Advarra Cloud Services Specification

Overview: The Advarra Cloud Services Specification details the cloud environment provided by Advarra ("Advarra Cloud") and the various services supported, including the service definitions, service levels, security policies, and customer responsibilities. This document does not address product support terms, which can be found in the **Advarra Support & Maintenance Services** document. This specification is an addendum for and subject to the Advarra Cloud Master Services Agreement (or the Advarra Cloud Addendum for existing customers) ("Agreement") for customers who have purchased the relevant solution(s) via an Advarra Order Form.

Table of Contents

Advarra Cloud Services Specification

1. Introduction

The Advarra Cloud is a purpose-built life sciences cloud platform to improve the delivery of applications to automate, streamline, connect, and expedite processes across the clinical trial lifecycle. Advarra Cloud consists of several on-demand services that support the lifecycle of clinical trials. Current services (or Current service offerings) are: 1) the Center for IRB Intelligence Platform (CIRBI). 2) Next-generation technology solutions that automate, streamline, and expedite processes across the clinical trial lifecycle in the form of OnCore and Clinical Conductor as Clinical Trial Management Suites. 3) Finally, platforms for the research site community including cancer treatment centers, academic medical centers, and health systems to provide compliant and confident execution of the protocol by sites, empower and inform study participants, and efficiently manage and monitor studies are provided within one intuitive platform.

In supporting these solutions, the Advarra Cloud allows customers to utilize Advarra solutions in a fully managed and hosted cloud-native environment. Advarra supplies the infrastructure, software, personnel, systems, and processes to provide the Advarra Cloud and solutions from the Advarra product suite. Key customer responsibilities are documented in the Customer Responsibilities subsection. The details of the solution are outlined in the following Service Definition, and, when required, additional detail is outlined in the various subsections of this specification.

2. Service Definition

The Advarra Cloud Services Specification covers the various aspects of the services/offerings running in the Advarra Cloud. The general specifications below apply for all Advarra Cloud offerings. Any offering that includes something specific, or outside the base-level specification, is noted in that offering's specific definition.

The Advarra Cloud provides the following systems, services, and benefits to all participating customers:

- **Infrastructure** - the Advarra Cloud provides the necessary hardware, software, and networking infrastructure to operate and run the associated Advarra application functionality up to the levels described in the customer's specific offering. This includes the necessary storage, operating systems, databases, load balancers, application servers, and related hardware components to host the purchased offering.
- **Instances** - some offerings will provide additional instances or environments (e.g., staging), and those are detailed in the various service offerings.
- **Infrastructure & Application Monitoring** - the Advarra Cloud provides application and infrastructure monitoring. Details of components monitored can be found in the service level terms below. Uptime and other types of system monitoring information on the environment is available for customers via the Advarra Support Portal.
- **Patch & Upgrade Management** - for all hardware, networking, and software components within the Advarra Cloud environment, Advarra provides scheduled patch and upgrade management as part of the Advarra Cloud. Advarra will monitor for applicable updates to supported components and software and schedule updates via the change management procedures outlined in the service specification. Where possible, Advarra Cloud will utilize a Blue-Green Deployment technique to eliminate downtime ("zero-downtime deployments") and reduce risk.
- **Continuity Management, Backup & Disaster Recovery** - Advarra's primary mission is to maintain the continuity of service. A base level of standard security, backup, and disaster recovery (DR) options is included with all Advarra Cloud offerings. The Disaster Recovery & Backup plan is detailed in the Service Level subsection below. Additional system availability and DR options may also be available. These will be detailed in the applicable order form.
- **Logging and Event Management** - the Advarra Cloud provides a modernized event capture and logging infrastructure to provide feedback on all aspects of the Advarra Cloud, including, but not limited to, security, infrastructure, and application events.
- **Security & Access Management** - the Advarra Cloud provides security management services as well as role-based access control for the monitoring and operation of the system. All access to the system is

logged and monitored. Details on the security operations can be found in the Advarra Cloud Security Policy subsection in this document.

- **Customer Secure Access** - Advarra supports SAML integration with leading Identity Providers (IdPs) for secure access and authentication. Additional details are available for connecting to the Advarra Cloud.
- **Security Features** - the Advarra Cloud provides encryption for data in motion between all Advarra Cloud components as well as data at rest within the Advarra Cloud system. This includes key management services for this security, provided by the Advarra Cloud. See the Advarra Cloud SOC 2 report for additional details.
- **Change Management** - There are detailed change management procedures for when and how Advarra will update and maintain the environment. These procedures are documented in the Change Management subsection and include the process for requesting a modification to an existing environment.
- **Customer Support** - the architecture and operation of the Advarra Cloud is designed to help ensure customers' success when using it to run their selected service. Several specific items are included with the Advarra Cloud that ensure the successful operation of the customer's solutions and environment:
    - **Service Management & Customer Support** - 24x7x365 access to the Advarra Support Portal for operations staff and support requests, email, and phone support for the customer's environment.
    - **Strategic Partner** - A Strategic Partner who will deliver personalized guidance to help navigate the customer's Advarra journey.
    - **Product Support** - The product support is outlined in the Advarra Support Terms which covers hours of operation, support level targets, escalation procedures, as well as other standard support terms.
    - **Training & Community Support** - included in all offerings is a level of access to the Onsemble Community which includes access to Advarra University. Advarra University provides online training, demos, and other related training options in an on-demand fashion. The Onsemble Community Portal also provides access to Advarra Product Support (Zendesk), Online Learning Portals, and release plans.
    - **Professional Services** - access to professional services can be coordinated and granted as required. A separate Statement of Work (SOW) may be required.

Additional Service offerings are detailed in the Advarra Cloud Services subsection and details of additional services provided are included there.

3. Advarra Cloud Services

Below are the current offerings available in the Advarra Cloud. Each offering is listed below, along with any specification requirements and/or relevant details for that offering. Again, these are in addition to the general specifications of the Advarra Cloud throughout this specification (unless otherwise noted).

3.1. Current Offerings

The following applications and services are currently available. Please refer to the Advarra Order Form for a definitive list of purchased services for the customer environment.

- **Advarra OnCore CTMS & Billing Compliance** (Biospecimen Management & Patient Registries are available as additional packages)
- **Advarra Research Evaluation System (EVAL)**
- **Advarra eRegulatory Management System (eReg)**
- **Advarra eSource + EDC**
- **Advarra Longboat**
- **Advarra One**
- **Advarra Analytics**

- **Advarra Insights Business Intelligence**
- **Advarra Payments**

For each of the available services, Advarra provides the following offering components that may be specific to each application.

Table 1: Offering Component Details

Offering Components	Details
Instances	• Advarra eREG, EVAL, and eSource+EDC, all ship with two instances: 1-Production and 1-Staging. • Advarra Insights, Payments, and Longboat all ship with one instance: Production. • Advarra OnCore customers will also receive a dedicated Training instance. • Staging and Training instances are defined below.[1]
Protocols	See Advarra Order Form for number of Supported Protocols per application
Backups	Seven days of backups are stored for all applications
Data Recovery Point Objective (RPO)	30 Minutes
Data Recovery Time Objective (RTO)	One Business Day (Does not include any external interface connectivity)

3.2. Validated Applications

Advarra places significant emphasis on providing useful tools that institutions can choose to adopt in the development of an overall compliance program. Advarra Cloud was designed for the life sciences industry with these regulatory requirements front and center. Based on our significant experience in this space, we designed a cloud platform and suite of applications that stay up to date and are easy to validate.

Advarra eRegulatory Management System (Advarra eReg), Advarra Longboat, and Advarra EDC are 21 CFR Part 11 compliant systems that may be used as a standalone system or in conjunction with Advarra's OnCore.

Advarra services operation can provide the validation packages themselves and related services to validate your use of the applications at Advarra. However, Advarra Cloud is an agile development platform that allows for quick response to regulatory changes, as well as complete traceability and auditability of the entire platform across each release.

Further, our solutions are hosted in AWS, a world-class secure hosting facility that is ISO27001 and SOC certified. The Advarra Cloud Specification explains our disaster recovery and business continuity plan in greater detail.

Advarra Cloud tracks every change to the customer environment and produces the necessary Installation Qualification (IQ) documentation for each software release.

4. Release Management

4.1. Release Management for Validated Applications

Advarra validated applications are generally released three times per year; however, the frequency can vary based on impact to the customer or validation environment. Upgrades and releases go through a vigorous testing and validation

[1] Staging and Training Instances are configured with less system resources than a production system, but otherwise technically the same in terms of setup, configuration, and operation. It is not intended for performance testing or substantial user loads.

process before being released to customers. Once ready for customer deployments, the release schedule is formal and is as follows:

1. The customer is notified that a new release has shipped, and an approximate date when upgrades will commence.
2. Customer Staging (Non-Prod) environments are upgraded first if applicable. Customers are notified when the upgrade is available, and if any items require their involvement, they are listed in the Release Impact Assessment by the product organization.
    a. Due to the natures of the software development process most releases do not require customer testing, in situations where customer testing is required Advarra requires that the customer complete their testing within a four-week window (most conservative estimates put the average change taking less than one day to test).
3. At the end of the four-week period[2], production environment upgrades will commence. Customer production environments are upgraded via the standard upgrade and release practices documented in this specification.

For additional information, please speak to your Advarra Customer Success Representative.

NOTE: The 21 CFR Part 11 regulation includes technical controls, procedural requirements, and administrative requirements. Software systems are an important component addressing the technical controls. Developing and implementing procedural and administrative areas of the requisite controls are the responsibility of the institution.

4.2. Release Management for All Other Applications

Advarra Cloud hosts a myriad of applications of different deployment types (e.g., multitenant applications, single tenant applications). In general, Advarra follows a strict release process to move products through various stages after they are officially released and approved for customer usage by our Quality Assurance teams.

Once products are ready for customer deployments, the release schedule is formal and is as follows:

1. The customer is notified that a new release has shipped, and an approximate date when upgrades will commence.
2. Customer Staging (Non-Prod) environments are upgraded first if applicable. Customers are notified when the upgrade is available, and if any items require their involvement, they are listed in the Release Notes by the product organization.

    Depending on the type of application, the software release, and the potential impact to customers, releases will generally stay in the staging environments for a period between two and four weeks for any customer testing that needs to occur.
3. At the end of the period, production environment upgrades will commence. Customer production environments are upgraded via the standard upgrade and maintenance practices documented in this specification.

4.3. Release Management for Central Services

Advarra Cloud hosts a number of central services such as Hub, Tenant Service, Insights, Data Exchange, Payments, Advarra SSO, and more. Like our per customer applications, our shared central services follow a strict release process that includes deployment and testing by our Quality Assurance department.

Once a product is ready for customer facing deployments, the Cloud team is notified of the release, and we schedule staging and production deployments. The time between staging and production deployments differs per product but is generally a period of up to two weeks.

Product teams may communicate the release dates, depending on the product, but in cases where there is no impact, we seamlessly move forward.

[2] In the case of Longboat or other validated applications in the future, if customer testing is not required, production upgrades may occur faster than the four-week windows specified.

5. Advarra Cloud Service Levels

These Service Levels Agreements (SLAs) pertain to the availability of the infrastructure for all Advarra Cloud offerings. This document does not address support services terms on product software, response times, and priority definitions, as these can be found in the **Advarra Support Terms.**

5.1. Service Level Commitments

During each calendar month, the Advarra Cloud will meet or exceed the Availability Requirement, except as expressly set forth below.

Table 2: Monthly Uptime Percentage

Components	Uptime Percentages and Service Credits
Monthly Uptime Percentage	99.5%
Monthly Uptime Percentage Service Credit Ranges and Applicable Credit Determinations	95% - 99.4% 5% of the Monthly Cloud Fee
	< 95% 10% of the Monthly Cloud Fee

5.2. Service Level Definitions

Downtime is calculated as the aggregate time (in minutes) each calendar month, as confirmed by Advarra following written notice from the impacted customer, that the applicable Advarra Cloud Service is experiencing a System Outage (as defined below). The length of Downtime will be measured from the time an incident occurs as confirmed by Advarra until the time when Advarra's testing confirms that the failure condition(s) reported are no longer present. Downtime does not include any failure condition(s) described above which occur due to an Exclusion Event (see below).

Exclusions include:

(1) During Scheduled or emergency system maintenance.

(2) Failure due to a Customer or User's acts or omissions, equipment, internet connectivity, or facilities;

i. including but not limited to (a) performance or non-performance of any services by a third party (other than Advarra) contracted by the customer to provide services to the customer or its users related to the Advarra Cloud Service, (b) any failure that the customer mutually agrees is not due to fault of Advarra or Advarra's contracted third-party service provider, or (c) failure of any code or configurations managed or written by the customer or any third-party vendor to the customer;

(3) The occurrence of a force majeure event.

(4) Internet failure or congestion.

(5) Any defect or failure of any third-party software or hardware that Advarra may agree to host as part of the Advarra Cloud Services offered, including where the manufacturer has discontinued maintenance and support of the third-party software or hardware; or

(6) Failures or other failures caused directly or indirectly by known or unknown computer viruses, worms, or other malicious programs, provided Advarra has not breached any of its obligations here or in the applicable agreement relating to virus protection protocols).

Cloud Fees will be calculated based on 20% of the recurring fees for the directly impacted Advarra Cloud Services(s) during the month in which the applicable performance deficiency occurs, excluding any taxes, one-time fees, third-party fees, travel or expense, professional services, or similar such additional fees divided by 12.

Monthly Uptime Percentage is calculated as the total number of minutes in a calendar month, minus the number of minutes of Downtime in such month, divided by the total number of minutes in such month.

Restoration occurs once access to the Advarra Cloud Services has been restored such that: (1) eligible customer content can again be stored in the Advarra Cloud Service; and (2) new associated customer data (as anticipated by the applicable Advarra Cloud Service(s) impacted) can be input into the Advarra Cloud Service.

System Outage is defined by a loss of network connectivity or system availability resulting in either the Advarra Cloud being not available by the user interface or the ability to authenticate to the interface is lost. An outage excludes the period during a scheduled maintenance window or emergency maintenance obligation.

5.3. Service Level Commitment Terms

Monthly Uptime Percentage - Advarra will meet the Monthly Uptime Percentage, as identified in Table 2 above, during each calendar month.

Downtime Report - Following the occurrence of a Downtime event, upon request by the customer, Advarra shall provide a report which will include, as applicable, a detailed description of the incident, start and end times of the incident, duration of the incident, business/functional impact of the incident, description of remediation efforts taken, and a description of outstanding issues or tasks relating to the incident.

5.4. Exclusive Remedies Terms

Monthly Uptime Percentage - In the event the Monthly Uptime Percentage during any calendar month is less than the applicable Monthly Uptime Percentage set forth in the Table 2 above, the customer shall be eligible to receive the applicable credit against Cloud Fees specified in Table 2 above, provided the customer submitted a technical support request within 24 hours of such Downtime.

Maximum Service Level Credit - Notwithstanding anything to the contrary, customers are only entitled to a maximum of one service level credit for all events occurring in a particular calendar month. The customer shall be entitled to only the largest service level credit that may be payable for one or more of the service level failures occurring in such calendar month.

Application of Service Level Credits - Service level credits will be applied first to any outstanding amounts that are due and owed from the customer, and then to future Cloud Fees.

Termination Remedy - If the customer earns a service level credit either: (i) in two consecutive calendar months, or (ii) in three calendar months during any six consecutive month period; then the customer may, by written notice to Advarra delivered within thirty days after the last credit described in either clause or (i) or (ii) above is earned, terminate the subscription to the Advarra Cloud Service(s) to which the credit(s) specifically apply.

Exclusivity - The remedies set forth above constitute the sole and exclusive remedies available to a customer for any failure to meet the service level commitments set forth in this Specification.

5.5. Availability Calculations

Advarra Cloud Uptime Monitoring – Advarra continuously monitors the user interface to measure uptime availability for the Advarra Cloud.

Monitored System Services – availability monitoring is made up of, but not limited to, the following critical system metrics:

- Firewall and Load Balancer health checks
- Resource Capacity on Servers (CPU/Memory/Disk Space)
- Monitoring the Health of the Operating System
- Monitoring System Logs
- Monitoring Application and Infrastructure Access Logs
- Monitoring Database Health and Performance of Database Indexing
- Monitoring Background Services such as backups
- System-wide Networking Performance Monitoring and Auditing

5.6. Scheduled Maintenance

For the purposes of the Service Level Commitment, Scheduled Maintenance is defined as:

- **Advarra Scheduled Maintenance Windows** - modification or repairs to shared infrastructure or platform patching and upgrades that Advarra has provided notice of at least 72 hours in advance **or** that occurs during 2:00 am to 9:00 am on Saturdays.
- **Scheduled Customer Maintenance** – maintenance of customer configuration that customer requests and that Advarra schedules with customers in advance (either on a case-by-case basis, or based on standing instructions), such as hardware or software upgrades.
- **Scheduled Customer Deployments** – as with maintenance, these are customer requests that Advarra schedules with the customer in advance (either on a case-by-case basis, or based on standing instructions), for the deployment of customizations, add-ons, or new rollouts of services that require the system to be restarted or taken offline.
- **Emergency Maintenance** – critical unforeseen maintenance needed for the security or performance of customer configuration or Advarra's network, where Advarra will use reasonable efforts to provide advance notice of as practical.

5.7. Response Time Definitions - Cloud Environment Operations

*These response targets are focused on requests for the Cloud environment. Please see the **Advarra Support Terms** for general customer support response targets.*

Support Response Time – is defined as the elapsed time between the first contact by an Authorized Support Contact, to report an issue and the target time within which Advarra's personnel report back to the designated support contact authorized to address the issue. Advarra is not responsible for a missed response time SLA if the designated support contact is unavailable and does not respond to the acknowledgement of the receipt of the reported issue. Support Response Time addresses communication time frames only; Advarra does not guarantee a problem fix, workaround, or other final disposition within these timeframes. This also assumes that the issue is properly and fully communicated with all applicable and associated information.

Service Requests Response Commitments – the following matrix covers response and resolution levels for typical customer requested actions related to ongoing operational support and maintenance of the Advarra Cloud for the applicable Advarra solution.

For prioritization and service level targets for production issues such as outages, major impacts, service interruptions, these service levels for the Advarra Cloud follow the Severity Definitions and Service Level Targets as defined in the Advarra Support Terms.

Table 3: Customer Request SLA Matrix

Category	Description/Examples	Response*	Resolution
New Instance Request	Request an additional environment instance after Advarra Order form is processed	Next Business Day	1 Week
Enhancement Requests	Document enhancement request and submit to Advarra Product Management & Engineering for review and feasibility.	1 Week	TBD

* *SLA Response is the confirmation of receipt, initial evaluation of the request and acceptance or request for more information. Business days are defined as 9:00 am-6:00 pm Monday-Friday Eastern Time, excluding any applicable local holidays.*

5.8. Backup & Storage

The Advarra Cloud has a defined backup and recovery framework. The system is designed to provide fault-tolerance and automated restores in most cases. Advarra strives to maintain a fault tolerant system to protect customer data against accidental data loss due to hardware or system failure.

Advarra stores an entire system back-up for 7 days. This backup includes a snapshot of the database, versioning of content with replication, and snapshots of file systems. The following is a detailed listing of the backed-up components and their retention period:

Table 4: Backup & Storage Retention Periods

Components	Retention Period
Content	AWS S3 Versioning & Replication – Length of contract
Database	7 Days
Application Configurations	7 Days (DB and EFS Volume)
Application and Infrastructure Logs	30 Days 1 Year long-term archive for forensic analysis only

5.9. Data Recovery Point Objective (RPO)

Data backup occurs at a fixed point in time according to a schedule specified by Advarra. Any data that is collected or created between backups is vulnerable to data loss. The length of time between backups is the Recovery Point Objective. This is the point back in time to which a customer's data can be recovered. Since backups take up considerable processing and storage resources, RPO levels are set per offering level, and enhanced back-up services are available if required. If a more frequent backup schedule is required than is stated in the offering, it must be pre-arranged with Advarra and may result in some additional fees.

5.10. Data Recovery Time Objective (RTO)

This is the maximum elapsed time required to complete the recovery of customer data. RTO is a function of the size of the data delivery circuit (e.g., an external AZ) and the total amount of data to be recovered.

5.11. Disaster Events and Disaster Recovery

Advarra schedules backups for all instances in the environment. Backup processes are monitored and checked for backup system operation errors, and regularly scheduled tests of the restoration procedures are performed. To ensure the readiness of Advarra's operators to complete the offline restoration process, Advarra runs scheduled drills at regular intervals to test restoration performance, as outlined in the Backup section.

If the Service is disrupted, Advarra will initiate its disaster recovery protocols to help ensure the timely restoration of the Service for the customer base. Depending on the type of disruption that has occurred, Advarra may elect to phase restoration to maximize benefit for its customer base (e.g., first restore the Advarra Service with indexes being rebuilt as required). Any data not immediately accessible after a disruption in the Service will be restored from the most recent backup and made accessible.

5.12. Advarra Cloud Incident and Problem Management Policy

Advarra will provide access to the Advarra Support Portal, which serves as the initial point of contact for incidents, issues, enhancements requests, and new service offerings. Details on accessing the Support Portal, methods of contact, and other related items can be found in the Advarra Support Terms.

5.13. Advarra Cloud Acceptable Use Policy

As a Cloud Platform, continued use of the Service is critical to all our customers. Use is subject to the standard Acceptable Use Policy terms Advarra provides for the Advarra Cloud. We monitor use by each of our customers, and we may adjust or limit usage if we determine any abuse, excessive use or similar events are occurring (such as reducing data flows / ingest that are causing instability in the Advarra Cloud environment).

For the full details of the Advarra Acceptable User Policy, please see the following: https://www.advarra.com/legal-files/Acceptable-Use-Policy-online.pdf

5.14. Advarra Cloud Off-boarding Assistance

In the unfortunate event that a customer wishes to cancel the Service, if requested, Advarra will provide an extract of all customer data within 30 days of termination. The Service will be unavailable after contract termination, and the customer instances and data will be deleted upon transferring of the extract or 30 days if not requested. All customer information, back-ups, data, will be expunged after the off-boarding is complete.

5.15. Advarra Cloud Security Policy

Advarra provides reasonable and appropriate security measures designed to protect the confidentiality, integrity, and availability of customer content hosted in the services utilizing the Advarra Cloud governed by this Advarra Cloud Services Specification.

For full details on the Advarra Technology Solutions Security, please see the following public statement on security, certifications, and controls: https://www.advarra.com/technology-solutions-security/

For Advarra Cloud, Advarra complies with the **SOC 2** required standards, and has conducted external security audits and received a **SOC 2 Type 2** certification for the Advarra Cloud. In addition to all general Advarra information security policies (which apply to our operations generally), the Cloud Security Policies govern all areas of security applicable to the Advarra Cloud.

The SOC 2 Report is available upon request under the confidentiality obligations of the agreement and is subject to any hosting and providers' confidentiality obligations. For additional details on the Advarra Cloud Security Policy or for a discussion with an Advarra information security representative and/or the Advarra Security Officer, please speak to your Advarra representative.

6. Advarra Cloud Customer Responsibilities

The Advarra Cloud Services Specification covers the various aspects of the services/offerings running in the Advarra Cloud

There are a variety of customer requirements to run the various services in the Advarra Cloud. These requirements are detailed below.

6.1. Customer Responsibilities

Customers are responsible for the following activities:

- Managing their access, and any access by their users or third parties, to the Advarra Cloud, and providing reasonable efforts to prevent unauthorized access or use of the Advarra Cloud and Content. (Advarra does not create or manage users or access control).
- Using best efforts to ensure the accuracy, quality, and legality of the data being provided to Advarra. Must ensure content uploaded is free of malware/viruses.
- Ensuring that they do not exceed their usage limits, as well as monitoring the connectivity with the Advarra Cloud infrastructure. Advarra will provide reasonable methods to monitor the health and capacity of the cloud instance.
- Managing passwords for access to the Advarra Cloud.
- Complying with current technical documentation, including API and developer guides if applicable.
- Providing prompt, accurate and detailed notification of any access or functional issues via the Advarra Support Portal to enable Advarra to address and resolve issues efficiently and in a timely manner.

6.2. Customer Technical Requirements for the Advarra Cloud

While we do not have technical requirements that would limit access to the platform, the below items are strongly recommended for our customer's own security and ease of use.

- IdP for Cloud Access or SSO Configuration - customer should provide an IdP that supports the SAML protocol, such as ADFS/Okta for integration with the Advarra Cloud.
- Integration Services will be made secure by the Advarra Cloud. It is our preference that the security of these be maintained, and we will aim to not support any insecure protocols or integration methods.

6.3. Data Access; Unintended Access to Your Data

The Advarra Cloud enables customers to provide access to their data stored in our online services. It is very important that customers carefully work to secure their applications and control access to their environment. If customers do not provide proper access controls, this could cause the customer's confidential information stored in the Advarra Cloud to be disclosed to unintended third parties or to the public.

6.4. Roles and Responsibilities for the Advarra Cloud

The Advarra team manages the customer's infrastructure and operations, as outlined in this Specification. The table below provides an overview of the responsibilities of the customer and the Advarra team for activities in the lifecycle of an application running within the Advarra Cloud.

- **"R"** stands for responsible party that does the work to achieve the task.
- **"C"** stands for consulted; a party whose opinions are sought, typically as subject matter experts; and with whom there is bilateral communication.
- **"I"** stands for informed; a party that is informed on progress, often only on completion of the task or deliverable.

All aspects of the physical infrastructure environment are the responsibility of Advarra. Only items that have customer responsibility are detailed below. Customers will receive notifications on infrastructure-related upgrades, outages, and the like.

Customer access to the environment is restricted to APIs and user interface-level access for Administrators and Users where appropriate.

Logging, Monitoring and Event Management	Customer	Advarra
Recording and monitoring all infrastructure change logs	I	R
Recording and monitoring all application change logs	I	R
Recording and monitoring all alarms and alerts for incident notification	C	R
Investigating and resolving all alarms from any source	I	R
Review of application audit and access logs	R	I

Incident and Problem Management	Customer	Advarra
Proactively notify Incidents on AWS infrastructure based on monitoring	I	R
Categorize Incident priority	I	R
Provide Incident response	I	R
Provide Incident resolution / infrastructure restore	I	R
Identify Problems in Cloud Environment	C	R
Perform RCA for Problems in Cloud Environment	C	R
Remediation of Problems in Cloud Environment	C	R

Security Management	Customer	Advarra
Manage the lifecycle of users, and their permissions for local directory services, which are used to access Advarra	R	I
Operate federated authentication system(s) for customer access to Advarra Cloud	R	I
Deploying, patching, and maintaining the appropriate security software in the environment	I	R
Monitoring malware on Instances	I	R
Monitoring for security incidents	I	R
Maintain and update virus signatures	I	R
Security event management	I	R
Notification to the customer of a security incident that requires notification	C	R

Patch & Continuity Management	Customer	Advarra
Monitor and patch for applicable updates to supported OS and software preinstalled	I	R
Notify customer of upcoming updates	I	R
Validated Applications (if required) validate changes within test window	R	C
Specify backup schedules	I	R
Execute backups per schedule	I	R
Validate backups	I	R
Request backup restoration activities	R	C
Execute backup restoration activities	I	R
Restore affected environments	I	R

Revision History

Version	Description of Changes	Section	Effective Date
0.1	Initial Release	n/a	10.15.2021
0.2	Added support for Longboat to document, clarified outages, clarified upgrades, added SOC 2 Type 2 update, and addressed minor grammatical issues	3, 4	06.11.2022
0.3	Added clarification for non-validated applications in the release process. Added support for Advarra Payments to Cloud, removed user restrictions for Insights (no longer required) and formatting issues.	3	10.28.2022
0.4	Document review.	n/a	03.12.2024
0.5	Moved Release Management to it's own section.	4	04.04.2024
0.6	Updated offerings.	3.1	05.09.2024

[Return to Table of Contents]