Why ISO 27001 Certification is Essential in eDiscovery

ZyLAB is one of the few companies in the eDiscovery space that has earned an ISO 27001 certification.

Other companies claim to be *compliant* with the data security practices set forth in ISO 27001. But anyone could say they are compliant. It holds nowhere near the same weight as obtaining ISO 27001 certification, which we did to unequivocally prove we safeguard your data using the most secure measures available.

Why do you care about semantics and some random standard? Because data breaches are a daily threat, and ISO 27001 certification protects you from their catastrophic effects.

Vulnerable Data & Security Risks Abound

Corporations and law firms are using eDiscovery platforms at higher rates than ever to help them process large amounts of data efficiently and effectively. Government agencies are also finding great value in using eDiscovery technology to manage their data and process public records requests.

Much of that data contains sensitive financial information, intellectual property, Social Security numbers and other personally identifiable information, trade secrets, and myriad other private and confidential information. If any of this information is exposed to the public, the party who failed to secure the data will suffer serious – often irreparable – damages to their business and reputation.

Make Sure You're Protected from Costly Consequences

IBM's 2018 Cost of a Data Breach found that globally, the impact of a data breach on an organization averages $3.86 million; though "mega" breaches can cost hundreds of millions. Legislation such as the General Data Protection Regulation and the California Privacy Act set harsh penalties for security violations. But costs surge from all sides when your data is under attack.

It seems as if everywhere you turn, another breach is costing another company millions of dollars. In 2018 alone:

- An unauthorized user accessed the unencrypted data of up to 500 million Marriott customers, which is expected to cost Marriott millions in fines, legal fees, compensatory damages, etc.
- Security failures such as allowing unauthorized access to facilities and equipment and failing to encrypt health data cost Fresenius Medical Care NA $3.5 million.
- Hackers discovered the modification of a single line of code on Ticketmaster's payment page that allowed them to steal the personal data of 40,000 customers.

These are just a few examples of the many varied ways data can be exposed or hacked. They are also important reasons to ensure your eDiscovery technology provider possesses an ISO 27001 certification that demonstrates they deliver the highest level of protection against security risks. Settling for a vendor without an ISO 27001 certification is like driving on icy roads with no seatbelt. (Just don't do it!)

Settling for an eDiscovery vendor that doesn't have an ISO 27001 certification is like driving on icy roads with no seatbelt.

Is ISO 27001 certification really that big of a deal?

Yes. Few companies earn an ISO 27001 certification because it is an arduous process with stringent guidelines that require applying risk management techniques to all of organization's people, processes and IT systems. The standard is divided into 18 sections and covers more than 200 controls. Annual audits and continued improvements are required for re-certification.

Certification takes an average of three years. It is also completely voluntary.

We, however, consider it mandatory. Law firms, government agencies, and organizations place their trust in us every day. Protecting your information assets is essential and doing it at the highest level possible is part of our commitment to always provide the best services possible.

What is ISO 27001?

The International Organization for Standardization (ISO) is an international, non-governmental organization that "brings together experts to share knowledge and develop voluntary, consensus-based, market relevant International Standards that support innovation and provide solutions to global challenges."

The ISO, along with the International Electrotechnical Commission (IEC), jointly publish the ISO/IEC 27000-series of standards, which recommends best practices for information security management.

ISO 27001 is the family's super star. It specifies the requirements for establishing an information security management system (ISMS) that preserves the confidentiality, integrity and availability of information in an organization.

ISO 27001 Certification and ZyLAB ONE

When governmental agencies, law firms, and companies with critical projects see our ISO 27001 certification, they immediately know their data will always be handled appropriately. Certification adds the assurance that we continually meet security goals based on requirements in ISO 27001 including:

- **Confidentiality:** Ensuring only authorized entities can access the system and its data.
- **Integrity:** Protecting against unauthorized alteration of information.
- **Availability:** Providing reliable access to information systems to authorized users.

Certification delivers instant proof that ZyLAB One protects your and your clients' data through top-grade security measures including:

- Using a secure data center hosted in Microsoft Azure Cloud
- Encrypting data at rest and in transit
- Isolating customer data through network security groups
- Using web application firewalls
- Requiring multi-factor authentication
- Performing regular vulnerability scans for viruses and malware
- Ensuring business continuation support and daily backups
- Using permission-based user roles and access to data

You're in Safe Hands

Yes, we're super proud of our ISO 27001 certification. (Go look at it here!) While we know it's quite an accomplishment, it's not our only one. Check out all the security guidelines and principles we adhere to by visiting the ZyLAB Trust Center. And rest assured you're in safe hands with us.