G-CLOUD 14 FRAMEWORK

SERVICE DEFINITION DOCUMENT

Ion Industries Ltd
2 Esh Plaza
Sir Bobby Robson Way
Newcastle upon Tyne
NE13 9BA

Telephone: 0191 4661231
Email: success@ionhq.co.uk

TABLE OF CONTENTS

SERVICE OVERVIEW

Sage Intacct, an award-winning true cloud accounting solution by Sage, has been designed for scale-ups to global enterprises in the UK. This robust platform efficiently manages various aspects of your financial operations, including accounting processes, financial management, account management, customer relations, cash flow, order tracking, bank reconciliation, general ledger, accounts receivable, and procurement.

Sage Intacct provides you with the capabilities to effectively manage financial reporting, project accounting, fund accounting, fixed assets management, time and expense tracking, multi-entity management, and expenditure control, all while maintaining strict adherence to accounting compliance standards.

Sage Intacct for Education

As a Sage Platinum Business Partner with extensive experience in the education sector, we implement and shape Sage Intacct software to the specific needs of multi-academy trusts, colleges, and universities. Sage Intacct for Education product is the result of extensive learnings gained from this sector, allowing educational organisation to benefit from efficiencies in the process of transitioning from legacy systems., Sage Intacct for Education is a best-in-class cloud-accounting solution that has been specifically tailored to meet the requirements of educational organisations.

Here is an overview of key functionality:

Core Financials and Accounting - Sage Intacct provides comprehensive financial management capabilities, including general ledger, accounts payable, accounts receivable, and cash management. It streamlines financial processes, automates transactions, and ensures accurate financial reporting.

Purchasing and Order Management - The platform facilitates efficient procurement processes, allowing you to manage purchase orders, vendor relationships, and inventory. Order entry, invoice processing, and contract management are seamlessly integrated.

Business Intelligence and Reporting - Sage Intacct offers robust analytic tools including fully drillable reporting, captivating visual dashboards, and performance cards. You can create customised financial reports, track key performance indicators (KPIs), and gain insights into your business health.

Integration with Third-Party Software - Sage Intacct seamlessly integrates with other best-in-class solutions.

True Cloud Multi-Tenant Solution - Sage Intacct is a true cloud accounting software hosted on a multi-tenant system. Clients share the same software application while their data remains isolated from other tenants. Regular upgrades ensure you always have access to the latest features.

Statutory Reporting and Compliance - Take advantage of prebuilt GAAP and IFRS-compliant statements and financial reports. Educational organisations will gain access to our proprietary automated management report pack consisting of the AAR Report, Benchmarking, SOFA Report, Budget Forecast Return (BFR), Counter Party and Main Accounts Return Report.

MANAGEMENT OF INFORMATION SECURITY

Sage Intacct is built natively in the cloud, meaning it is designed to be scalable, highly available, and easy to manage. It is deployed for all UK customers on Amazon Web Services (AWS), providing highly reliable, secure, and scalable hosting services trusted by millions of customers worldwide.

AWS leads the industry as a trusted repository for customer data with world-class security and privacy programs. All Sage Intacct UK customer data is stored and processed in the cloud. By utilising the powerful hosting platform from AWS, Sage Intacct can handle:

- An unlimited number of concurrent users
- Up to 100 million application requests per day
- 1 billion API calls per month.
- Over 50 billion financial records

It provides a secure infrastructure and flexible tools that help you and us comply with global privacy and data protection regulations. Its comprehensive and flexible data security model secures data at all levels, including infrastructure, network, application, and database security.

Sage Intacct is served 100% over HTTPS, with connections secured via the latest versions of TLS. The API and application endpoints are TLS/SSL only and score an “A” rating on SSL Labs’ tests.

Security Certifications

Sage Intacct performs various types of internal and third-party audits to validate compliance for all core business activities relating to the operational delivery of their secure, global cloud finance management system.

- SSAE 18 SOC 1 Type II
- SOC 2 Type II
- ISAE 3402 / ISAE 3000
- PCI-DCC Level 1 (US)
- HIPAA (US)
- GDPR (UK & EU)

The Sage Intacct application is deployed on the AWS platform, which has the following certifications and security assurance reports and more:

- ISO 9001 / 27001 / 27017 / 27017
- SOC 1 / 2 / 3
- NIST Cybersecurity Framework
- Cyber Essentials Plus

Further information is available on the AWS compliance site:
https://aws.amazon.com/compliance/programs

Dedicated Security Team

Sage has a Global Chief Information Security Officer (CISO) reporting directly to the Sage Board, who heads a dedicated Global Security team working across the enterprise. The team's functions cover Product Security and Architecture, Compliance, Security Engineering, Cyber Defence Operations, Business Continuity and Crisis Response. Sage also has a Global Risk and Compliance team overseeing all business risks.

DATA PROTECTION

Sage takes data privacy very seriously and adhere to all legal and regulatory obligations conferred on us as a processor. Sage act in accordance with your customer instructions as detailed in the Agreement (comprising the terms and conditions and data protection addendum).

You are responsible for the accuracy, quality, integrity, reliability, and appropriateness of data submitted. You must comply with applicable laws in your use of Sage services.

Sage Intacct acts as a data processor. You will be the data controllers – you determine which data you submit as organisation and personal information.

All AWS and Sage contracts are compliant with GDPR Article 28. You can configure the Sage Intacct's application's security functionality to comply with local data protection laws if needed.

Sage maintains a Legal and Compliance Register and utilises a Sage Compliance Hub to support colleagues in identifying regulatory or legislative changes that may impact on the content of policies or procedures. It also helps them respond to emerging risks effectively via the Sage Global Risk Management framework.

Access Rights Only employees that need access to customer data processing and storage systems have access to customer data. AWS technical operations employees must authenticate to access and manage production systems.

No remote access is permitted to the backend platform – all access is via the web portal which have dedicated secure log in details. Multi-Factor Authentication is used on AWS and Sage Intacct to ensure access to cloud services are protected. Sage enforce MFA into Sage Intacct administration systems for every Sage Intacct employee.

Training

The Sage Legal and Data Privacy teams offer expert support and guidance to all colleagues, with regular training provided to raise awareness. Sage has an internal Data Protection Policy applicable to all employees which clearly sets out their data protection obligations and regular awareness and refresher training is mandatory.

AUDITING

Sage performs various types of internal and third-party audits to validate compliance for all core business activities relating to the operational delivery of their secure, global cloud finance management system.

- SSAE 18 SOC 1 Type II
- SOC 2 Type II
- ISAE 3402 / ISAE 3000
- PCI-DCC Level 1 (US)
- HIPAA (US)
- GDPR (UK & EU)

ENCRYPTION LEVELS

All data is stored and processed in AWS data centres. Currently, the primary centre is in Dublin, Ireland with the business continuity backup location in Frankfurt, Germany.

All data sent to or from the Sage Intacct system is encrypted in transit and at rest using at least a 256-bit encryption key.

AWS encrypts all production data and backups using Triple-DES 128-bit or AES-256 block-level storage encryption.

Sage Intacct acts as a data processor. You will be the data controllers – you determine which data you submit as organisation and personal information.

All the AWS and Sage contracts are compliant with GDPR Article 28. You can configure the Sage Intacct’s application’s security functionality to comply with local data protection laws if needed.

Sage Intacct is served 100% over HTTPS, with connections secured via the latest versions of TLS. The API and application endpoints are TLS/SSL only and score an “A” rating on SSL Labs’ tests.

INCIDENT RESPONSE AND RISK

AWS has 24/7 dedicated Computer Security Incident Response Teams (CSIRT). They oversee and respond immediately to information from leading network security tools, including intrusion detection systems, security event management, threat monitoring from third party authorities and perimeter monitoring.

AWS Security Operations Centres are located around the world and are responsible for monitoring, triaging, and executing security programs for their data centres. They oversee physical access management and intrusion detection response while also providing global, 24/7 support to the on-site data centre security teams.

In short, they support security with continuous monitoring activities such as tracking access activities, revoking access permissions, and being available to respond to and analyse a potential security incident.

Sage has a documented Risk Management Policy owned by the Business Integrity and Assurance team, which is responsible for overseeing all business risks, with detailed requirements for reporting, recording, assessing, and managing risks across the business. In addition, Sage Intacct maintains a risk register of information assets applicable to the service. Information risk owners are assigned to make sure risks are appropriately treated and escalated to the Global Risk Register if necessary.

All risks are recorded in the Sage Governance, Risk and Compliance tool (Sage GRC), and all colleagues receive regular training to ensure they are risk aware and know the importance of identifying, reporting, and managing risks.

The documented process includes procedures for reporting, assessment, containment and resolution and keep a detailed record of all incidents.

Audits of the process are conducted every year, or sooner if there's a significant change. Incidents are reported to stakeholders and affected customers (where appropriate) in a timely manner and in accordance with legal and regulatory obligations.

Sage has an executive sponsored, globally approved Incident, Emergency and Crisis Management Policy, which includes data breach management.

In the event of a suspected or confirmed data breach, the Incident process is invoked with additional support from dedicated legal subject matter experts. If the breach needs to be notified to the ICO, Sage will do so in accordance with legal and regulatory obligations.

SOFTWARE DEVELOPMENT

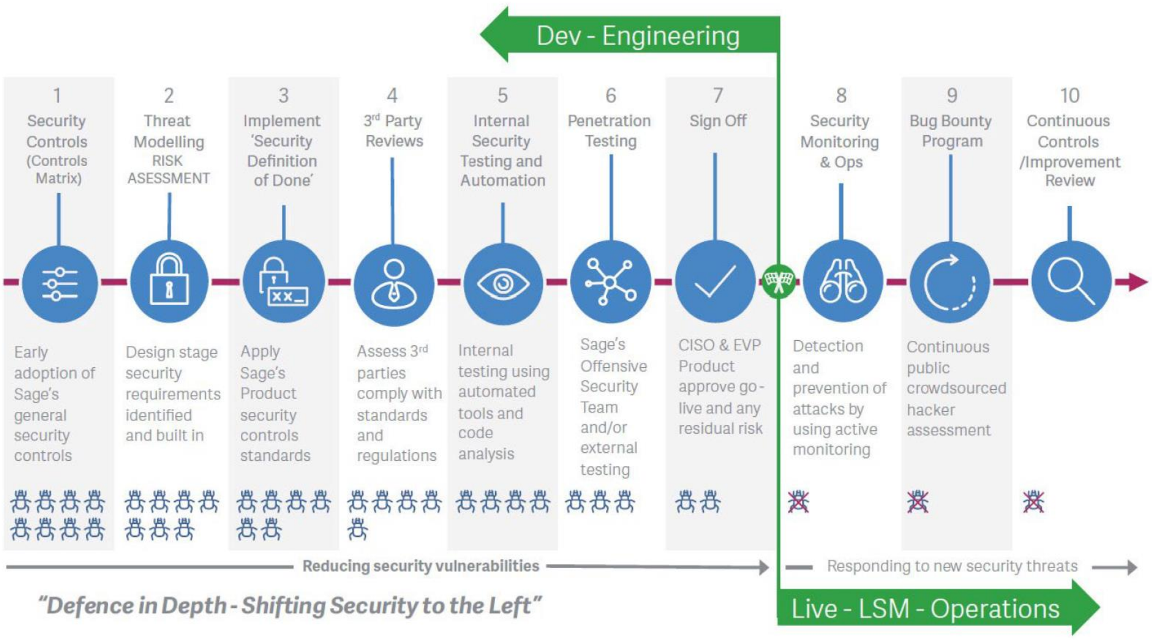
Sage has a defined secure software development lifecycle (SSDLC) to carry out changes and issue releases in a secure, controlled manner. It covers design, development, QA testing, and release, with security considered throughout the lifecycle.

Sage has produced a set of secure software development policies, standards, and processes to support the product engineering teams, including architecture and development design principles, source code management, cryptography, data retention and access controls. All documentation is published on the Sage Internal Developer Portal.

Software upgrades are strictly controlled on the AWS platform, with automated testing and security checks required. Changes and releases are managed through the Sage SDLC, are strictly controlled and a history of all changes and approvals is recorded in the change, case management and version control systems.

All changes to the cloud environment for the platform require the following to be documented in the change ticket: Risk Summary, Impact Severity, Impact Scope, Verification Plan, Back-out plan in advance and scheduled to provide the least impact.

Sage Secure Software Development Lifecycle:



Release Updates and Security Vulnerability Testing

Sage have functioning, frequently used automation in place so that they can safely and reliably rollout changes to the application within minutes.

Sage Intacct releases updates to its services each quarter. These updates are automatic, require no action on your part, and include significant new features and product enhancements.

Sage publishes all release notes here:
https://www-p04.intacct.com/ia/docs/en_GB/releasenotes/all-release-notes.htm

Sage uses a suite of enterprise security tools for application security testing and vulnerability management, and Secure Software Development and Technical Vulnerability Management Standards are aligned with industry standards and best practices (e.g. ISO 27001, OWASP) to ensure vulnerabilities are remediated.

PHYSICAL ACCESS

Sage Intacct is hosted in AWS Data centres and Physical access to the data centres is tightly controlled and follows rigorous security protocols.

AWS data centre physical security begins at the Perimeter Layer. This Layer includes a number of security features depending on the location, such as security guards, fencing, security feeds, intrusion detection technology, and other security measures.

AWS restricts physical access to people who need to be at a location for a justified business reason. Employees and vendors who have a need to be present at a data centre must first apply for access and provide a valid business justification. The request is reviewed by specially designated personnel, including an area access manager. If access is granted, it is revoked once necessary work is completed.

AWS Security Operations Centres are located around the world and are responsible for monitoring, triaging, and executing security programs for the data centres. They oversee physical access management and intrusion detection response while also providing global, 24/7 support to the on-site data centre security teams. In short, they support Sage's security with continuous monitoring activities such as tracking access activities, revoking access permissions, and being available to respond to and analyse a potential security incident.

Like other layers, access to the Infrastructure Layer is restricted based on business need. By implementing a layer-by-layer access review, the right to enter every layer is not granted by default.

Access to any particular layer is only granted if there is a specific need to access that specific layer. The Data Layer is the most critical point of protection because it is the only area that holds customer data. Protection begins by restricting access and maintaining a separation of privilege for each layer. In addition, threat detection devices, video surveillance and system protocols are deployed, further safeguarding this layer.

AWS Global Infrastructure:
AWS operates a global network of data centres strategically located in different regions around the world. Each region consists of multiple Availability Zones (AZs) which are essentially separate data centres within close proximity to each other.

Physical Security Measures:

- Perimeter Security: AWS data centres are surrounded by high perimeter fencing to prevent unauthorised access.
- Access Control Points: Only authorised personnel are allowed to enter AWS data centres. Access is granted through multiple authentication mechanisms such as biometric scanners, access cards, and PIN codes.
- 24/7 Security Guards: Trained security personnel monitor the premises round the clock to ensure physical security.
- Video Surveillance: Comprehensive video surveillance systems are installed throughout the facilities to monitor activities.
- Intrusion Detection Systems (IDS): Advanced IDS are deployed to detect and prevent unauthorised access attempts.

Data Centre Design:

- Redundancy: AWS data centres are designed for high availability and fault tolerance. They feature redundant power sources, networking equipment, and cooling systems to minimise the risk of downtime.
- Fire Suppression Systems: Advanced fire detection and suppression systems are in place to mitigate the risk of fire-related incidents.
- Environmental Controls: Data centres are equipped with environmental controls to maintain optimal temperature and humidity levels for equipment operation.

Access Control Policies:

- Least Privilege: AWS follows the principle of least privilege, which means that employees are granted only the minimum level of access required to perform their job duties.
- Role-Based Access Control (RBAC): Access to sensitive areas within the data centre is restricted based on job roles and responsibilities.
- Two-Factor Authentication (2FA): Multi-factor authentication is required for accessing critical systems and infrastructure.

Visitor Management:

- Pre-Approval: All visitors must be pre-approved and undergo a strict identification verification process before being granted access to AWS data centres.
- Escort Requirement: Visitors are typically escorted by authorised personnel while inside the data centre premises.

Compliance and Certifications:

- ISO 27001: AWS data centres adhere to the ISO 27001 standard for information security management.
- SOC 1, 2, and 3: AWS undergoes regular audits to obtain SOC 1, SOC 2, and SOC 3 certifications, which attest to the security, availability, and confidentiality of their services.
- PCI DSS: AWS is compliant with the Payment Card Industry Data Security Standard (PCI DSS), allowing Sage Intacct to process payment transactions securely.

Continuous Monitoring and Auditing:

- Security Audits: AWS conducts regular security audits and assessments to ensure compliance with industry standards and best practices.
- Incident Response: In the event of a security incident, AWS follows a documented incident response process to mitigate the impact and prevent recurrence.

CONTROLLING THE DATA CENTRE ENVIRONMENT

The Environmental Layer is dedicated to environmental considerations from site selection and construction to operations and sustainability. AWS carefully chooses data centre locations to mitigate environmental risk, such as flooding, extreme weather, and seismic activity.

AWS proactively prepares for potential environmental threats, like natural disasters and fire. Installing automatic sensors and responsive equipment are two ways AWS safeguard the data centres. Water-detecting devices can alert employees to problems as automatic pumps work to remove liquid and prevent damage. Similarly, automatic fire detection and suppression equipment reduces risk and can notify AWS employees and firefighters of a problem.

In addition to addressing environmental risks, sustainability considerations are also incorporated into the data centre design. AWS has a long-term commitment to use 100% renewable energy.

When companies move to the AWS Cloud from on-premises infrastructure, they typically reduce carbon emissions by 88% because AWS data centres can offer environmental economies of scale. Organisations generally use 77% fewer servers, 84% less power, and tap into a 28% cleaner mix of solar and wind power in the AWS Cloud versus their own data centres.

To find out more about sustainability initiatives and to track AWS's progress, visit https://sustainability.aboutamazon.co.uk/environment/the-cloud.

DISASTER RECOVERY AND BUSINESS CONTINUITY

As the Sage Intacct application is hosted on AWS, Sage can leverage the business continuity and disaster capabilities the platform offers to ensure the service remains available. Further details on AWS business continuity capabilities are available here: https://aws.amazon.com/compliance/data-center/controls/.

The AWS Business Continuity Plan outlines measures to avoid and lessen environmental disruptions. It includes operational details about steps to take before, during, and after an event. The Business Continuity Plan is supported by testing that includes simulations of different scenarios. During and after testing, AWS documents people and process performance, corrective actions, and lessons learned with the aim of continuous improvement.

Water, power, telecommunications, and internet connectivity are designed with redundancy, so AWS can maintain continuous operations in an emergency. Electrical power systems are designed to be fully redundant so that in the event of a disruption, uninterruptible power supply units can be engaged for certain functions, while generators can provide backup power for the entire facility. People and systems monitor and control the temperature and humidity to prevent overheating, further reducing possible service outages.

Backups and Disaster Recovery Plan

Sage Intacct adheres to and maintains measures to secure data backups. For UK customers Sage Intacct's database is backed up and stored in AWS S3 storage. Besides S3, AWS also take daily AWS Snapshots of all DB servers (which also get stored in their respective AWS region).

The combination of all these backups allows us to restore DB servers for various kind of failures (Single Server, Regional Outrage, Point in time recovery etc) and provide a Restore Point Objective (RPO) of no more than 4 hours and Restore Time Objective (RTO) of no more than 24 hours. Besides databases, all other type of servers processing customer data is backed up via AWS snapshots. There are no tape backups (nor they are necessary). Transmission of data is via secured protocols. Sage will make commercially reasonable efforts to maintain uptime of 99.8%/calendar month.

Business Continuity Plan

Sage as a documented Business Continuity Policy supported by global, regional, and local business continuity plans. The Sage Crisis Management team is composed of representatives from the Executive Committee, supported by experts from Risk, Security, Travel, People, Property, IT, and Communications.

The AWS Business Continuity Plan is an operations process guide outlining how to avoid and lessen disruptions due to natural disasters with detailed steps to take before, during, and after an event. To mitigate and prepare for the unexpected, AWS tests the Business Continuity Plan regularly with drills that simulate different scenarios. AWS document how people and processes perform, then debrief on lessons learned and any corrective actions that may be needed to improve their response rate.

Sage and AWS are trained and ready to rebound from disruptions quickly, which includes a methodical recovery process to minimise further downtime due to errors.

SERVICE CONSTRAINTS

The Sage Intacct service adheres to quarterly release schedules for planned maintenance completion. These schedules are announced in advance and are scheduled for Friday evenings outside of regular hours to minimise any impact on users of the service.

Additionally, accessing the Sage Intacct service is hassle-free, requiring only an internet connection and a supported browser. This streamlined accessibility enhances user experience, allowing individuals to seamlessly utilise the service from any location with internet access. Supported browsers include popular options such as Edge, Chrome, Safari, and Firefox, ensuring compatibility across various platforms and devices for a smooth and consistent user experience.

CUSTOMISATION

Across the Sage Intacct customer base there are a number of bespoke and turnkey integrations on the marketplace created to seamlessly interconnect with existing organisational systems.

Sage Intacct boasts a robust and comprehensive API that spans across the entirety of its application suite, empowering users with seamless connectivity and integration capabilities tailored to their specific business requirements. There are a growing number of bespoke and turnkey integrations on the marketplace created to seamlessly interconnect with your existing organisational systems.

Specifically, within the Education sector, ION have built an automated management report pack consisting of the AAR Report, the Benchmarking, SOFA Report, Budget Forecast Return (BFR), Counter Party and Main Accounts Return Reports that can be as one pack.

SERVICE LEVELS

Sage and ION are committed to your success. To demonstrate Sage's commitment, Sage have established their Buy With Confidence™ program, outlining the level of service you can expect from them in the operation of the Sage Intacct Services. They strive to make every interaction productive.

Sage's goal is to provide 24x7 availability of the Sage Intacct application service and offer subscription credits for availability below 99.8%. You can receive a credit of 10% of your subscription fees for the month in which the outage event(s) occurred for every percentage point that Service Availability falls below 99.8%, up to a maximum of 50% of the applicable subscription fees for that month.

Sage performs regular transaction log backups and daily data backups to redundant local storage, periodically replicated offsite, and transaction backups are frequently replicated offsite for disaster recovery. No more than 4 hours of a customer's transactional work will be lost due to catastrophic events (Recovery Point Objective), and in the event of a disaster, the application service will be available within 24 hours (Recovery Time Objective).

ION's Support Services are open Monday to Friday 9am – 5pm excluding bank holidays.

Service Level Agreement

Actual Service Levels Achieved in 2023 – 99.7%.

Package	Priority	Response Time	Fix Time	% Within Target
Managed Services	P1 – Urgent	2 Hours	13 Hours	80%
	P2 – High	2 Hours	20 Hours, 30 Minutes	80%
	P3 – Medium	Fix Time subject to Backlog Prioritisation	When Resource is available	80%
	P4 – Low	Fix Time subject to Backlog Prioritisation	When Resource is available	80%

Priority	Definition
P1 – Urgent	An incident which has caused the service to fail completely. This category also includes incidents which have the potential to cause damage to client revenue or incur legal implications.
P2 – High	A loss of one or more components or content with limited business impact, meaning the client can still operate with a degraded or reduced set of services.
P3 – Medium	A minor loss or service or content with little impact on the client.
P4 – Low	Service requests, information, question, guidance, training and change requests.

ONBOARDING

Planning

ION understands the importance of setting the project up for success from Day 1. During the Planning Phase ION will collaboratively work with you to establish the most suitable route to mutual success. We will create a bespoke project delivery plan, identifying potential risks and ensuring expectations are aligned. We will work with you to define a clear process, incorporating mutually agreed roles and responsibilities, timelines, and quality gates. We will also agree the best way to work with each other and ensure all levels of stakeholder management and engagement are planned and receive the reporting and analysis that they require as we progress through each phase.

Discovery

We will work together to comprehensively define the scope and execution of the project, represented through critical success factors, project requirements and solution design. At the end of the Discovery phase, there will be absolute certainty of project scope, identified risks and contingency plans in place to mitigate those risks.

We will also work with you to define the data approach for the project which will define how the migration of data from one system to another will be managed, along with starting to build an inventory of the actual data for the project.

Finally, our ISO9001 accredited QA team will define a tailored Test Strategy Plan to achieve the highest quality in the delivery of our system to your organisation.

Implementation Phase

This phase represents the setup, configuration, and quality assurance of the desired solution for the organisation within the test environment; this will be the baseline Sage Intacct solution that you will subsequently train and test in. The solution will be set up and configured based on information gathered in the Implementation Workbook and Discovery Workbook completed in the Discovery phase and is representative of the Solution Design Document. The Quality Assurance phase runs in parallel with the build and is performed by the ION ISO9001 accredited QA team, involving full end-to-end testing with test plans, test scripts and an “End of Test” report produced to ensure a quality and assured build.

Training and Testing Phase

The Training and Testing phase of the project occurs once the system has been built and verified by our QA team. You will be given access to the system to perform User Acceptance Testing.

To enable you in performing Testing, we will provide you with the appropriate training, consisting of bespoke virtual training sessions, led by our team of Specialists, with agreed and tailored agendas for the organisation over a period of typically 3-4 weeks. All sessions can be recorded for your future reference.

The Test phase is end-user driven; through the provision of test scripts and training we strive to ensure that end users can familiarise themselves with the system and can navigate and operate with confidence.

As part of our training offering, we supply an array of supplementary resources such as dedicated knowledge bases and interactive workbook, vies that are available 24/7. Throughout the implementation phase, users will also benefit from a dedicated testing and training implementation copy of Sage Intacct.

Deployment Phase

Upon the completion of Training and Testing and following the resolution of any changes or fixes identified within that phase, the project will move to Deployment. The key objective of this phase is to move the quality assured, tested solution from the Test environment into the Production environment, ready for Go Live. This phase will be led by ION and prepares the solution for the penultimate phase before Go Live, Data Migration.

Opening Balance Migration

This phase exists to ensure the solution is populated with the appropriate designed and cleansed data ahead of being ready for sign off, Go Live and operation. Whilst the accuracy and integrity of the data ultimately sits with the users, ION is on hand to support through provision of the data migration templates, training and assistance on best practice throughout the process.

Go Live

This is the final step in the project life cycle. It refers to the mutually agreed sign-off of project deliverables, formal handover, and deployment of the solution into the organisation's live environment. ION will also support you in the operation of the system in your day-to-day business tasks, while you familiarise and become confident in the use of the system.

Customer Success

After your Go Live, you'll seamlessly transition into a complimentary 2-month Support Services period, accompanied by your dedicated customer success team. This team comprises of a named Account Manager and Sage Intacct Specialist. Expect regular check-ins, daily or weekly, to address any support issues you encounter. Additionally, we'll be by your side to guide you through the challenges of your initial month-end period with your new finance system.

OFFBOARDING

Once you have given notice to terminate your contract you will have up to 90 days to retrieve your data from the system. This can be exported from the solution in its original format, such as CSV or Excel, with a simple click-and-download function. At the end of your contract, customers would have the opportunity to pay for a read-only license giving them access to your data for a 2-year period.

ORDERING AND INVOICING

Following a thorough business and technical requirements review, our team at ION will work closely with you to identify and align the appropriate modules for your solution and agree on the commercial offering. Subsequently, a comprehensive contract will be drafted, outlining the project's scope, the estimated timeframe for implementation, and the licensing terms provided by Sage.

Upon mutual agreement and signing of the contract, a sales order will be generated encompassing the first-year annual license fees, support services, and the one-time implementation charge.

Our implementation service operates on a fixed fee model, ensuring transparency and predictability throughout the project lifecycle. Payments will be invoiced at predetermined milestones during the implementation process.

In adherence to our standard payment policy, payment is due within 14 days of issue of invoice.

CONTRACT TERMINATION

License contracts for 3-Years, and 5-Years are available. All license subscriptions will automatically renew for additional 1-Year periods, based on the terms confirmed in the contract, unless the Customer provides the Supplier with notice of non-renewal at least 90 days before the end of the relevant subscription term.

Midterm terminations are not allowed, except as outlined in the termination clauses of the terms and conditions. ION follows relevant guidelines and legislation such as GDPR and ICO during data extraction. Therefore, at the end of contracts, users are permitted to extract data via excel and csv file types. Additionally, Archive read-only licenses are available for users who wish to retain data within the system, with nominal charges applicable.

All this information is detailed in the SLA provided at the onset of contracted services, which is mutually agreed upon by the client and accessible on the Sage website at: https://www.sageintacct.com/customer-terms-uki/sla. Furthermore, Customer Data can be exported at any time.

Sage will retain Customer Data in the production environment for up to 90 days after termination or expiration of the Agreement and may assist in exporting Customer Data during this period at the standard hourly consulting rate. After the 90-day period, Sage reserves the right to delete all Customer Data and is not obligated to make it available further.

AFTER SALES SUPPORT

At ION, we believe in providing comprehensive support throughout the entire implementation process of our services. From the initial stages to post-launch support, our dedicated team ensures that your transition to using our solutions is smooth and efficient.

Upon engaging with ION, you will be assigned a dedicated implementation team comprising a Consultant, Project Manager, and Sage Intacct Specialist. Each member of this team plays a crucial role in guiding you through the implementation process.

Your Consultant will work closely with you to understand your specific requirements and objectives. They will provide expert advice on how to best leverage our services to meet your business needs. With their deep understanding of our solutions, they will tailor the solution to align with your goals and workflows.

The Project Manager will oversee the entire implementation process, ensuring that tasks are completed on time and within budget. They will coordinate with both your internal team and our experts to address any challenges that may arise during the implementation phase. Their goal is to ensure a seamless transition to our services while minimising disruptions to your operations.

Throughout the implementation process, our Sage Intacct Specialist will be available to provide guidance and assistance whenever you need it. Whether it's answering technical questions or troubleshooting issues, they are dedicated to ensuring that you have a positive experience with our solutions.

Once the implementation project has been completed and signed off, you will transition to your dedicated account manager. Your account manager will serve as your main point of contact with ION and Sage moving forward. They will be there to support you every step of the way, ensuring that you continue to derive maximum value from our services.

Your account manager will proactively engage with you to understand your evolving needs and provide ongoing support and guidance. Whether it's exploring new features, addressing any concerns, or providing additional training, they are committed to helping you succeed with ION and Sage.