management program?	☐ X	☐	☐	

ORGANIZATIONAL SECURITY	Yes	No	N/A	Notes or Comments
Is there a respondent information security function responsible for security initiatives?	☐ X	☐	☐	Jama's Information Security Officer is responsible for all security initiatives.
Do external parties have access to Scoped Systems and Data or processing facilities?	☐	☐ X	☐	

ASSET MANAGEMENT	Yes	No	N/A	Notes or Comments
Is there an asset management policy or program that has been approved by management, communicated to appropriate constituents and an owner to maintain and review the policy?	☐ X	☐	☐	Tools are in place to maintain assets for cloud and in office workstations.
Are information assets classified?	☐ X	☐	☐	

HUMAN RESOURCE SECURITY	Yes	No	N/A	Notes or Comments
Are security roles and responsibilities of constituents defined and documented in accordance with the respondent's information security policy?	X			Yes. Jama's Information Security Program is based on ISO 27001 and includes sections defining roles and responsibilities. A high-level overview of the program can be found here: https://www.jamasoftware.com/trust/
Is a background screening performed prior to allowing constituent access to Scoped Systems and Data?	X			Yes. Background checks are performed for all roles at Jama.
Are new hires required to sign confidentiality agreements upon hire?	X			
Is there a security awareness training program?	X			Yes. Jama's Information Security awareness training must be completed annually.
Is there a disciplinarily process for non-compliance with information security policies?	X			
Is there a constituent termination or change of status process?	X			

PHYSICAL AND ENVIRONMENTAL SECURITY	Yes	No	N/A	Notes or Comments
Is there a physical security program?	X			Jama has electronic card readers on all doors. All users are required to use their badge to gain access to our office. Additional physical security of the data center is handled by Amazon.
Are reasonable physical security and environmental controls present in the building/data center that contains Scoped Systems and Data?	X			Jama has electronic card readers on all doors. All users are required to use their badge to gain access to our office. Additional physical security of the data center is handled by Amazon (AWS).
Are visitors permitted in the facility?		X		Visitors are not allowed in the data center.

COMMUNICATIONS AND OPERATIONS MANAGEMENT	Yes	No	N/A	Notes or Comments
Are Management approved operating procedures utilized?	X			

COMMUNICATIONS AND OPERATIONS MANAGEMENT	Yes	No	N/A	Notes or Comments
Is there an operational change management / change control policy or program that has been approved by management, communicated to appropriate constituents and an owner to maintain and review the policy?	☐ X	☐	☐	Jama's change management process is outlined in our SDLC documentation. These processes are audited by Tuv Sud in accordance with our Fit for Purpose certifications for functional safety.
Do third party vendors have access to Scoped Systems and Data? (backup vendors, service providers, equipment support maintenance, software maintenance vendors, data recovery vendors, etc.)?	☐ X	☐	☐	Third parties don't have access to unencrypted scoped data. Our hosting provider, AWS does not have logical access to the data, and all data is encrypted in transit and at rest.
Is there an anti-virus / malware policy or program (workstations, servers, mobile devices) that has been approved by management, communicated to appropriate constituents and an owner to maintain and review the policy?	☐ X	☐	☐	Our anti-virus/malware program has been implemented within our offices. All systems used by the Company and systems accessing the production environment have antivirus. Jama is hosted on hardened Linux servers and the software is contained Docker containers. Jama is researching the possibility of running antivirus on the Linux OS. We utilize commercial firewall products for protection of DMZ, VLANs, and separating security zones including corporate assets.

COMMUNICATIONS AND OPERATIONS MANAGEMENT	Yes	No	N/A	Notes or Comments
Are system backups of Scoped Systems and Data performed?	☐ **X**	☐	☐	Jama has a DR/BCP which outlines our restoration and recovery guidelines in the event of a disaster. Part of that plan includes the recovery of resources within AWS. Jama's application is hosted in AWS US West (Oregon) region which consists of three availability zones. Our primary hosting infrastructure runs out of one of those three zones. Since our backups are stored in all three availability zones, and a real-time replication of our databases are stored in a second availability zone, we have the ability to quickly recover from a disaster. RTO: We support a RTO of 30 minutes for failures within AWS US West (Oregon) region. Our RTO for failures where we have to move outside of the AWS US West (Oregon) region is 4 hours. RPO: We support an RPO of less than 5 minutes for failures within AWS US West (Oregon) region. Our RTO for failures where we have to move outside of the AWS US West (Oregon) region is less than 24 hours.
Are firewalls in use for both internal and external connections?	☐ **X**	☐	☐	Jama has firewalls in place on all networks, and provide network segregation. Jama has host-based IDS on systems where the client is supported.

COMMUNICATIONS AND OPERATIONS MANAGEMENT	Yes	No	N/A	Notes or Comments
Are vulnerability assessments, scans or penetration tests performed on internal or external networks?	☐ **X**	☐	☐	Jama has integrated OWASP into our development processes, as well as other security best practices. Jama also performs regular vulnerability and penetration tests in-house, as well as through third-parties on internal and external networks. More information can be found in the attached Security Overview, and on our website at https://www.jamasoftware.com/trust
Are there external network connections (Internet, intranet, extranet, etc.)?	☐ **X**	☐	☐	
Is wireless networking technology used?	☐ **X**	☐	☐	
Is there a removable media policy or program (CDs, DVDs, tapes, disk drives) that has been approved by management, communicated to appropriate constituents, and an owner to maintain and review the policy?	☐ **X**	☐	☐	
Is Scoped Data sent or received electronically or via physical media?	☐	☐ **X**	☐	No PHI or PII data is stored in the Jama Connect system.
Are Web services provided?	☐ **X**	☐	☐	

ACCESS CONTROL	Yes	No	N/A	Notes or Comments
Are electronic systems used to transmit, process or store Scoped Systems and Data?	☐ X	☐	☐	
Are unique user IDs used for access?	☐ X	☐	☐	
Are passwords required to access systems transmitting, processing or storing Scoped Systems and Data?	☐ X	☐	☐	
Is remote access permitted?	☐ **X**	☐	☐	All remote access to our production systems are required to go through a Bastion host. Direct access to our production systems is not permitted.

INFORMATION SYSTEMS ACQUISITION DEVELOPMENT & MAINTENANCE	Yes	No	N/A	Notes or Comments
Are business information systems used to transmit, process or store Scoped Systems and Data?	X			
Is application development performed?	X			
Is there a formal Software Development Life Cycle (SDLC) process?	X			SLDC procedure documentation available upon request.
Are systems and applications patched?	X			
Is a web site supported, hosted or maintained that has access to Scoped Systems and Data?	X			
Are vulnerability tests (internal/external) performed on all applications at least annually?	X			
Are encryption tools managed and maintained for Scoped Data?				We support TLS 1.0 and higher for all communications to the application. We also use AES 256 for encrypting data-at-rest.

INCIDENT EVENT AND COMMUNICATIONS MANAGEMENT	Yes	No	N/A	Notes or Comments
Is there an Incident Management program?	X			

BUSINESS CONTINUITY AND DISASTER RECOVERY	Yes	No	N/A	Notes or Comments
Is there a documented policy for business continuity and disaster recovery that has been approved by management, communicated to appropriate constituents and an owner to maintain and review the policy?	X			
Is there an annual schedule of required tests?	X			

BUSINESS CONTINUITY AND DISASTER RECOVERY	Yes	No	N/A	Notes or Comments
Are BC/DR tests conducted at least annually?	☐ **X**	☐	☐	All DR/BC plans are reviewed, and tabletop tested yearly, or whenever there is a significant change to the environment. The full functional test should include all DR/BC points of contact. A formal test plan must be developed prior to the functional test, and test procedures are developed to include key sections of the DR/BC, including the following: •Notification procedures; •System recovery on an alternate platform from backup media; •Internal and external connectivity; and Reconstitution procedures. Results of the test are documented in an After Action Report, and Lessons Learned are developed for updating information in the DR/BC.
Is there a Pandemic Plan?	☐ **X**	☐	☐	Jama can operate remotely.
Is a Business Impact Analysis conducted at least annually?	☐ **X**	☐	☐	
Is there insurance coverage for business interruptions or general services interruption?	☐ **X**	☐	☐	

COMPLIANCE	Yes	No	N/A	Notes or Comments
Is there an internal audit, risk management or compliance department with responsibility for identifying and tracking resolution of outstanding regulatory issues?	☐ X	☐	☐	
Is there an internal compliance and ethics reporting mechanism and training program for employees to report compliance issues?	☐ X	☐	☐	

MOBILE	Yes	No	N/A	Notes or Comments
Are mobile devices used to access Scoped Systems and Data?	☐	☐ X	☐	We do not allow scoped data to be stored on a mobile device. Limited access to scoped systems is permitted via mobile devices, such as SSH or secure websites.

PRIVACY	Yes	No	N/A	Notes or Comments
Is Scoped Data transmitted, processed, or stored that can be classified as non-public information (NPI), personally identifiable information (PII), or sensitive customer financial information? If yes, describe and list types of data.	☐ X	☐	☐	Data types can be found under https://www.jamasoftware.com/privacy/
Is Scoped Data transmitted, processed, or stored that can be classified as protected health information, electronic health records, or personal health records? If yes, identify the classifications.	☐ X	☐	☐	The solution can store this type of information, however it's at the discretion of the organization purchasing our solution and is not controlled by Jama.
For Scoped Data, is personal information about individuals transmitted to or received from countries outside the United States? If yes, identify the countries.	☐	☐ X	☐	Jama does not permit the removal or transfer of data outside of our hosting systems. The customer can designate a physical location to store their users' personal data. Jama offers a hosted service in North America.
For Scoped Data is there a dedicated person (or group) responsible for privacy compliance. If yes, describe. If no, explain reason	☐ X	☐	☐	We have a dedicated security director responsible for privacy compliance.
For Scoped Data, is there a documented privacy policy or procedures to protect confidential information?	☐ X	☐	☐	Information on privacy and procedures can be found under https://www.jamasoftware.com/privacy/

PRIVACY	Yes	No	N/A	Notes or Comments
For Scoped Data are there regular privacy risk assessments conducted? If yes, provide frequency and scope. If no, explain reason.	☐ X	☐	☐	Internally we scan our application for vulnerabilities on a quarterly basis. In addition to our own expertise within our Development, Quality and DevOps teams to provide our clients with a secure application, we contract with a third-party vendor that provides us with a detailed report once a year.
Is there formal privacy awareness training for employees, contractors, and third-party users to ensure confidentiality and privacy of Scoped Data?	☐ X	☐	☐	Each employee who handles sensitive data is contractually bound to maintain customer confidentiality and trained on the intricacies of handling sensitive data.
Is there a formal process for reporting and responding to privacy complaints or privacy incidents for Scoped Data? If yes, describe. If no, explain reason.	☐ X	☐	☐	Information on privacy and procedures can be found under https://www.jamasoftware.com/privacy/
Is there a data classification and retention program for Scoped Data that identifies the data types that require additional management and governance?	☐ X	☐	☐	We have retention rules in place based on data types. Data is removed at the earliest timepoints within legal constructs.
Is there a documented response program to address privacy incidents, unauthorized disclosure, unauthorized access or breach of Scoped Data?	☐ X	☐	☐	Information on privacy and procedures can be found under https://www.jamasoftware.com/privacy/
Is Scoped Data disclosed to third parties? If yes, describe	☐	☐ X	☐	
Is Scoped Data disclosed to third parties outside of the U.S.? If yes, describe.	☐	☐ X	☐	
Are there contractual controls to ensure that Scoped Data shared with third parties is limited to defined parameters for access, use and disclosure? If yes, describe the controls, If no, explain reason.	☐	☐	X ☐	
Is there a business associate contract in place to address obligations for the privacy and security requirements of the services provided?	☐	☐	☐ X	The standard MSA includes language addressing obligations to protect sensitive data.

PRIVACY	Yes	No	N/A	Notes or Comments
Is there a documented privacy program with administrative, technical, and physical safeguards for the protection of Scoped Data?	☐ **X**	☐	☐	
Is there a process for ensuring the accuracy of Scoped Data at the direction of the client? If yes, describe. If no, explain reason.	☐	☐	☐ **X**	The solution can store this type of information, however it's at the discretion of the organization purchasing our solution and is not controlled by Jama.
Is there a process to ensure that the personal information provided by an individual is limited for the purposes described in the respondent's privacy notice? If yes, describe. If no, explain reason.	☐ **X**	☐	☐	
Are constituents regularly monitored for privacy compliance? If yes, describe. If no, explain reason.	☐ **X**	☐	☐	Yes. We conduct regular audits of our access logs to proactively detect any misconduct with regards to privacy compliance.
Are there documented policies, procedures, and controls to limit access based on need to know or minimum necessary for constituents? If yes, describe.	☐ **X**	☐	☐	Jama restricts access to our production systems on an 'as needed' basis. All access must be approved and is audited regularly.
Are enforcement mechanisms applied to constituents who violate privacy policies or confidentiality requirements?	☐ **X**	☐	☐	
Are transactions for covered accounts accessed, modified, or processed, including address changes and discrepancies? If yes, describe.	☐	☐	☐ **X**	
Is customer data accessed, transmitted, processed, or stored that can be classified as consumer report information provided by a consumer reporting agency?	☐	☐ **X**	☐	

SOFTWARE APPLICATION SECURITY	Yes	No	N/A	Notes or Comments
Is software provided?	☐ X	☐	☐	
Is there a secure software development lifecycle policy that has been approved by management, communicated to appropriate constituents and an owner to maintain and review the policy?	☐ **X**	☐	☐	Jama tests for OWASP top 10. We also perform peer code reviews, full QA testing of all changes, and periodic code security scans. See attached security overview document in the zip file.

CLOUD SECURITY	Yes	No	N/A	Notes or Comments
Are Cloud Services provided? If yes, what service model and deployment model is provided (select all that apply):	☐ X	☐	☐	
Software as a Service (SaaS)	☐ X	☐	☐	
Platform as a Service (PaaS)	☐	☐	☐ X	
Infrastructure as a Service (IaaS)	☐	☐	☐ X	
Private cloud	☐	☐	☐ X	
Public cloud	☐ X	☐	☐	
Community cloud	☐	☐	☐ X	
Hybrid cloud	☐	☐	X ☐	
Can clients define the legal jurisdictions where their data can be transmitted, processed or stored?	☐	☐ X	☐	
Is data segmentation and separation capability between clients provided? If yes, describe.	☐ X	☐	☐	Jama's SaaS hosting is done in a multi-tenant environment, however each tenant has a dedicated database instance and a virtual application profile allowing for each customer to have unique configurations for their authentication settings, database settings, attachment storage path, and other customer specific configurations.
Is Scoped Data encrypted?	☐ X	☐	☐	
Are clients provided with the ability to generate a unique encryption key?	☐	☐ X	☐	
Are clients provided with the ability to rotate their encryption key on a scheduled basis?	☐	☐ X	☐	
Is standards based federated ID capability available to clients (e.g., SAML, OpenID)?	☐ X	☐	☐	SAML
Are application self-service features or an Internet accessible self-service portal available to clients? If yes, describe.	☐	☐ X	☐	

CLOUD SECURITY	Yes	No	N/A	Notes or Comments
Is there a management approved process to ensure that image snapshots containing Scoped Data are authorized prior to being snapped?	☐	☐ X	☐	
Is there a cloud audit program to address client audit and assessment requirements? If yes, describe.	☐	☐ X	☐	
Is an agile development methodology in operation?	☐ X	☐	☐	Process documentation available upon request.
Is there a formal process to ensure clients are notified prior to changes being made which may impact their service? If yes, describe.	☐ X	☐	☐	
Is there a scheduled maintenance window? If yes, what is the frequency?	☐ X	☐	☐	This can vary but typically is around an hour.
Is there a scheduled maintenance window which results in client downtime, If yes, what is the period of the downtime?	☐ X	☐	☐	The monthly maintenance can require 2 hours of downtime.
Is there an online incident response status portal which outlines planned and unplanned outages? If yes, how long after an unplanned outage is this updated?	☐ X	☐	☐	For unplanned maintenance, our Ts & Cs require us to provide 24 hours notice.
Is there a 24x7x365 staffed phone number available to clients to report security incidents?	☐ X	☐	☐	
Are applications created and released into production? If yes, what is the release frequency?	☐ X	☐	☐	The Jama Connect application is updated once per month.
Is there an automated secure source code review? If yes, what is the frequency?	☐ X	☐	☐	Minimum of once a year.
Is source code security reviewed manually? If yes, what is the frequency?	☐ X	☐	☐	Manual security review is performed with every peer review prior to check-in.
Are automated penetration tests performed? If yes, what is the frequency?	☐	☐ **X**	☐	We perform annual penetration tests, but they are not automated.
Are clients provided with the ability to specify where their data will be stored? If yes, describe at what level (e.g., data center, country)?	☐ **X**	☐	☐	Yes, if hosted, the customer can select from a data storage location in North America, Europe and Asia Pacific.
Does the ability exist to legally demonstrate sufficient data segmentation, in the event of a client subpoena or a forensics incident, so as not to impact other client's data? If using resource pooling?	☐ **X**	☐	☐	Jama can provide an export of the specific customer's database to retain current state.

CLOUD SECURITY	Yes	No	N/A	Notes or Comments
Is there a self-service portal or API call available to clients which provides the ability to place a &&&Legal hold&&& on client data which may be subject to a legal action, without impacting other client's data retention or destruction schedules?	☐	☐ X	☐	Jama can provide an export of the database to retain current state.
Is a Cloud API available to clients?	☐ X	☐	☐	
Is there a client management portal which allows distributed business accounts (business units/departments) to be managed under a single central corporate account?	☐ X	☐	☐	We leverage AWS management console.
Are staff required to use two factor authentication to remotely access the production cloud environment containing Scoped Data?	☐ X		☐	
Are staff able to access client Scoped Data in an unencrypted state?	☐ X		☐	Staff can access client's data via the Jama application interface upon receiving client permission.
Are staff able to access client's encryption key?	☐	☐ X	☐	
Is there a process which allows the client to specifically list who from the cloud provider, will have access to their Scoped Systems and Data? If yes, describe.	☐	☐ X	☐	
Are staff technically prevented from accessing the cloud environment via non-managed private devices?	☐ X	☐	☐	
Are there controls to prevent one client attempting to compromise another client in a resource pooled environment? If yes, describe.	☐	☐	☐	Local firewall rules and anti-malware agents.
Is a default hardened base virtual image available to clients?	☐	☐	☐	
Can clients run their own security services within their own cloud environment? If yes, describe.	☐	☐ X	☐	
Is there a specific Recovery Time Objective(s) (RTO)? If yes, specify the RTO for the scoped services.	☐ X	☐	☐	Our current RTO is 30 minutes for failures within AWS. Our RTO for failures where we must move outside of AWS is 4 hours.
Are the failover sites for the underlying infrastructure running on different vendor physical systems?	☐	☐ X	☐	
Is the critical infrastructure running active/active at two or more sites?	☐	☐ X	☐	
Are sites failed over as part of normal operation or as part of a test? If yes, what is the frequency?	☐	☐ X	☐	

CLOUD SECURITY	Yes	No	N/A	Notes or Comments
Are all suppliers of critical hardware, network services and facility services involved in annual continuity and recovery tests?	☐ X	☐	☐	Our hosting provider, AWS, performs regular continuity and recovery tests on their services.
Are all critical technology service providers described on an architecture diagram that includes physical systems and facilities?	☐ X	☐	☐	
Is there sufficient redundancy capacity to ensure services are not impacted in multi-tenancy environments during peak usage and above?	☐ X	☐	☐	
Do contracts include a penalty or remediation clause for breach of availability and continuity SLAs?	☐ X	☐	☐	
Is a Hypervisor used to manage systems used to transmit, process or store Scoped Data? If yes, describe the controls used to protect the hypervisor and the managed Guest Operating Systems.	☐ X	☐	☐	Yes. Jama uses Amazon Web Services (AWS) which controls the hypervisor.