Acumatica
The Cloud ERP

Confidentiality, Integrity, and Availability
The Security Foundation of Acumatica's Cloud ERP

In the midst of migrating your organization's most important applications and data processing capabilities to the cloud?

Maybe it's time your ERP functions made the jump.

The Acumatica Cloud Enterprise Resource Planning (ERP) application is based on the latest Software as a Service (SaaS) architecture, ensuring the highest level of security, availability, and performance. Hosted primarily on Amazon Web Services (AWS) and Microsoft Azure (Azure), it can be accessed from any device connected to the Internet. Acumatica's cloud technology is also built to scale, allowing its SaaS resource levels to grow with your organization's needs.

Recognizing that migrating critical enterprise functions to the cloud carries significant risks for any organization, Acumatica's Cloud ERP solution is based on core information security principles: confidentiality, integrity, and availability. Acumatica's information security program, integrated into the core of our business, continuously identifies information security and operational risks, evaluates those risks, and develops remediation strategies. By maintaining a control environment that is both strong enough and flexible enough to execute remediation strategies when needed, Acumatica protects your key ERP functions and data while ensuring that any new threats or risks are promptly identified and managed.

Acumatica's information security program synthesizes people, processes, and technology. This promotes both the development and operational maintenance of the Cloud ERP solution as well as the ongoing management of customer production environments and data. Acumatica works to continuously improve this focus through:

- Identifying and mitigating information security and operational risks
- Maintaining detailed information security and operational policies and procedures
- Implementing security classifications for customer data to ensure that the necessary controls are in place to keep data safe
- Assessing information security risk and applying best-practice risk remediation strategies in order to mitigate potential risks before they become a threat to a client
- Independently auditing and certifying the security and operations of our control environment
- Conducting regular and up-to-date information security awareness trainings to ensure employees are aware of the latest threats and risks to data security

Our Commitment to Your Organization

When it comes to information security, the implementation details matter. Acumatica is committed to the protection and availability of your data and ERP functions. Combining a world-class application with the industry standard for hosting environments (AWS and Azure) means that Acumatica's Cloud ERP

solution puts both the confidentiality and integrity of your data and the availability of your applications front and center.

Confidentiality

- Acumatica isolates each client's data into a unique database using a multi-tenant approach to SaaS, creating better data security and preserving data confidentiality
- User account management is governed by Acumatica's Access Management Policy
- Segregation of duties means that only users with the highest need have access to data and environments and that critical functions have been separated appropriately
- Customers are given unique access credentials to their Cloud ERP application. Each organization can:
    - Configure user ID and password complexity requirements as needed
    - Implement role-based access control within the Acumatica ERP solution
    - Limit logins to a specific Internet Protocol (IP) address
    - Create one-time passwords
    - Encrypt sensitive database information
- A distinct Acumatica URL using Secure Sockets Layer (SSL) encryption is issued to each client ensuring secure connections to Cloud ERP.
- Data is never stored on the user's computer; all data remains on Acumatica servers. As users complete forms, only small bits of data are transferred to the web browser; once forms are completed, no data remains in the browser
- Each customer environment is segmented by a firewall

Integrity

- The Acumatica IT support team is available 24x7 to respond to malware alerts and handle security incidents as they arise
- Acumatica's intrusion detection system (IDS) alerts Acumatica's team to any security breach that might compromise the confidentiality, integrity, or availability of your data
- Acumatica web servers are protected against Distributed Denial of Service (DDoS) attacks by AWS Shield service, which defends against the most common, frequently offering network and transport layer attacks with real time automatic mitigations
- Critical ERP functions and data are centrally monitored and audited and can be configured based on customer specifications to meet detailed requirements
- The production environment is monitored using Symantec and TrendMicro to prevent, detect, and remove malicious viruses such as Trojans, worms, spyware, browser hijackers, and many others
- Access to program source code (as well as designs, specifications, verification plans, and validation plans) is strictly controlled in order to prevent unauthorized functionality unintentional changes from being introduced into the environment
- Security patches are kept up-to-date through regular identification, assessment, and application

of new patches
- Acumatica Web Server Hardening policy is applied to all web servers to create an additional layer of protection against known vulnerabilities and attacks
- Unnecessary or outdated services and protocols are regularly disabled, removed, or reconfigured
- Acumatica maintains separate development, test, and production environments to reduce the risk of accidental changes or unauthorized access to production software or business and customer data
- All systems and upgrades go through an acceptance process before deployment
- Operating system configurations follow strict internal processes and are tested prior to deployment
- Secure coding practices are used during the Software Development Lifecycle (SDLC) and system update processes
- An annual risk assessment and penetration test is performed on each individual system, network device, firewall, and application

Availability
- Acumatica's customers can count on 24x7x365 availability with historical uptime performance consistently near 100% and well above industry standards
- Hosting providers, AWS and Azure, assure 24x7x365 technology availability and global support
- Network performance and system processing are constantly monitored, and all incidents are subject to a rigorous internal resolution process to ensure your organization never loses access to your information
    - Logging software collects data from system infrastructure components and endpoints, monitoring system performance, potential security threats and vulnerabilities, resource utilization, and unusual system activity or service requests
    - Systems are configured to log key security events including authentication events and file access
    - Health and capacity metrics are monitored and reviewed on an ongoing basis so that your systems and processes never experience lags or downtimes.
- Backup and recovery processes mean that customer data, essential business information, and critical systems can be recovered in the event of a critical failure or natural disaster. Acumatica's processes include:
    - Multi-level, nightly, encrypted backups of each customer environment
    - Backups are replicated offsite on a daily basis to various global locations
    - Monthly data restoration is performed for testing purposes
    - A Business Continuity Plan (BCP) is in place and regularly tested
- Each database transaction is written to a Transaction Log with each Transaction Log being exported offsite every 15 minutes ensuring that, at any point, Acumatica can restore a customer

database with a maximum data loss of 15 minutes

- Using Acumatica's snapshot capabilities, customers can export all data from the database and import it to another Acumatica instance elsewhere, keep offline backups of their own data, or setup their own test environments without needing direct access to their Acumatica database server.

Acumatica has an established incident response plan for security breaches, fraud, faults, and other disruptions to business processes, contractual agreements, or data privacy. Any security incidents that are detected are resolved using Acumatica's Information Security Policy. The Incident Response Team (IRT) handles incidents quickly and expediently to reduce the impact to your organization.

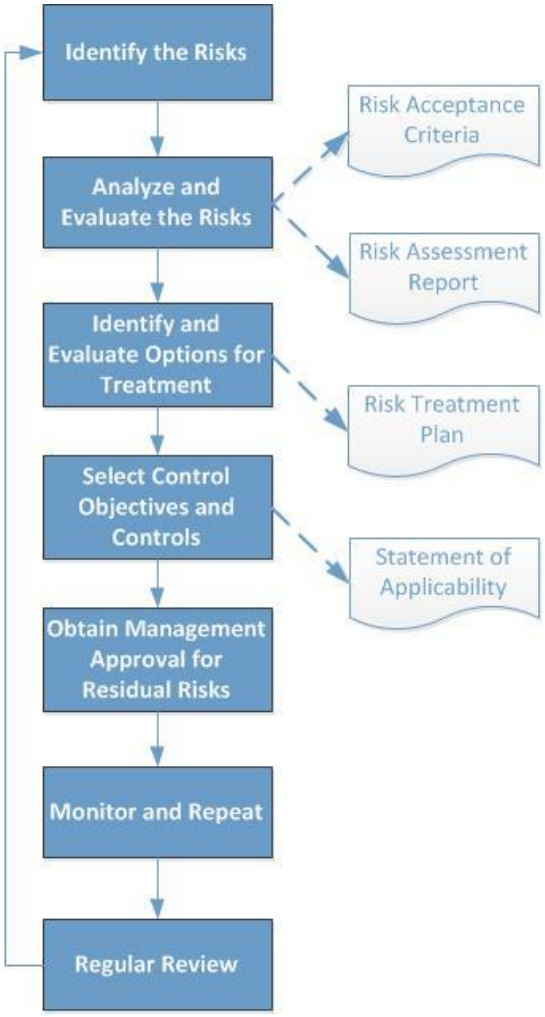
Risk Management

Acumatica recognizes that risk management is critical to protecting your organization and, as such, has an information security risk assessment and treatment (ISRA) process. The ISRA process ensures that potential impacts do not become real and, if they do, contingencies are in place to deal with them appropriately. Acumatica also follows the industry standard, ISO/IEC 27001, when identifying risks to the confidentiality, availability, and integrity of information and assets.

The ISRA process is shown in the diagram below:

Acumatica
The Cloud ERP

Confidentiality, Integrity, and Availability
The Security Foundation of Acumatica's Cloud ERP



Secure Infrastructure

When evaluating your cloud computing options, it is important to consider the entire service stack of the cloud provider. Many different organizations may be involved in providing infrastructure and application services, increasing your organization's risk. A disruption at any layer of the cloud/application stack could compromise the confidentiality, integrity, or availability of your data.

Acumatica starts with the most reliable hardware infrastructure in the industry to supply the virtual fabric for its customer environments. Amazon and Microsoft have many years of experience in designing, constructing, and operating large-scale data centers. This experience has been applied to their state-of-the art cloud-based hosting platforms and infrastructure: AWS and Azure are built for scalability and extreme reliability through their innovative architectural and engineering approaches.

Acumatica
The Cloud ERP

Confidentiality, Integrity, and Availability
The Security Foundation of Acumatica's Cloud ERP

Acumatica's Cloud ERP solution provides a SaaS stack that is supported by strong operational and security policies, procedures, and controls as a direct result of their technology partnerships. By leveraging the cloud infrastructure of Amazon and Microsoft, Acumatica's clients benefit from a tightly controlled and secure environment grounded in the physical hardware and data centers that set the industry standard for operational and security process excellence. Some of the operational and security process benefits are that:

- Amazon and Microsoft data centers both receive SSAE16/ISAE 3402 Attestations and are ISO 27001 Certified. Their data centers are located in non-descript buildings that are physically constructed, managed, and monitored 24-hours a day for unauthorized access and environmental threats. Data centers are surrounded by a fence with access restricted through badge controlled gates.
- Both organizations restrict access to audit logs to authorized personnel based on job responsibilities. Event logs are archived on secure infrastructure and are retained.
- The cloud fabric agent hosts are Host OS and Native OS. These hardened operating system images run on computing and storage nodes, which has the benefit of reducing the surface area exposed by APIs or unused components. These reduced-footprint operating systems include only those components necessary to the environment, which both improves performance and minimizes the potential attack surface.
- Amazon and Microsoft both regularly scan for vulnerabilities on their hosts. Vulnerability scanning is performed on server operating systems, databases, and network devices with the appropriate vulnerability scanning tools.
- Amazon and Microsoft have developed robust incident management frameworks to detect, escalate, and respond to incidents. Incident management teams perform 24x7 monitoring, including documentation, classification, escalation, and coordination. Events, thresholds, and metrics have been defined and configured to detect incidents and alert the appropriate teams.

Acumatica's Cloud ERP solution and its technology partners Amazon and Microsoft provide a SaaS stack that is supported by strong operational and security policies, procedures, and controls with the objective keeping your data safe, secure, and available.