bakertilly

Proprietary & Confidential

Acumatica
The Cloud ERP

Cloud ERP System

SOC 3
Relevant to Security and Availability

Integrated SOC 3 Report Prepared in Accordance with the AICPA Attestation Standards and IAASB ISAE No. 3000 (Revised) Standards

OCTOBER 1, 2024 TO SEPTEMBER 30, 2025

Table of Contents

I. Independent Service Auditor's Report

Acumatica, Inc.
3075 112th Avenue NE, Suite 200
Bellevue, WA 98004, USA

To the Management of Acumatica:

Scope

We have examined Acumatica's accompanying assertion in Section II titled "Acumatica's Assertion" (assertion) that the controls within Acumatica's Cloud ERP System (system) were effective throughout the period October 1, 2024 to September 30, 2025, to provide reasonable assurance that Acumatica's service commitments and system requirements were achieved based on the trust services criteria relevant to security and availability (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus – 2022)*, in AICPA *Trust Services Criteria*.

Acumatica uses Amazon Web Services (AWS) as a platform as a service (PAAS) provider (subservice organization). Acumatica's description of the boundaries of its system indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Acumatica, to achieve Acumatica's service commitments and system requirements based on the applicable trust services criteria. The description presents the types of complementary subservice organization controls assumed in the design of Acumatica's controls. The description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

Service Organization's Responsibilities

Acumatica is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Acumatica's service commitments and system requirements were achieved. Acumatica has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Acumatica is responsible for selecting, and identifying in its assertion, the applicable trust services criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the AICPA and in accordance with International Standard on Assurance Engagements 3000 (Revised), *Assurance Engagements Other Than Audits or Reviews of Historical Financial Information*, issued by the International Auditing and Assurance Standards Board. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that controls were not effective to achieve Acumatica's service commitments and system requirements based on the applicable trust services criteria
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve Acumatica's service commitments and system requirements based on the applicable trust services criteria

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Service Auditor's Independence and Quality Control

We are required to be independent and to meet our other ethical responsibilities in accordance with the Code of Professional Conduct established by the AICPA and the International Ethics Standards Board for Accountants' Code of Ethics for Professional Accountants.

We applied the Statements on Quality Control Standards established by the AICPA and, accordingly, maintain a comprehensive system of quality control.

Inherent Limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, management's assertion that the controls within Acumatica's Cloud ERP System were effective throughout the period October 1, 2024 to September 30, 2025, to provide reasonable assurance that Acumatica's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Baker Tilly US, LLP

Seattle, Washington
December 19, 2025

Acumatica
The Cloud ERP

II. Acumatica's Assertion

We are responsible for designing, implementing, operating, and maintaining effective controls within Acumatica's Cloud ERP System (system) throughout the period October 1, 2024 to September 30, 2025, to provide reasonable assurance that Acumatica's service commitments and system requirements were achieved based on the trust services criteria relevant to security and availability (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus – 2022)*, in AICPA *Trust Services Criteria*. Our description of the boundaries of the system is presented in Attachment A and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period October 1, 2024 to September 30, 2025, to provide reasonable assurance that Acumatica's service commitments and system requirements were achieved based on the trust services criteria. Acumatica's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in Attachment B.

Acumatica uses Amazon Web Services (AWS) as a platform as a service (PAAS) provider (subservice organization). The description of the boundaries of our system indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Acumatica, to achieve Acumatica's service commitments and system requirements based on the applicable trust services criteria. The description presents the types of complementary subservice organization controls assumed in the design of Acumatica's controls. The description does not disclose the actual controls at the subservice organization.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period October 1, 2024 to September 30, 2025, to provide reasonable assurance that Acumatica's service commitments and system requirements were achieved based on the applicable trust services criteria.

Attachment A - Acumatica's Description of the Boundaries of Its Cloud ERP System

A. System Overview

1. Services Provided

Founded in 2008, Acumatica is a technology provider that develops adaptable cloud- and browser-based enterprise resource planning (ERP) software and solutions designed to improve productivity of small and medium-sized businesses.

Built on cloud and mobile technology, and a unique customer-centric licensing model, Acumatica delivers a suite of fully integrated business management applications, such as Financial, Customer Relationship Management (CRM), Construction, Distribution, Project Accounting, and Service Management, on a robust and flexible platform. In the interconnected world, Acumatica enables customers to take full control of their businesses, plays to their organizations' unique strength, and supports customers by following them anywhere on any device.

Acumatica is a global company with commercial headquarters in Kirkland, Washington, United States.

Acumatica's web-based ERP applications are built on top of its internally developed platform. The server software can be deployed on-premises, hosted in a data center, or run on a cloud-computing platform. The software can be licensed or purchased as a Software as a Service (SaaS) solution. The SaaS version of Acumatica is the scope of this report. The Company and its partners continue to develop horizontal and vertical extensions of features and functionality in the software and platform. Currently, Acumatica's product line includes general business applications and vertical editions:

- Acumatica General Business/Financial Management
- Acumatica Commerce Edition
- Acumatica Construction Edition
- Acumatica Distribution Edition
- Acumatica Manufacturing Edition
- Acumatica Field Service Edition

SUBSERVICE ORGANIZATIONS

Acumatica uses Amazon Web Services (AWS) as a platform as a service (PAAS) provider.

This subservice organization is excluded from the scope of this report.

2. Infrastructure

Acumatica's Cloud ERP System delivered as a SaaS application is based on a modern SaaS architecture. The Company's SaaS services are hosted on AWS and can be accessed from any web browser on any internet-connected device. Acumatica's technology is built for scalability which allows Acumatica SaaS resource levels to scale from small to extra-large. SaaS deployment enables Acumatica to ensure the highest levels of security, availability, and performance. Acumatica SaaS includes a range of benefits backed by SLAs such as disaster recovery, backup service, 24x7 access, high availability, monitoring, software updates, and application maintenance.

Acumatica's SaaS application currently runs on Microsoft SQL Server hosted on AWS which provides cloud infrastructure. AWS follows strict guidelines and uses architectural and engineering approaches to guard against physical and environmental threats. AWS has extensive experience in designing, constructing, and operating large-scale data centers. Physical access is strictly controlled, both at the perimeter and at ingress points by security staff and video surveillance. Staff members pass two-factor authentication to access the data center. Visitors and contractors are required to present identification and are escorted by authorized staff. There are also fire detection and suppression, power, climate and temperature, and electromechanical support systems.

Acumatica's hosting providers use standard hardware and software configurations to host the SaaS services, including servers, routers, and switches, Microsoft SQL Server Internet Information Services (IIS), and Windows Server. Systems and upgrades go through a system acceptance process before being deployed. Operating system configurations are performed according to detailed Acumatica configuration baselines and tested prior to deployment. Users are provided with access to the SaaS services they have been specifically authorized to use. Acumatica controls the use of its network resources through a firewall.

Acumatica has a formal process for security patch identification, assessment, and application to keep up to date with critical and security patches provided by the manufacturer. Production servers are configured to ensure that servers in the Acumatica production environment have the appropriate software revisions and required patches applied on time. The regular checking processes safeguard to prevent unneeded services and protocols are disabled, removed, or accordingly configured. Acumatica follows a standardized approach when provisioning new servers to the production environment by verifying that servers are configured according to the Acumatica information security policy.

Acumatica's production ecosystems, which include desktop PCs and laptops, are protected by security protection software such as Microsoft ATP. This software package is configured to perform regular updates and continuously monitor the production environment to prevent, detect, and remove malicious viruses such as malware, spyware, browser hijackers, and many others. The Acumatica IT Support Team is available 24x7 to respond to malware alerts and to take appropriate action based on the standardized incident handling processes. Any machine found to be infected by malware gets disconnected from the network immediately.

In addition to secure coding practices, a vulnerability self-assessment, including penetration testing, is performed annually by the Development Team or by a third party in order to identify any security weaknesses that could allow access to the Acumatica SaaS services and/or network. Penetration tests are performed on external and internal critical devices. Vulnerability assessments of production systems and external penetration testing are conducted on an annual basis.

Acumatica has monitoring applications in place to monitor overall systems as well as monitoring the individual hardware. IT procedures exist for the escalation of systems availability issues and potential security breaches. Production servers and the supporting network infrastructure are monitored for system and process failures, availability, downtime, and capacity issues. Alerts are designed and put in place to send out immediate notification to support personnel in the event of a failure or reaching a critical threshold.

Acumatica has built a system that enables 24x7 availability and to meet SLA uptime commitments to customers. Contracts and agreements are in place to provide support for critical hardware equipment.

Acumatica has established an incident response plan to respond to security breaches, fraud, faults, and other disruption to business processes, contractual agreements, or privacy. Security incidents detected are resolved using Acumatica's Information Security Policy. The Incident Response Team (IRT) manages incidents handling to reduce negative impact on operations. The incident response plan includes the following:

- Identification
- Initial Assessment
- Containment (First Response)
- Eradication
- Recovery
- Lessons Learned

Incidents reported by internal or external users are documented, dated, and tracked in the Acumatica's JIRA tracking system. Issues are assigned a severity level and assigned to appropriate incident response team members to take ownership and resolve the incident.

3. Software

To unlock business potential, Acumatica application suites are web-based, fully integrated, and work on a centralized database system. They can be accessed anywhere, anytime, and on any device. Designed for businesses looking for modern enterprise software powered by the cloud, the Acumatica Cloud ERP System delivers a suite of fully integrated applications, powered by a robust and flexible platform. Acumatica's product line includes general business applications and vertical editions:

- *General Business/Financial Management* – A powerful financial application simple enough for smaller businesses and comprehensive enough for complex multi-national companies. It provides web-based accounting in a feature–rich, integrated operational suite ecosystem.
- *Customer Relationship Management (CRM)*– Web-based CRM applications for managing leads, contacts, opportunities, and customer accounts. It provides a single consolidated view of customer contacts and real-time dashboards and reports to help manage forecasts, quotas, and results.
- *Commerce Edition* - Manage eCommerce orders, inventory, picking-packing-shipping, returns, customer support, and accounting from one dashboard. Tightly integrates Financials, Sales, Inventory, CRM, and Fulfillment systems with popular eCommerce platforms, including native integration to webstores. Offers native support for customer specific pricing, products with variants, multiple warehouses, discounts and promotions, shipment tracking, and more.

- *Distribution Edition* – Automates and increases efficiency in purchasing, order fulfillment, and inventory tracking. It manages sales orders, tracks inventory, fills orders, and improves purchasing.
- *Manufacturing Edition* – Integrates production planning, material purchasing, and shop floor scheduling with customer management, sales orders, inventory, purchasing, and accounting for real-time coordination of multi-plant activities.
- *Construction Edition* – Manages budgeting, inventory, time sheets, billing, profitability, and reporting for individual business initiatives, with editions available for construction specific entities as applicable. Its features are integrated with general ledger, accounts payable, accounts receivable, sales orders, purchase orders, inventory management, and the time and expense mobile application.
- *Field Services Edition* – Tracks and optimizes processes of field services operations. Service orders, appointments, contracts, warranties, routes, staff skills, equipment capabilities, preventative maintenance schedules, and a drag-and-drop dispatch board are all available.

Some of the most popular features of the Acumatica suites that help customers drive growth, manage costs, and be more productive are:

- Ease of use for maximum productivity
- Speed and performance
- Extensible
- Third-party solutions and integrations
- Technology advancements

4. People

Acumatica is a global company on a mission to help businesses be more efficient and effective. Acumatica has an active Board of Directors that meets regularly. The Board of Directors and Advisors provides strategic guidance to senior management.

The CEO is responsible for providing leadership to position the Company at the forefront of the ERP industry. The responsibilities of the CEO are to develop and maintain a strategic plan to advance Acumatica's mission and objective and to promote revenue, research and development, profitability, and growth as an organization. The CEO also oversees Acumatica's operations to ensure quality, service and cost-effective management of resources. Acumatica's leadership team members report directly to the CEO.

Acumatica has a team of approximately 280 employees in its global organizational structure. The global structure is departmentalized with an executive level functional leader providing organizational support for Acumatica's business activities. The global executive level structure is composed of the following key functions:

ENGINEERING AND DEVELOPMENT

Led by the CTO, Acumatica's engineering and development organization is responsible for design, development, testing, and deployment of the Company's core technologies and product. Acumatica also uses contract developers under the CTO's direction to supplement the engineering and development group. The Company invests substantial resources in research and development to drive core technology innovation and to bring new products to global markets.

Acumatica has historically targeted major product releases twice per calendar year. In addition, the Company provides maintenance releases with bug fixes and incremental functionality on at least a quarterly basis. The release cycles enable Acumatica to be responsive to customers by delivering new functionality on a frequent basis.

PRODUCT MANAGEMENT, SERVICES, AND SUPPORT

Led by the CPO, Acumatica's services and support organization is responsible for providing professional services and technical support to the Company's partners and end-user customers. Professional services include implementation, customizations and training delivered in person, phone-based, over the internet, and/or through webinars.

PARTNER PROGRAMS AND STRATEGY

Led by the Vice President, Partner Program and Strategy, reporting to the CRO, Acumatica's partner organization is responsible for the recruitment, onboarding, training and enablement of Value-Added Resellers (VARs). The partner program and strategy activities include implementation and training delivered in person, phone-based, over the internet, and/or through webinars.

SALES

Led by the Vice President of Partner Sales, reporting to the CRO, the sales organization is responsible for the global sales of Acumatica's SaaS products, licensed software and services. Acumatica sells its products primarily through partners including VARs, Independent Software Vendors (ISV), and Original Equipment Manufacturers (OEMs). The customer success team within the sales organization led by the CRO is responsible for supporting existing customers' use of Acumatica solutions.

MARKETING

Led by the CMO, Acumatica's marketing organization focuses on establishing the Company brand, generating awareness, creating leads, and cultivating the Company community. The marketing team consists primarily of partner marketing, campaigns, product marketing, field events, digital marketing, and corporate communications.

FINANCE AND LEGAL OPERATIONS

Led by the CFO, Acumatica's Finance organization is composed of the Finance and Legal departments. Responsibilities of these departments include support of the sales, and marketing organizations. Activities include the negotiation of contracts and agreements, intellectual property assets and patent protection, accounting, commissions, tax, travel, and corporate risk management, corporate governance, and compliance.

HUMAN RESOURCES

Led by the Chief People Officer, Acumatica's Human Resource organization is composed of the Human Resources and Recruiting departments. Responsibilities of these departments include support of the engineering and development, services and support, sales, marketing, sales and general & administrative organizations. Activities include recruiting, onboarding, employee development, performance assessment, employee benefits, and payroll.

INFORMATION SECURITY OPERATIONS

Led by the Sr. Director of Cyber Security, Responsibilities of Acumatica's Information Security team include overseeing the enterprise information security strategy and ensuring corporate and customer assets are protected. Activities include risk management, management of information security solutions and technology, auditing, corporate governance, and compliance.

SECURITY OPERATIONS CENTER

Led by the Sr. Director of Cyber Security, Acumatica employs services from Ontinue, The MDR division of Open Systems to provide 24x7 monitoring, reporting and mitigation of cyber threats for both Acumatica corporate and customer hosted environments.

5. Data

Acumatica's SaaS application receives data input from customers. Data is not stored on a customer's computer or services, but instead data remains on Acumatica's servers. As customers provide data through the application interface, only small bits of the data are transferred to the web browser, and even then, only for a brief instant. Once forms are completed, no data remains in the web browser.

Transmission of data is secure and encrypted using SSL technologies. Acumatica provides an Acumatica URL that is protected by SSL standards. In addition, Acumatica's intrusion detection system (IDS) detects attempts to compromise the confidentiality, integrity, and/or availability of customers' data, and/or to circumvent security controls. In the event of intrusion attempts, the intruder is locked out of the system, and an investigation is conducted to identify and locate the origin of the intruder.

Acumatica performs continuous automated backups of data with daily, weekly, monthly, and quarterly retention periods at no extra charge to customers. Additionally, incremental backups of transaction logs are performed frequently throughout the current day. Acumatica backs up transactional data to an additional geographic zone for an additional layer of protection and disaster recovery. In the event of a disaster, where a data center hosting customers' data is completely shut down, Acumatica quickly goes through a fail-over recovery procedure and services resume from an alternate data center. Acumatica's SLA uptime guarantee continues to provide data protection during this duration.

6. Processes and Procedures

As a company in pursuit of excellence, Acumatica has put in place processes and procedures which include but are not limited to:

- System Development Lifecycle (SDLC) governs the design, testing, implementation, configuration, modification, and maintenance of systems components.
- Change management process governs changes to production systems and applications, including emergency or escalation change requests.
- Incident handling process governs management of incidents and reduces the impact to operations.
- Access management process governs access to systems including web applications, third-party applications, local system accounts, and domain accounts are controlled through a formal registration process based on users' specific roles.
- Risk assessment and treatment process governs procedures for potential risks, known and unknown, that could negatively impact the overall objectives of the business.
- The backup and recovery process governs procedures for customers' data, essential business information, and critical systems being regularly backed up and can be recovered in the event of a critical failure or natural disaster.
- Capacity planning process governs procedures for production hardware capacity maintaining adequate levels of performance to satisfy customers' needs.
- Business continuity plan governs the Company business in the event of unexpected and unplanned circumstances related to key risks for employee safety, and the Company's capability of maintaining critical activities and providing services to partners and customers.
- Information security policy governs security standards and procedures addressing the confidentiality, availability, and integrity of Acumatica data and systems.

B. Complementary Subservice Organization Controls

Acumatica's controls related to the Cloud ERP System cover only a portion of overall internal control for each user entity of Acumatica. It is not feasible for the criteria related to the Cloud ERP System to be achieved solely by Acumatica. Therefore, each user entity's internal controls must be evaluated in conjunction with Acumatica's controls, taking into account the types of controls expected to be implemented by the subservice organizations as described below.

Complementary Subservice Organization Controls	
Amazon Web Services	
1	The subservice organization is responsible to ensure that network devices in the scope boundary are configured to log and collect security events and monitored for compliance with established security standards.
2	The subservice organization is responsible to ensure that electronic intrusion detection systems are installed to monitor, detect, and automatically alert appropriate personnel of security incidents.
3	The subservice organization is responsible for physical and logical access to client data restricted to personnel with a business need for access.

Complementary Subservice Organization Controls	
4	The subservice organization is responsible to ensure physical and logical access is revoked in a timely manner upon termination.
5	The subservice organization is responsible to ensure that changes are tested and released into production do not occur until appropriate signoffs are obtained and documented.

C. User Entity Responsibilities

There are no controls at the user entity that are necessary, in combination with Acumatica's controls, to provide reasonable assurance that Acumatica's service commitments and system requirements were achieved based on the applicable trust services criteria (complementary user entity controls).

There are, however, certain responsibilities that users of the system must fulfill for the user entity to derive the intended benefits of the services of the Acumatica's Cloud ERP System. The user entity responsibilities presented below should not be regarded as a comprehensive list of all controls that should be employed by user entities. User entities are responsible for their own control environments and their operational effectiveness.

User Entity Responsibilities	
1	Notifying Acumatica of any specific security requirements to their infrastructure.
2	Understanding and complying with their contractual obligations to Acumatica.
3	Alerting Acumatica about any regulatory changes within their industry that might affect their services.
4	Notifying Acumatica of changes to specific contact information such as phone numbers, emails address, fax and/or mail addresses.
5	Allowing only authorized personnel to know and understand the services, networks, and supporting infrastructure of their company.
6	Ensuring that system logging is enabled and sufficient for their purposes.
7	Managing all application-level audit tracking not specifically provided by Acumatica as part of contractual service.
8	Implementing security, policies, and procedures that help protect their systems from unauthorized or unintentional use, modification, addition, or deletions and limit threats from connections from other networks.
9	Creating passwords that are sufficiently complex and maintaining policies that support routine changes of the passwords.
10	Managing the access to production systems provided to customer employees. Ensuring that customer employee access abilities are commensurate with the responsibility assigned to said employee.

Attachment B – Principal Service Commitments and System Requirements

Acumatica designs processes and procedures to meet its objectives for the services provided. The objectives are based on the service commitments Acumatica makes to its customers, the laws and regulations that govern delivery of its services, and the financial, operational, and compliance requirements the Company has established for these services. Acumatica technology services are subject to the security requirements, legal requirements, as well as state security laws and regulations in the jurisdictions in which Acumatica operates.

Security commitments to customers are documented and communicated in Acumatica's Service Level Agreements (SLAs), as well as in the Terms of Use, and General Data Protection Regulation (GDPR) disclosed on the Company's website.

Security commitments are standardized and include, but are not limited to, the following:

- Acumatica is committed to protecting the security of customers' personal information. Acumatica uses a variety of security technologies and procedures to help protect customers' personal information from unauthorized access, use, or disclosure.
- Acumatica security principles are designed to permit system users to access the information they need based on their role in the system while restricting them from accessing information not needed for their role.
- Acumatica employs redundant, next-generation firewalls, intrusion detection, and prevention services monitored 24x7x365.

Acumatica establishes operational requirements to support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated through internal policies, standards and procedures, system design and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected.