ANNEX II

SECURITY PRINCIPLE AND CRITERIA TABLE

The following controls may be modified from time to time as appropriate to provide an equal or better level of security:

Control #	Control Activity Specified by Intapp
CONTROL ENVIRONMENT	
CC1.1 COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	
CC1.1.1	Documented policies and procedures are in place to guide personnel in the entity's security, availability, and confidentiality commitments and the associated system requirements. The policies and procedures are communicated to internal personnel via the company intranet.
CC1.1.2	Employees are required to sign and acknowledge a confidentiality statement agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties.
CC1.1.3	Policies are documented and maintained that address remedial actions for lack of compliance with policies and procedures.
CC1.1.4	Employment candidates undergo a background screening as a component of the hire process.
CC1.2 COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	
CC1.2.1	The board of directors establishes and maintains a formal charter and set of bylaws which describes their responsibilities and oversight of management's system of internal control.
CC1.2.2	The board of directors has sufficient members who are independent from management and objective in evaluations and decision making.
CC1.2.3	Board of directors and committee meetings are held on at least a quarterly basis to review internal control performance.
CC1.3 COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	
CC1.3.1	Organizational charts are in place to communicate the defined key areas of authority, responsibility, and lines of reporting to personnel related to the design, development, implementation, operation, maintenance, and monitoring of the system. These charts are communicated to employees and updated as needed.
CC1.3.2	Documented job descriptions are in place to establish and define the structure, reporting lines, and authorities and responsibilities for employment positions.
CC1.3.3	Management has assigned the responsibility of the maintenance and enforcement of the entity's security, availability, and confidentiality policies and procedures to the security committee.
CC1.4 COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	
CC1.4.1	New employee hiring documentation is in place to guide the hiring process and include verification that candidates possess the required qualifications to perform the duties as outlined in the job description.
CC1.4.2	Employment candidates undergo a background screening as a component of the hire process.
CC1.4.3	Training courses are available to new and existing employees to maintain and advance the skill level of personnel.
CC1.4.4	Employees are required to complete security awareness training at least annually.
CC1.4.5	Policies are documented and maintained that address remedial actions for lack of compliance with policies and procedures.

CC.1.4.6	Personnel are evaluated on an annual basis to ensure that they have the skills and knowledge to perform their job responsibilities.
CC1.5 COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	
CC1.5.1	Responsibility for controls is clearly assigned to roles in the organization through documented procedures.
CC1.5.2	Documented job descriptions are in place to establish and define the structure, reporting lines, and authorities and responsibilities for employment positions.
CC1.5.3	Policies are documented and maintained that address remedial actions for lack of compliance with policies and procedures.
CC1.5.4	Personnel are evaluated on an annual basis to ensure that they have the skills and knowledge to perform their job responsibilities.
COMMUNICATION AND INFORMATION	
CC2.1 COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	
CC2.1.1	An information security policy is formally documented and reviewed on an annual basis that identifies information required to support the functioning of internal control and achievement of objectives and associated protection, access rights, and retention requirements.
CC2.1.2	Vulnerability assessments are performed by Intapp SOC personnel on a quarterly basis to identify the functionality of control activities, and remediation plans are proposed and tracked through resolution.
CC2.1.3	Annual penetration testing is performed by a third-party vendor, and remediation plans are proposed and tracked through resolution.
CC2.1.4	The entity's IT security group monitors the security impact of emerging technologies and the impact of changes to applicable laws or regulations are considered by senior management.
CC2.1.5	Management reviews audit reports from third-party service providers on an annual basis to help ensure compliance with security, availability and confidentiality commitments and system requirements.
CC2.2 COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	
CC2.2.1	Documented policies and procedures are in place to guide personnel in the entity's security, availability, and confidentiality commitments and the associated system requirements. The policies and procedures are communicated to internal personnel via the company intranet.
CC2.2.2	Employees are required to acknowledge their security responsibilities upon hire and on an annual basis thereafter.
CC2.2.3	Documented job descriptions are in place to establish and define the structure, reporting lines, and authorities and responsibilities for employment positions.
CC2.2.4	Documented escalation procedures for reporting security, availability, or confidentiality incidents are provided to internal users to guide users in identifying and reporting failures, incidents, concerns, and other complaints.
CC2.2.5	Management holds a quarterly company-wide strategy meeting that discusses and aligns internal control responsibilities, performance measures and incentives with company business objectives.
CC2.2.6	Employees are required to sign and acknowledge a confidentiality statement agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties.
CC.2.2.7	Security committee meetings are held on a quarterly basis to discuss ongoing objectives and their effect on the system.
CC2.3 COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	
CC2.3.1	Information regarding the design and operation of the system and its boundaries is communicated to external users via the company website.
CC2.3.2	The entity's security, availability, and confidentiality commitments and the associated system requirements are documented in customer contracts and on the company website.

CC2.3.3	Customer notifications are provided using the cloud services status webpage.
RISK ASSESSMENT	
CC3.1 COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	
CC3.1.1	Documented policies and procedures are in place to guide personnel in identifying business objective risks, assessing changes to the system, and developing risk management strategies as a part of the risk assessment process.
CC3.1.2	Management formally documents and reviews the company's security objectives to help ensure they align with the company's mission and are utilized as part of the annual risk assessment process.
CC3.1.3	Management holds a quarterly company-wide strategy meeting that discusses and aligns internal control responsibilities, performance measures and incentives with company business objectives.
CC3.2 COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	
CC3.2.1	Documented policies and procedures are in place to guide personnel in identifying business objective risks, assessing changes to the system, and developing risk management strategies as a part of the risk assessment process.
CC3.2.2	A formal risk assessment is performed on an annual basis. Risks that are identified are rated using a risk evaluation process and are formally documented, along with mitigation strategies, for management review.
CC3.2.3	The risk assessment includes the analysis of potential threats and vulnerabilities introduced from doing business with vendors and business partners.
CC3.2.4	Vulnerability assessments are performed by Intapp SOC personnel on a quarterly basis and results are included in the risk assessment, and remediation plans are proposed and tracked through resolution.
CC3.3 COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	
CC3.3.1	Documented policies and procedures are in place to guide personnel in identifying the potential for fraud as part of the risk assessment process.
CC3.3.2	A formal risk assessment is performed on an annual basis that considers the potential for fraud. Risks that are identified are rated using a risk evaluation process and are formally documented, along with mitigation strategies, for management review.
CC3.4 COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	
CC3.4.1	A formal risk assessment is performed on an annual basis that considers the impact of changes to the system. Risks that are identified are rated using a risk evaluation process that accounts for changes in risk from the prior year, and are formally documented, along with mitigation strategies, for management review.
CC3.4.2	The entity's IT security group monitors the security impact of emerging technologies and the impact of changes to applicable laws or regulations are considered by senior management.
CC3.4.3	Management reviews audit reports from third-party service providers on an annual basis to help ensure compliance with security, availability and confidentiality commitments and system requirements.
CC3.4.4	Security committee meetings are held on a quarterly basis to discuss ongoing objectives and their effect on the system.
MONITORING ACTIVITIES	
CC4.1 COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	
CC4.1.1	Vulnerability assessments are performed by Intapp SOC personnel on a quarterly basis to identify the functionality of control activities, and remediation plans are proposed and tracked through resolution.
CC4.1.2	Annual penetration testing is performed by a third-party vendor, and remediation plans are proposed and tracked through resolution.

CC4.1.3	Management reviews audit reports from third-party service providers on an annual basis to help ensure controls are operating effectively and any identified risks are addressed.
CC4.1.4	Documented escalation procedures for reporting security, availability, or confidentiality incidents are provided to internal users to guide users in identifying and reporting failures, incidents, concerns, and other complaints.
CC4.1.5	Monitoring applications are utilized to monitor system performance and are configured to send automated alerts to DevOps personnel when predefined thresholds have been exceeded.
CC4.1.6	An internal compliance assessment is completed on an annual basis. The assessment results are documented and reviewed by management.
CC4.1.7	Management compiles and provides internal control performance metrics to the security committee on a quarterly basis. These metrics are formally documented in the internal control performance dashboard for committee review.
CC4.2 COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	
CC4.2.1	Vulnerability assessments are performed by Intapp SOC personnel on a quarterly basis to identify the functionality of control activities, and remediation plans are proposed and tracked through resolution.
CC4.2.2	Annual penetration testing is performed by a third-party vendor, and remediation plans are proposed and tracked through resolution.
CC4.2.3	Management compiles and provides internal control performance metrics to the security committee on a quarterly basis. These metrics are formally documented in the internal control performance dashboard for committee review.
CONTROL ACTIVITIES	
CC5.1 COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	
CC5.1.1	Documented policies and procedures are in place to guide personnel in the assessment of the potential risks and vulnerabilities and the development of control activities related to the security, availability, and confidentiality of data and service.
CC5.1.2	A formal risk assessment is performed on an annual basis to assess the potential risks, vulnerabilities, and control activities related to the security, availability, and confidentiality of data and service.
CC5.2 COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	
CC5.2.1	Control activities over technology are identified as part of the annual risk assessment process to support the achievement of objectives and are documented within the risk assessment report.
CC5.3 COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	
CC5.3.1	Documented policies and procedures are in place to guide personnel in the entity's security, availability, and confidentiality commitments and the associated system requirements. The policies and procedures are communicated to internal personnel via the company intranet.
CC5.3.2	Policies are documented and maintained that address remedial actions for lack of compliance with policies and procedures.
CC5.3.3	Employees are required to complete security awareness at least annually.
LOGICAL AND PHYSICAL ACCESS CONTROLS	
CC6.1 The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	
CC6.1.1	Production system user access requests are documented in a ticket and require the approval of management.

CC6.1.2	The in-scope systems are configured to authenticate users with unique user credentials and enforce predefined user account and minimum password requirements or SSH private key authentication.
CC6.1.3	Predefined security groups are utilized to assign role-based access privileges and segregate access to data within the in-scope systems.
CC6.1.4	Administrative access privileges to the in-scope systems are restricted to user accounts accessible by authorized personnel.
CC6.1.5	The in-scope systems are configured to enforce multi-factor authentication to access the production environment.
CC6.1.6	A log monitoring system is utilized to monitor and log events for certain in-scope systems that include, but are not limited to, the following: · Account management · Logon events · Policy change · Privileged use
CC6.1.7	Employees are required to acknowledge their security responsibilities upon hire and on an annual basis thereafter.
	AWS and Microsoft Azure are responsible for managing logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services where the Intapp OnePlace and DealCloud Platform systems reside.
CC6.2 Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	
CC6.2.1	Production system user access requests are documented in a ticket and require the approval of management.
CC6.2.2	System access to the in-scope production systems is revoked upon termination of employment.
CC6.2.3	User access reviews are performed on an annual basis to ensure that access to data is restricted.
	AWS and Microsoft Azure are responsible for managing logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services where the Intapp OnePlace and DealCloud Platform systems reside.
CC6.3 The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	
CC6.3.1	Production system user access requests are documented in a ticket and require the approval of management.
CC6.3.2	The in-scope systems are configured to authenticate users with unique user credentials and enforce predefined user account and minimum password requirements or SSH private key authentication.
CC6.3.3	Predefined security groups are utilized to assign role-based access privileges and segregate access to data within the in-scope systems.
CC6.3.4	Administrative access privileges to the in-scope systems are restricted to user accounts accessible by authorized personnel.
CC6.3.5	User access reviews are performed on an annual basis to ensure that access to data is restricted.
	AWS and Microsoft Azure are responsible for managing logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services where the Intapp OnePlace and DealCloud Platform systems reside.
CC6.4 The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	
	AWS and Microsoft Azure are responsible for restricting physical access to data center facilities, backup media, and other system components including firewalls, routers, and servers.

CC6.5 The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	
	AWS and Microsoft Azure are responsible for restricting physical access to data center facilities, backup media, and other system components including firewalls, routers, and servers.
	AWS and Microsoft Azure are responsible for managing logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services where the Intapp OnePlace and DealCloud Platform systems reside.
CC6.6 The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	
CC6.6.1	A firewall system is in place to filter unauthorized inbound network traffic from the Internet.
CC6.6.2	Security groups and NSGs acting as a firewall system are in place to restrict inbound and outbound traffic.
CC6.6.3	Security personnel review the security group and NSG rulesets on at least an annual basis.
CC6.6.4	Web servers utilize transport layer security (TLS) encryption for web communications.
CC6.6.5	Encrypted VPNs are required for remote access to production and enforce username and password for authentication.
CC6.6.6	Vulnerability assessments are performed by Intapp SOC personnel on a quarterly basis to identify the functionality of control activities, and remediation plans are proposed and tracked through resolution.
CC6.6.7	Annual penetration testing is performed by a third-party vendor, and remediation plans are proposed and tracked through resolution.
CC6.6.8	An intrusion detection system (IDS) is utilized to analyze and report network events and to block suspected or actual network security breaches.
CC6.6.9	Security monitoring tools are configured to alert SOC team for possible or actual security breaches.
CC6.6.10	Production databases are configured to encrypt data at rest.
	AWS and Microsoft Azure are responsible for managing logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services where the Intapp OnePlace and DealCloud Platform systems reside.
CC6.7 The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	
CC6.7.1	Policies are in place that prohibit the transmission of sensitive information over the Internet or other public communications paths unless it is encrypted.
CC6.7.2	Web servers utilize TLS encryption for web communications.
CC6.7.3	Encrypted VPNs are required for remote access to production and enforce username and password for authentication.
CC6.7.4	The automated backup systems are configured to encrypt backup media.
	AWS and Microsoft Azure are responsible for implementing controls for the transmission, movement, and removal of the underlying storage devices for its cloud hosting services where Intapp OnePlace and DealCloud systems reside.
CC6.8 The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	
CC6.8.1	Cloud-based endpoint protection software is configured to protect registered production servers and workstations in real-time.
CC6.8.2	Vulnerability assessments are performed by Intapp SOC personnel on a quarterly basis to identify the functionality of control activities, and remediation plans are proposed and tracked through resolution.
CC6.8.3	File integrity monitoring tool is in place to monitor, detect, and alert upon unauthorized software installation or configuration changes to certain production systems.
SYSTEM OPERATIONS	

CC7.1 To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	
	AWS and Microsoft Azure are responsible for monitoring any configuration changes of the logical access controls system for the underlying network, virtualization management, and storage devices where Intapp OnePlace and DealCloud systems reside.
CC7.1.1	The DevOps team has formally documented standard build procedures for installation and maintenance of production servers.
CC7.1.2	Vulnerability assessments are performed by Intapp SOC personnel on a quarterly basis to identify the functionality of control activities, and remediation plans are proposed and tracked through resolution.
CC7.1.3	Annual penetration testing is performed by a third-party vendor, and remediation plans are proposed and tracked through resolution.
CC7.1.4	Security personnel review the security group and NSG rulesets on at least an annual basis.
CC7.2 The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	
	AWS and Microsoft Azure are responsible for monitoring any configuration changes of the logical access controls system for the underlying network, virtualization management, and storage devices where Intapp OnePlace and DealCloud systems reside.
CC7.2.1	Documented escalation procedures for reporting security, availability, or confidentiality incidents are provided to internal users to guide users in identifying and reporting failures, incidents, concerns, and other complaints.
CC7.2.2	A log monitoring system is utilized to monitor and log events for certain in-scope systems that include, but are not limited to, the following: • Account management • Logon events • Policy change • Privileged use
CC7.2.3	Monitoring applications are utilized to monitor system performance and are configured to send automated alerts to DevOps personnel when predefined thresholds have been exceeded.
CC7.2.4	Vulnerability assessments are performed by Intapp SOC personnel on a quarterly basis to identify the functionality of control activities, and remediation plans are proposed and tracked through resolution.
CC7.2.5	An IDS is utilized to analyze and report network events and to block suspected or actual network security breaches.
CC7.2.6	Security monitoring tools are configured to alert SOC team for possible or actual security breaches.
CC7.3 The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	
CC7.3.1	Documented escalation procedures for reporting security, availability, or confidentiality incidents are provided to internal users to guide users in identifying and reporting failures, incidents, concerns, and other complaints.
CC7.3.2	Automated and manual systems are utilized to document and track security incidents and remediation activities.
CC7.3.3	Incidents requiring a change to the system follow the standard change control process.
CC7.3.4	An IDS is utilized to analyze and report network events and to block suspected or actual network security breaches.
CC7.3.5	Security monitoring tools are configured to alert SOC team for possible or actual security breaches.
CC7.4 The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	

CC7.4.1	Documented escalation procedures for reporting security, availability, or confidentiality incidents are provided to internal users to guide users in identifying and reporting failures, incidents, concerns, and other complaints.
CC7.4.2	Automated and manual systems are utilized to document and track security incidents and remediation activities.
CC7.4.3	Security committee meetings are held on a quarterly basis to discuss the effect of identified security vulnerabilities on the ability to meet business objectives and to identify corrective measures.
CC7.5 The entity identifies, develops, and implements activities to recover from identified security incidents.	
CC7.5.1	Documented escalation procedures for reporting security, availability, or confidentiality incidents are provided to internal users to guide users in identifying and reporting failures, incidents, concerns, and other complaints.
CC7.5.2	Automated and manual systems are utilized to document and track incidents and remediation activities.
CC7.5.3	Security committee meetings are held on a quarterly basis to discuss the effect of identified security vulnerabilities on the ability to meet business objectives and to identify corrective measures.
CHANGE MANAGEMENT	
CC8.1 The entity authorizes, designs, develops, or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	
CC8.1.1	Change management policies and procedures are in place to guide personnel in change management procedures through the change lifecycle.
CC8.1.2	A change management meeting is held on a weekly basis to discuss and communicate the ongoing and upcoming projects that affect the system.
CC8.1.3	A change tracking system is in place to centrally document, manage, and monitor changes from change requests through implementation.
CC8.1.4	Changes are authorized, peer reviewed, tested, and approved prior to implementation.
CC8.1.5	Development and test environments are logically separated from the production environment.
CC8.1.6	Version control software is utilized to restrict access to application source code and provide rollback capabilities.
CC8.1.7	The version control software is configured to restrict users from merging or deploying code without secondary approval.
CC8.1.8	The ability to modify application source code is restricted to user accounts accessible by authorized personnel.
CC8.1.9	The ability to implement changes into the production environment is restricted to user accounts accessible by authorized non-development personnel.
CC8.1.10	Administrative access privileges within the version control software are restricted to user accounts accessible by authorized personnel.
CC8.1.11	Client data is not utilized for application change control development or testing.
CC8.1.12	File integrity monitoring tool is in place to monitor, detect, and alert upon unauthorized software installation or configuration changes to certain production systems.
RISK MITIGATION	
CC9.1 The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	
CC9.1.1	Documented policies and procedures are in place to guide personnel in the assessment of the potential risks and vulnerabilities and the development of control activities related to the security, availability, and confidentiality of data and service.
CC9.1.2	A formal risk assessment is performed on an annual basis that considers potential business disruptions. Risks that are identified are formally documented for management review and includes the objectives and associated risks that address the security, confidentiality, integrity, and availability of the in-scope systems.

CC9.1.3	Disaster recovery and business continuity plans are in place to guide personnel in procedures to protect against disruptions caused by an unexpected event.
CC9.1.4	Risk mitigation activities consider the use of insurance to offset the financial impact of loss events that would otherwise impair the ability of the entity to meet its objectives.
CC9.2 The entity assesses and manages risks associated with vendors and business partners.	
CC9.2.1	A vendor management policy is in place that addresses the following: • Due diligence process prior to accepting new vendors or business partners • Monitoring process to review vendor and business partner compliance on a periodic basis • Termination of contracts
CC9.2.2	Confidentiality agreements are required to be in place with third parties prior to sharing information designated as confidential.
CC9.2.3	Management reviews audit reports from third-party service providers on an annual basis to help ensure compliance with security, availability and confidentiality commitments and system requirements.

Additional Criteria for Availability

Control #	Control Activity Specified by Intapp
A1.1 The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.	
	AWS and Microsoft Azure are responsible for ensuring capacity demand controls are in place to meet Intapp's availability commitments and requirements.
A1.1.1	Monitoring applications are utilized to monitor system performance and are configured to send automated alerts to DevOps personnel when predefined thresholds have been exceeded.
A1.1.2	Security committee meetings are held on a quarterly basis to review availability trends.
A1.2 The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.	
	AWS and Microsoft Azure are responsible for ensuring environmental protection controls are in place to meet Intapp's availability commitments and requirements.
A1.2.1	An automated backup system is in place to perform scheduled backups of production databases on a daily basis.
A1.2.2	The automated backup system is configured to replicate production databases to multiple regions.
A1.2.2	The automated backup system is configured to notify DevOps personnel regarding the failure of backup jobs.
A1.2.3	Disaster recovery and business continuity plans are in place to guide personnel in procedures to protect against disruptions caused by an unexpected event.
A1.3 The entity tests recovery plan procedures supporting system recovery to meet its objectives.	
A1.3.1	DevOps personnel perform restorations from backup files as a component of standard business operations.
A1.3.2	A disaster recovery plan exercise is performed and tested on an annual basis.

Additional Criteria for Confidentiality

Control #	Control Activity Specified by Intapp
C1.1 The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.	

C1.1.1	The entity's confidentiality, data retention and disposal commitments, and the associated system requirements are documented in customer contracts and on the company website.
C1.1.2	Documented data retention policies are in place to guide personnel on the procedures for retention of customer data.
C1.1.3	Product management reviews the retention of customer data on an annual basis to verify that customer data is retained in accordance with data retention commitments.
C1.2 The entity disposes of confidential information to meet the entity's objectives related to confidentiality.	
C1.2.1	The entity's confidentiality, data retention and disposal commitments, and the associated system requirements are documented in customer contracts and on the company website.
C1.2.2	Documented disposal policies are in place to guide personnel on the procedures for disposal of customer data.
C1.2.3	Product management reviews the disposal of customer data on an annual basis to verify that customer data is disposed of in accordance with data disposal commitments.
C1.2.4	A customer data destruction ticket is completed to track the disposal of customer data upon termination of the services in accordance with the documented data disposal commitments.