



Service Definition Document

Contents

SERVICE OVERVIEW	2
DATA PROTECTION	3
Auditing	3
Encryption Levels	4
Incident Response Facilities.....	4
Data Protection Training and Procedures	5
Access Rights	5
Secure Software Development	6
Physical Access.....	7
Controlling the Data Centre Environment.....	7
DISASTER RECOVERY AND BUSINESS CONTINUITY	8
ONBOARDING AND OFFBOARDING SUPPORT	8
Onboarding - Approach	8
Offboarding	10
SERVICE LEVELS	10
Service Constraints.....	11
CUSTOMISATION	11
ORDERING AND INVOICING	11
CONTRACT TERMINATION	12
AFTER SALES SUPPORT	12

SERVICE OVERVIEW

Solutions for Accounting provide Sage Intacct. This is the market leading software solution for all manner of accounting, finance, and business management needs. It is also the first, and only, AICPA-preferred financial management solution, and is the leader in customer satisfaction, as awarded by G2.

Coming from the well-recognised Sage brand who have been providing software in the small to medium sized business for decades Intacct is their first true cloud solution.

Offering highly sophisticated, powerful, flexible and customisable configuration, interrogation and integrated reporting, it is a 'Best of Breed' comprehensive finance system.

Key features include:

- Six levels of dimensionality as standard within the Chart of Accounts set up, meaning all data input can be correctly tagged with reportable meta data, at the point of entry.
- Effective in-system reporting of income and expenditure, balance sheets, cash balance, cash flow details, tracking of assets and expenses.
- Purchase and Sales Order management.
- Provides a simple, flexible connection service to dozens of related solutions, through the Sage Marketplace Partner program.

With years of experience working with the education sector Solutions for Accounting look to fine tune the system configuration at implementation to perfectly fit the needs of educational organisations of all types and sizes.

Across its global client base, Sage Intacct reduces time to close by as much as 79%, and seeing real-time reporting across hundreds of consolidated entities, finance leaders using Sage Intacct can drive growth. The solution is built for the cloud – its multi-tenant, true cloud foundation brings robust technology infrastructure to your organisation, without the high costs of managing servers. It provides the elasticity companies need to grow, handling:

- Up to 100 million application requests per day.
- 1 billion API calls per month.
- Over 50 billion financial records.

Sage Intacct customers achieve an average 250% ROI and payback in less than 6 months from initial sign up. The software ensures compliance and auditability, with the audit trails, visibility, and forecasting necessary to support an IPO.

DATA PROTECTION

Sage Intacct is built natively within the cloud, and deployed for UK customers on AWS, providing reliable, secure, and scalable 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. Sage policies regarding data protection are published and available to all employees on our Intranet, supported by standards such as ISO:27001. Sage Intacct holds the following security certifications:

- ISO 9001/27001/27017/27018.
- SOC 1/2/3.
- NIST Cybersecurity Framework.
- Cyber Essentials Plus.

Auditing

Sage Intacct performs various internal and third-party audits to validate compliance for all core business activities relating to the operational delivery of our global cloud finance management system. These include:

- SSAE 18 SOC 1 Type II.
- SOC 2 Type II.
- ISAE 3402 / ISAE 3000.
- GDPR (UK & EU).



CSA

Cloud Security
Alliance Controls



ISO 9001

Global Quality
Standard



ISO 27001

Security
Management
Controls



ISO 27017

Cloud Specific
Controls



ISO 27018

Personal Data
Protection



PCI DSS Level 1

Payment Card
Standards



SOC 1

Audit Controls
Report



SOC 2

Security, Availability,
& Confidentiality
Report



SOC 3

General Controls
Report

Encryption Levels

Sage Intacct is served 100% over HTTPS, with connections secured via the latest versions of TLS. All data sent to or from Sage Intacct is encrypted in transit using at least 256-bit encryption. Our API and application endpoints are TLS/SSL only and score an “A” rating on SSL Labs’ tests. To protect the perimeter of the environment, AWS uses edge routers, stateful firewalls and Intrusion Detection Systems (IDS). Only approved network traffic passes through the perimeter firewalls.

Incident Response Facilities

AWS has 24/7 dedicated Computer Security Incident Response Teams, who 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. Devices are protected against malware using a suite of enterprise endpoint protection systems, managed by our 24/7 Cyber Defence Operations (CDO) team, with real-time monitoring, alerting, and reporting.

Data Protection Training and Procedures

Sage conducts regular security training and awareness campaigns to embed and reinforce a culture of security throughout our organisation and ensure organisation-wide compliance and adherence to best practice Data Protection and Information Governance standards. Training is mandatory for all employees and includes online training, process-specific refreshers, and best practice updates for security, risk, anti-bribery, and corruption are provided annually at a minimum, or whenever significant industry changes occur. Training is delivered through a blend of learning methods, including gamification, exercises without repetition, live invocation, and micro-learning, ensuring best practice data security measures embedded into daily working.

Product engineers receive additional annual mandatory training on secure software development best practice. We work with a Security Champion Programme, who liaise closely with our Global Application Security team to ensure our software remains secure and that data is protected. Our platform provider, AWS, ensures all employees that manage the customer-facing environment complete AWS's certification and training programmes. We operate a robust third-party security assurance and due diligence process for supplier risk assessment and approval. AWS provides us with regular evidence of their continued compliance with industry-leading security frameworks and standards, and we monitor their performance through regular audit reports and supplier review management meetings. Security compliance reports can be made available on request upon signage of an NDA.

All employees must confirm acceptance of the terms of our Acceptable Use Policy, and partners are required to read and sign an annual security declaration of compliance.

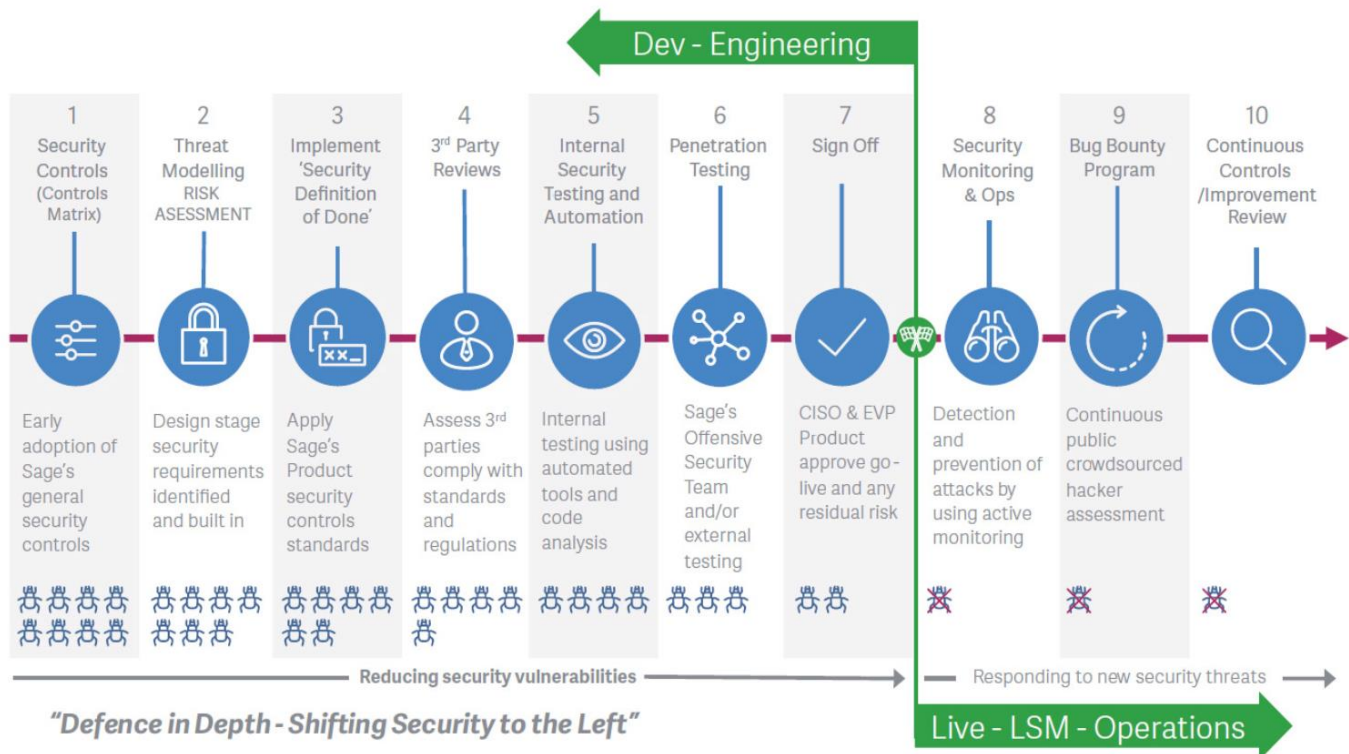
Access Rights

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.

Multi-Factor Authentication is used on AWS and Sage Intacct to ensure access to cloud services are protected. We enforce MFA into Sage Intacct administration systems for every Sage Intacct employee.

Secure Software Development

Please see the below diagram which outlines Sage's procedure for secure software development:



Sage Intacct releases updates to its services each quarter. These are automatic and require no action on the part of the customer. Change is securely managed through automated testing and security checks on the AWS platform. Changes are managed through the Sage SDLC. 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.

Physical Access

AWS provides physical data centre access only to approved employees. All must apply for access and provide a valid business justification. These requests are granted based on the principle of least privilege, where requests must specify to which layer of the data centre the individual needs access and are time-bound. Requests are reviewed and approved by authorised personnel, and access is revoked after the requested time expires. Once granted admittance, individuals are restricted to specific areas within their permissions.

Data centre access is regularly reviewed, and access will be automatically revoked when an employee's record is terminated in Amazon's HR system. When access rights expire, access will be immediately revoked. AWS monitor data centres using global Security Operations Centres, which are responsible for monitoring, triaging, and executing security programs. They provide 24/7 support by managing and monitoring data centre access activities, equipping local teams and other support teams to respond to security incidents by triaging, consulting, analysing, and dispatching responses.

Physical access points to all server rooms are recorded by CCTV, with images retained in line with legal and compliance requirements. Physical access is controlled at building ingress points by professional security staff utilising surveillance, detection systems, and other electronic means. Multi-factor authentication mechanisms are used to control access to data centres, and entrances to server rooms are secured with devices that sound alarms to initiate an incident response if the door is forced or held open.

Electronic intrusion detection systems are installed within the data layer to monitor, detect, and automatically alert appropriate personnel of security incidents. Ingress and egress points to server rooms are secured with devices that require everyone to provide multi-factor authentication before granting entry or exit. These devices will sound alarms if the door is forced open without authentication or held open. Door alarming devices are also configured to detect instances where an individual exits or enters a data layer without providing multi-factor authentication. Alarms are immediately dispatched to 24/7 AWS Security Operations Centres for immediate logging, analysis, and response.

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 we 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 Sage 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.

DISASTER RECOVERY AND BUSINESS CONTINUITY

Sage leverages the business continuity and disaster capabilities the AWS platform offers to ensure service remains available. The AWS Business Continuity Plan outlines measures to avoid and lessen environmental disruptions, including operational details on steps to take before, during, and after an event. The plan is further supported by testing that includes simulations of various scenarios to ensure efficacy in our recovery approach. During and after testing, AWS and Sage will document people and process performance, corrective actions, and lessons learned with the aim of continuous improvement.

AWS also incorporates pandemic response policies and procedures into its disaster recovery planning to prepare for rapid response to infectious disease outbreak threats. Mitigation strategies include alternative staffing models to transfer critical processes to out-of-region resources, and activation of a crisis management plan to support critical business operations. Pandemic plans reference international health agencies and regulations, including points of contact for international agencies.

ONBOARDING AND OFFBOARDING SUPPORT

Onboarding - Approach

Solutions for Accounting Limited's implementation methodology is a delivery framework of phases, tasks, and milestones throughout the project. There are four key Phases:

Phase 1: Design

- Project begins with a kick-off meeting charting the course for the project.

- A project plan is created and mutually agreed upon establishing roles, responsibilities, tasks, and timing of deliverables.
- Business analysis meetings are held to understand and capture functional requirements.
- Functional requirements are translated into a solution definition to be implemented.
- Data is collected and populated by Client into templates for upload.
- **Sign-off: This stage is deemed complete with client signing off the detailed Statement of Work**

Phase 2: Build

- Phase begins only on completion of Design phase.
- Intacct Production environment is created for Client.
- The defined solution is setup and configured.
- Finalised data templates are uploaded.
- **Sign-off: This stage is deemed complete following a walkthrough of the key processes and workflows to the satisfaction of the client.**

Phase 3: Model

- Phase begins only on completion of Build phase.
- Client tests the configured solution to confirm Intacct is working as designed and to gain hands-on experience.
- Changes are documented and applied to the Production environment as defined in the Change Control section of this Statement of Works.
- **Sign-off: This stage is deemed complete with client completing a customised User Acceptance Testing document.**

Phase 4: Deploy

- Phase begins only on completion of Model phase.
- Intacct Production environment is live and ready for use by Client to process transactions.
- Post-live data templates such as GL balances, Open bills/invoices, etc. are populated by Client and uploaded.

Each phase ends with a milestone event, which must be passed to move to the next phase. A Statement of Work will be defined as part of the Design phase, which will detail the solution definition and works to be undertaken by Solutions for Accounting. It will also identify key stakeholders, including Solutions for Accountings Project Manager – who will be your primary point of contact throughout the project.

Should it be required, the escalation path for the duration of the project will be:

Project Manager – all queries should in the first instance be directed to the dedicated project manager.

Director – Any escalated queries will be passed to the technical director or operations director depending in the nature of the query.

Offboarding

In terms of offboarding, at the end of the contract, we will adhere to all relevant guidelines and legislation, such as GDPR and ICO during the extraction of data. Users are, thus, encouraged to utilise the fully functional API available within the application to export their data. This data can be exported into the following formats:

- Reports provided in flat file format, such as CSV (comma separated values).
- A database, where data can be extracted (additional charges apply).
- The application of archive read-only licenses, which are available to users, if there is a desire to keep the data on the system (nominal charges apply).

All data extraction will operate in compliance with Article 17 of GDPR and ICO guidelines. As such, in most cases, data will be deleted within 30 days. However, in instances where requests are more complex, information will be deleted within 60 days, and the client will be given notification of the reason for this.

SERVICE LEVELS

Sage's goal is to provide 24/7 availability of the Sage Intacct service, and they offer subscription credits for availability below 99.8% as a standard Service Level Agreement. Availability is backed up by a complete disaster recovery programme.

Sage's system 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).

Solutions for Accounting operate a single comprehensive support package model offering: Unlimited use of the support helpdesk, delivered by our highly experienced and qualified product experts; either by phone or by email, according to customer preference. The service is available between the hours of 8:30am and 5:30pm, 5 days a week, with an average response time of less than 4 hours, and with 86% of support calls being resolved during the first contact.

Service Constraints

The service is subject to quarterly release schedules for the completion of planned maintenance. These are published in advance to ensure customers are aware of planned maintenance, and this is conducted out of hours on a Friday evening to minimise business impact.

The service only requires an internet connection and a supported browser to be utilised. Supported browsers include:

- Edge.
- Chrome.
- Firefox.
- Safari.

CUSTOMISATION

Across the Sage Intacct customer portfolio there are a vast number of turnkey integrations as well as many custom integrations and bespoke system modifications.

The software solution is customisable to ensure effective application to a range of industries, including:

- Healthcare.
- Hospitality.
- Education
- Not for Profit/Charitable.

The solution also has a fully functional API across the entire application.

In the education sector Solutions for Accounting has written and maintains a suite of reports specifically designed for Multi Academy Trusts. A direct integration to the Department for Education also allows for integrated Academies Accounts Return (AAR) reporting and submission.

ORDERING AND INVOICING

Following a thorough technical and business review the appropriate modules and 3rd party system will be identified and commercial agreements made.

A sales order for the 1st year annual costs and implementation costs will be signed to formalise the partnership.

The implementation project will be on a fixed fee basis and billed at appropriate milestones as detailed in the scheme of works agreed with the customer.

Payment terms are:

- Software: upon acceptance
- Services: 14 days from invoice

CONTRACT TERMINATION

Subscriptions are renewed annually, at least 30 days' notice prior to the renewal date is required to terminate an agreement at renewal. Midterm terminations are not permitted, except in accordance with the termination clauses of the terms and conditions.

AFTER SALES SUPPORT

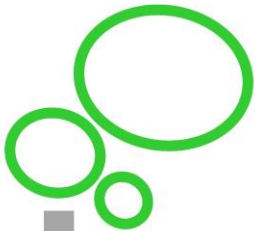
Throughout implementation extensive training and support is offered by the professional services team, with a dedicated project manager assigned to every implementation.

After the implementation project is completed, telephone and email support is provided by Solutions for Accounting's team of Intacct specialists.

Solutions operate a single comprehensive support package model offering: Unlimited use of the support helpdesk, delivered by our highly experienced and qualified product experts; either by phone or by email, according to customer preference.

The service is available between the hours of 8:30am and 5:30pm, 5 days a week, with an average response time of less than 4 hours, and with 86% of support calls being resolved during the first contact. We have one of the biggest support teams in the UK and their exceptional level of service been consistently recognised by Sage.

There is also a rich source of information in the in-product help guide and customer community knowledge base.



Solutions

for **Accounting**