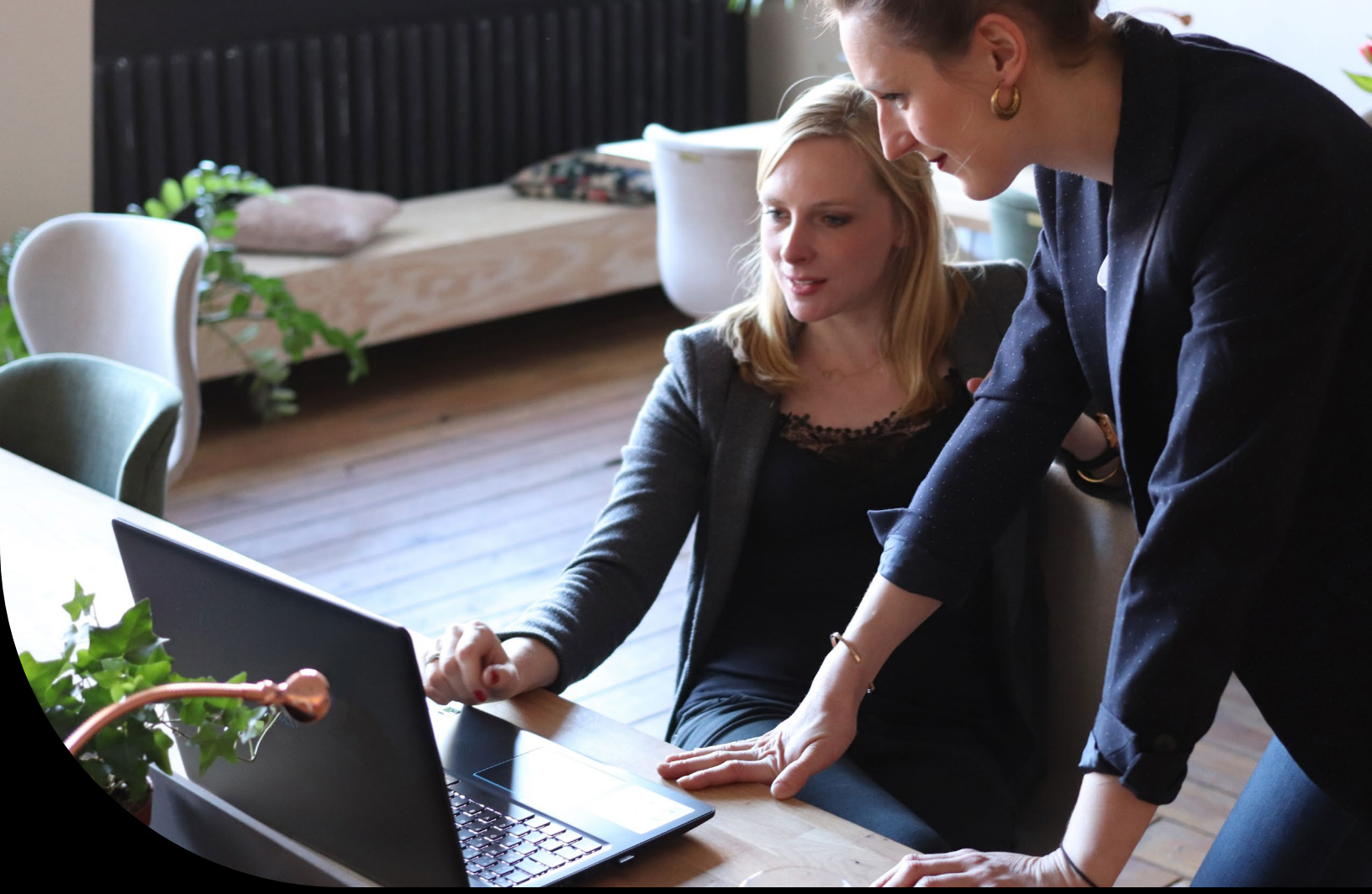


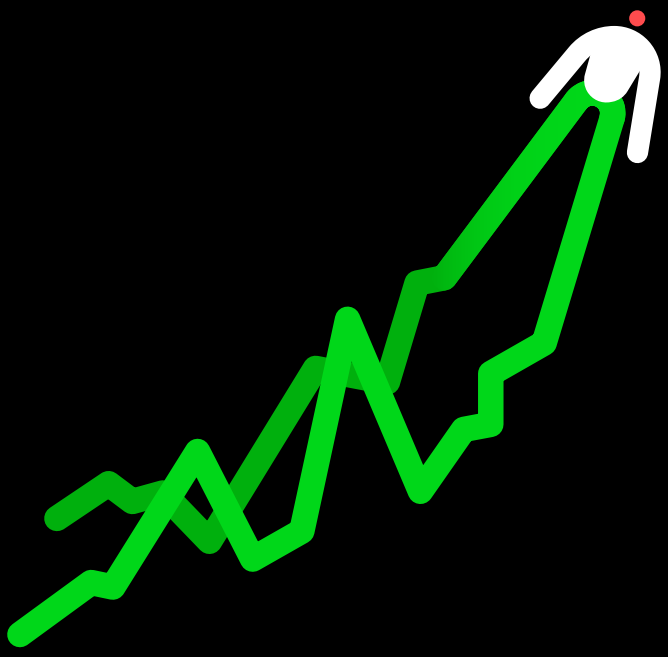
White paper

How Sage Intacct Supports SOX Compliance

Sage

EQUATION TECHNOLOGIES

Table of contents



Sage

EQUATION TECHNOLOGIES

SOX Section 404 compliance

Sarbanes-Oxley (SOX) compliance is a must for public companies, but several key provisions also apply to accountants, auditors, and executives at small and medium-sized businesses as well. SOX mandates that covered entities must have sufficient controls in place to protect against potential liabilities and threats.

Regardless of whether your organization is a covered entity for SOX, many of its requirements are considered best practices and beneficial to all businesses. These practices help to ensure the accuracy of financial statements, as well as protect your business and its stakeholders from lawsuits, fraud, cyber attacks, and more.

The majority of systems-related requirements are part of SOX section 404. SOX doesn't go into specifics about the components systems must include. The law instead places the burden on auditing and consulting firms to render judgement on whether a firm's internal controls meet compliance.

Each financial statement a company produces must contain an internal controls report that details the control system's structure along with a manager's evaluation of its effectiveness. During audits, the auditors use these reports to assess whether the company's internal controls comply with SOX. They look for the two categories of controls:

1. **Preventative controls**: Measures that aim to deter errors or fraud from happening in the first place. This includes documentation and authorization practices.

2. **Detective controls**: Steps to find errors in a company's processes after they have already occurred

Sage Intacct was built to assist companies in complying with SOX. As the only preferred financial management system of the AICPA, it offers the functionality companies both large and small need to meet the preventative and detective internal control requirements.

IT security

Over the nearly 20 years since the passage of SOX, cybersecurity threats have become more commonplace. In response, the Security Exchange Commission issued updated guidance in 2018 requiring companies to "establish and maintain appropriate and effective disclosure controls and procedures that enable them to make accurate and timely disclosures of material events, including those related to cybersecurity."

Security for logins
A basic aspect of any internal control system is its ability to reduce the likelihood of unauthorized access to privileged information by both internal and external parties. The first line of defense against breaches is login security.

Sage Intacct offers a secure login process with the following features:

- Minimum password length
- Periodic password expiration
- Session timeouts
- IP address restrictions by user or entity
- Two-factor authentication

OR

- Single Sign On

Access security
While login security significantly increases the difficulty of breaching financial management software systems for non-employees, it's also vital to set boundaries within the system for employees based on their role and department. User permissions functionality reduce the chances of an internal breach by giving employees access only to the resources they need to perform their role.

Sage Intacct allows administrators to restrict modules different employees can access based on their role and department. For

example, an IT manager could give a new employee who handles accounts payable access to only the Sage Intacct Accounts Payable module while preventing them from accessing modules such as Accounts Receivable and Cash Management.

Segregation of duties
In addition to preventing unauthorized access to privileged information, SOX Section 404 requires companies to segregate duties, separating and assigning steps in a process to different owners as a double-check for accuracy and fraud. Auditors require organizations to document how segregation of duties is achieved within their systems.

User permission functionality in Sage Intacct promotes compliance with this requirement. Sage Intacct administrators can assign user permissions within each Sage Intacct module and function, preventing employees from performing multiple steps in the workflow.

An example of this functionality is the ability to separate the duties of importing bank transactions from bank reconciliations.

Administrators can also establish smart rules within Sage Intacct to reject input from users who don't have permission to perform certain tasks. Smart rules allow administrators to set criteria for conditions that must be met before an action can be recorded in Sage Intacct. One of the available criteria is a user's access level. When a user who doesn't have appropriate access permissions attempts to save an action in Sage Intacct, they receive an error message rejecting the input.

The Sage Intacct approvals functionality adds an additional layer to a company's efforts to segregate duties. This functionality is discussed in further detail in the approvals section below.

Integrations security
The IT security measures covered in SOX extend beyond a company's financial management software. It's also important to prevent unauthorized access to any applications that integrate with the financial management system and to document who accessed the application along with the time and date of access.

To simplify security for integrations with marketplace partner applications, customers create a user ID separate from those used within the core system for every third-party integration. This allows specific permissions to be granted for each integration. Additionally, each marketplace partner is provided a "token" by Sage Intacct to allow specific audit tracking for all transactional activity of each marketplace partner.

On top of activity tracking, Sage Intacct also employs IP filtering for application partners. IP filtering prevents unauthorized access to the application by filtering out traffic based on IP addresses. When a user with an authorized IP address requests access to the application, the filter allows them to enter without any additional prompting. Unauthorized IP addresses are not allowed access.

Cloud security
You can trust Sage Intacct to be secure and reliable. We guarantee 99.8 % uptime, airtight data security, and comprehensive disaster recovery.

Sage Intacct protects your data stored in the cloud with both physical and digital security. All Sage Intacct cloud hosting facilities are protected 24 hours a day, 7 days a week by armed security guards and monitored by security cameras. In addition, Sage Intacct servers are isolated within the larger data center to add another layer of physical security. Sage Intacct has data centers around the world. And in the event of a disaster that affects data center service, such as a major storm or wildfire, customer data can be restored to a specific minute using a backup data center.

For the purposes of digital security, Sage Intacct cloud hosting facilities periodically undergo extensive third-party penetration testing, in which paid hackers attempt to infiltrate the system, to assess the effectiveness of their digital safeguards. Sage Intacct cloud hosting facilities are also required to have the major security certifications, including:

- SOC 2
- PCI
- HIPAA

Data centers that possess the three certifications above are considered "top of the line." These certifications, combined with the routine penetration tests mentioned before, provides peace of mind, knowing that financial data is as secure as possible.

Approvals

The finance team has full visibility into what step each transaction is in during the approval process.

All internal controls systems need an approvals process for transactions. A well-developed approvals process can act as a defense against routine errors and fraud by having an experienced manager review transactions that meet certain thresholds.

Sage Intacct allows administrators to establish thresholds for approvals based on several factors. These factors include amount, frequency, and type, along with overrides by department. Additionally, the finance team has full visibility into what step each transaction is in during the approval process.

The Sage Intacct approvals functionality also promotes segregation of duties since only users with manager-level permissions can approve a transaction. Its usage prevents a single user from initiating a transaction and then approving of it.

Sage Intacct gives finance teams the power to create approval workflows for the following forms of transactions:

- AP Bills
- Purchasing
- AP Payments
- Expense Reports
- Timesheets
- Journal Entries

Audit trails

Every year, covered companies are required to participate in a SOX audit conducted by a third-party auditing firm and to share the results with company stakeholders. These audits are the second form of internal controls—detective controls. While it's not possible to eliminate audits entirely, companies can shorten the amount of time auditors spend on site through careful documentation throughout the year.

Sage Intacct embeds audit traceability in all its relevant features, which means a record of all user actions pertinent to an audit are kept centrally within Sage Intacct. As a result, the finance team has access to the information auditors need.

User login history
Auditors need to understand who can access a company's financial management software. They need comprehensive login security along with documentation of who successfully logged in.

Sage Intacct documents each time a user either successfully or unsuccessfully logs into the system and creates a record with the user ID included. Regardless of whether the user was successful in logging in or not, their user ID, a timestamp, and the IP address of the device they used to log in are recorded. If they are successful in logging in, their session duration is included in the record as well.

Database records
Companies need to document the actions a user performs after logging in since auditors may need to investigate these transactions.

Whenever a user creates, edits, or deletes a record, Sage Intacct automatically documents the user ID of the employee who did so, while also creating a timestamp of when the action occurred. In doing so, Sage Intacct can show a task's chain of custody, so they know who they should consult should questions arise.

As users navigate Sage Intacct, the system documents changes that occur within the following action types:

- **Base tables**, such as customer, vendor, contracts, and others
- **Transactions**, including invoices, bills payments, journal entries, and others
- **Other features**, including custom reports and user setups

System-level audit trails
Changes in system configuration are important to track since changes could impact all users.

Each time a user changes a configuration on the Sage Intacct platform, such as within the general ledger or accounts payable, the user ID of the employee along with a timestamp and IP address are recorded.

Other tasks documented by Sage Intacct include the following:

- **Email delivery**
- **Smart Events**: A custom trigger that occurs when a certain condition is met, such as an email being sent when a transaction crosses a certain cost threshold
- **Offline job history**: Actions logged even when the system is performing work offline

For medical industry companies in need of HIPPA-compliant audit traceability, the Sage Intacct advanced audit functionality can also record each time a user views a customer, vendor, or contact in the system.

Application integration audit trail
Audit trails for integrated applications help auditors identify applications that access Sage Intacct and for what purpose to help protect against cybersecurity breaches.

In Sage Intacct, any time an API call takes place with a third-party application, a new report is created. Each report includes a timestamp, as well as a sender ID (unique token) and the function performed, such as creating an invoice or paying a bill. After an API report is compiled, users can access it within Sage Intacct.

Process checklists

Finance managers design processes and workflows to help them comply with regulations, as well as for general adherence to business processes. Auditors often request documentation of these processes to validate that processes comply and that the processes are consistently followed.

Sage Intacct gives finance teams the power and flexibility to define their own processes using custom process checklists. Checklists can be used for a variety of proceses, including the close process, vendor onboarding, and more. They allow finance managers to define the steps in a process and assign owners. Sage Intacct tracks the completion of each step, as well as who completed the step and the date and time it was completed.

Similarly, finance teams can create process checklists specifically for contract revenue recognition, where employees can record events for each individual contract such as when a contract was initiated and the date on which a service is rendered. Upon completion, a manager with proper permissions in Sage Intacct can then approve of the contract. Revenue recognition practices are a major component of SOX, which makes this process checklist valuable to any company operating under a subscription model.

Conclusion

Your finance team does its own due diligence each day, from documenting work to carefully reviewing transactions. Sage Intacct makes your own audits, as well as SOX compliance, simpler by centralizing many of these tasks and providing you with increased visibility and control. It also eases your transition to SOX compliance by providing extensive security, audit trails, and checklists to adhere to processes.

About Sage Intacct

Sage Intacct is the #1 cloud financial management system for data-driven, growing organizations. Our modern, true cloud solution with open APIs, gives multi-location or multi-entity organizations a shared chart of accounts, instant and continuous consolidations, and centralized payables while eliminating manual processes for payments and intercompany accounting. Sage Intacct helps you save time and improve accuracy—without adding staff.

About Equation Technologies

Equation Technologies provides business management solutions for mid-sized companies in the USA and Canada. We make carefully crafted recommendations from among the industry's best-performing ERP software, including Sage Intacct and Sage 300. We help you **reduce the risk in choosing and implementing solutions** by:

- Listening closely to your challenges and exactly how your business works.
- Developing processes that match your business, not requiring you to conform to a software system.
- Mapping out efficiencies using technology to improve operations without adding staff.

Our main goal is simple: have a clear understanding of our clients' goals. We believe the only way to sufficiently grasp that information is by listening first, and offering valuable advice later. We also know that one single approach is not right for all businesses. We leverage our team's vast education and business experiences across industries to focus on our clients' unique needs. We understand the importance of your business. We know when you call on us, time is of the essence and we value & respect your time.

Equation Technologies
533 2nd Street Encinitas, CA 92024
866-436-3530
www.equationtech.us