Why ISO27001 Certification is a CTO’s eDiscovery Dream

As the Chief Technology Officer or IT department leader, all the pressures of information security management fall squarely on your shoulders. And those pressures are significant. IBM calculated that a single data breach costs an organization an average of $3.86 million. The accompanying reputation damage can sink a company’s credibility forever.

So, when your company’s leaders turn to you to determine whether a software vendor is trustworthy, much rides on your answer. How can you tell whether a software vendor is truly capable of safeguarding your (and your clients’) critical data?

Knowing that so much is at stake doesn’t make your response any easier to determine. But there is one thing that does: An ISO 27001 certification.

What is ISO 27001 certification?

The International Organization for Standardization (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 best-known standard in the family. It outlines the requirements for an information security management system (ISMS) to manage the security of assets such as financial information, intellectual property, personally identifiable information, and other private and confidential information.

An organization that wants to reassure its customers it adheres ISO 27001 guidelines can get certified by an accredited certification body that meets ISO-defined independent audit criteria. A software vendor who has earned an ISO 27001 certification has invested a significant amount of time and effort into developing an ISMS that effectively manages sensitive information securely.

ISO compliance does not mean ISO certification

Do not be fooled by semantics. Many vendors claim they operate in *compliance* with ISO 27001. But they have not performed the activities necessary nor taken the precautions required to earn a **certification**.

What stops them? An ISO 27001 certification is no trivial matter. An organization must go through an intensive process that requires a great deal of collaborative effort, experience, and expertise to complete and maintain. In fact, it takes the average organization three years to become certified.

Challenges of ISO 27001 Certification Process

Certification is a stringent process in which a company identifies situations that may put data at risk and implements controls to address those risks. ISO 27001 consists of 18 sections and covers more than 200 controls.

Certification requires the adoption of policies for protecting information in areas such as human resources, physical security, software development, operational security, business continuity, access management, asset management, vendor management, and so on. The company must evaluate all their people, processes, and IT systems and systematically apply risk management processes to each.

Among many other requirements, an organization must also establish and maintain:

- A risk register for the continuous management of identified risks
- An internal ISMS steering board or committee
- A thorough and detailed ISMS manual

- A systemized process for regular internal audits

The image below briefly describes a few of the details involved during a potentially 3-year-long certification process:

Why ISO 27001 is Important for eDiscovery

Businesses and law firms use eDiscovery technology to manage massive amounts of data during critical legal and business-oriented processes including litigation, arbitration, responding to subpoenas and regulatory requests, monitoring compliance, preparing virtual data rooms, and so on. Government agencies use eDiscovery for many of the same reasons as well as to help prepare responses to public records requests.

The data involved in these processes almost always contains significant amounts of private and confidential information that, if exposed to the public or obtained by hackers, could cause catastrophic financial and reputational damage, as described above.

Data breaches continue to occur at unprecedented rates every year. According to Experian, significant data breaches—those that affected millions of users—rose from about 200 in 2005 to more than 1,300 in 2017. In the last two months of 2018 alone, we saw major data breaches incurred by Atrium Health (over two million patient records), Marriott (information on 500 million customers) and Quora (100 million users affected).

An ISO 27001 certification establishes that an eDiscovery vendor has taken every possible precaution to prevent data breaches like these and has addressed all potential security risks to ensure your data is constantly protected.

Data & Systems Security with ZyLAB ONE

ZyLAB ONE is an eDiscovery platform used to process confidential data that requires the highest level of protection against security risks. Our customers place their trust in us every day, and ISO 27001 plays a critical role in how we meet our responsibility to manage and protect their information assets.

Our ISMS steering committee has designed controls for ensuring only authorized entities can access the system and its data as well as controls for preventing the unauthorized alteration of information processed in our services. ISO 27001 security requirements are met through a host of measures including:

- Secure data center hosted in Microsoft Azure Cloud
- Data encryption at rest and in transit
- Customer isolation through network security groups
- Application Gateway (Web Application Firewall)
- Multi-factor authentication
- Regular vulnerability scans for viruses and malware
- Business continuation support and daily backups
- Permission-based user roles and access to data

Your Security Matters to Us

When you see that we have an ISO 27001 certification, you can rest assured that your data will remain protected with us. Case closed. You need look no further. But just in case you want to, you can download the white paper ZyLAB One Security and Compliance for more information describing the principles and policies we follow to ensure your data is protected, please.