Security Framework

Icertis maintains a formal information security program and information security team focused on protecting the information assets of our customers. The following provides a high-level overview of elements of the security that surrounds customer data in connection with our services.

Area	Icertis Contract Intelligence (ICI) Platform
Risk Management	Icertis has identified and classified assets based on the criticality. Security risks related to the ICI instance, internal personnel, assets, and external parties (such as contractors, customers, and vendors) are identified and addressed via the ISO 27001: 2013 framework and applicable controls. Risk management is a continuous process adapted at Icertis.
Information security policies and framework, compliances	The ICI Platform is hosted on the Microsoft Azure cloud platform and available as a SaaS offering to subscribers. The ICM Platform is developed using Microsoft technologies like .NET, ASP.NET MVC, SQL Server, etc. These services provided to Icertis by Microsoft follows industry practices and security measures towards ensuring high availability, confidentiality, integrity, and privacy of the cloud based services we provide to the Subscriber. For Azure data center compliance, please refer to https://azure.microsoft.com/en-in/overview/trusted-cloud/ Icertis is an ISO 27001, ISO 27017, and 27018 certified organization. Icertis also complies with ITAR and has SOC2 (Type1, type2) certifications.
Human resource security	All employees working on the ICI Platform are subject to background verification, and are bound by contractual obligations of confidentiality. Employees go through various training sessions necessary to perform their duties, including training regarding information security covering specific topics such as GDPR and HIPAA.
Asset management	Icertis maintains the assets in its cloud infrastructure, which are managed, and monitored by an internal cloud operations team.
Physical and environmental security	The ICI Platform is hosted on the Microsoft Azure cloud. For Azure data center compliance, please refer to https://azure.microsoft.com/en-in/overview/trusted-cloud/
Communication and Ops management	The ICI Platform is hosted on the Microsoft Azure cloud with VNET, which are protected by various Azure security features such as DDoS protection, intrusion detection/intrusion prevention systems (IDS/IPS), web filtering, network antimalware. Access to all other infrastructure components is deterred from outside Azure VNET because each subnet is protected by a NSG (Network Security Group). Web endpoints of the ICI Platform application are exposed using HTTPS.
Application security	IT senior management ensures that any business-critical changes at the application level are pre-approved and go through thorough security review. This is induced from architecture designing, specification defining phase to the deployment and testing phase. Icertis has adopted the Microsoft security development lifecycle. Icertis commissions regular third party vulnerability assessments and penetration testing for the application. All builds, including nightly builds go through the security scanning.

	The ICI Platform can integrate with a subscriber identity provider for user authentication using industry-standard protocols like SAML2. OAuth\Open ID, WS-Fed. If Multi-Factor authentication is enabled on the identity provider side, the ICI Platform by default, supports it. Active threat monitoring and prevention using the Azure Security Center is configured. Audits logs are maintained and monitored at a specific frequency. Microsoft Azure services to Icertis to support the ICI offering include a high availability and disaster recovery capability. All data at rest is encrypted using AES 256-bit encryption, which is provided by underlying Azure services. Encryption keys are managed by Microsoft Azure. If required, Icertis can manage the encryption keys in the Azure Key Vault. For data in transit, data encryption is done using the certificate. Icertis has detailed audit logs in the system. The transaction audit log is captured in the history of the transaction. The ICI Platform captures all user actions on the user record with date and time stamp.
Access Control	Strict role-based access control is implemented in the ICI Platform. Icertis understands that the management of authentication (the user's identity) and authorization (the user's permissions) is critical to an application's overall security posture. The ICI Platform supports various kinds of authentication mechanisms. Authorization is generally implemented using various authorization features provided within the ICI Platform.
BCP and DR	Icertis is hosted on and stores data in a Microsoft Azure data center. The particular Microsoft Azure data center may be selected by the Subscriber at the outset of the subscription. Regular backups are performed for production data as per Azure's frequency and backups are stored on the geo replicated Azure BLOB storage.
Security Incident communication management	Icertis will notify the Subscriber in case of violation or breach of security resulting in a loss or unauthorized disclosure of Subscriber Data. A formal information security incident management process is followed. Incidents are reported by an observer or internal teams monitoring activities and are acted upon immediately. The incident is contained first, to minimize impact, and then resolved. A root cause analysis is then performed and documented. Mitigation or resolution actions are performed and documented. Internal escalations are performed as needed. The entire incident is documented for generating a knowledge base.
Data Security and Privacy	Icertis treats data provided by Subscribers to the ICI Platform as confidential. Icertis has implemented technical and organizational measure to protect the data, including PII.