COALFIRE ISO

INFORMATION SECURITY MANAGEMENT AND PROTECTING DATA IN THE CLOUD

ANAB ACCREDITED MANAGEMENT SYSTEMS CERTIFICATION BODY

COALFIRE ISO

ADVANTAGES OF ISO 27001 CERTIFICATION:

- It is an independent verification that your company's ISMS meets the security standard
- Provides an internationally recognized verification to your organization's commitment to information security
- Is not compliance limited in scope, allowing for an organization-wide approach to information security, if required.

ISO 27001 is a globally recognized standard that provides a risk-based information security management system (ISMS) for all types of information within the organization. It provides a framework for the design, implementation, monitoring and continuous improvement of the ISMS, and certification to the standard demonstrates that the organization has adopted a comprehensive approach to information security within the boundaries of the framework.

Today, CISO, security teams and top Managers are required to accommodate increasingly stringent data laws from differing countries, vet the information security programs of vendors and partners, and better manage the risks of their own proprietary and client data. Obtaining an ISO 27001 certification provides an organization with an independent verification that their information security program meets an international standard, identifies information that may be subject to data laws and provides a risk based approach to managing the information risks to the business. Coalfire ISO has certified a leading Cloud Service provider that needed its multiple sites across three continents to meet ISO 27001 standards. This allowed them the ability to provide their customers with an independent validation that their ISMS meets the ISO 27001 information security standard across all sites.

ISO CERTIFICATION PROCESS

Organizational, security, maturity is a factor in timing for completion of the certification process.

Initial Certification Review

Stage 1 – Review of policies and processes of your ISMS. Confirmation of readiness for Stage 2 Audit.

Initial Certification Review

Stage 2 – In-depth testing to determine if the ISMS is implemented, monitored and maintained per the ISO 27001 standard.

ISO 27001 certification at the conclusion of this stage.

Surveillance Audit

There are 2 succeeding annual audits, for the 3-year ISO 27001 certification period, to confirm the ISMS is still being operated in-line with the initial certification.

Re-Certification

Full ISO 27001 audits will occur prior to the expiry of the 3-year cycle to ensure continuity of the certification.

PROTECTING PERSONALLY IDENTIFIABLE INFORMATION IN THE CLOUD WITH ISO 27018

Organizations that process, store and transmit personally identifiable information (PII) in their cloud on behalf of their customers, will want to strongly consider this add-on to ISO 27001. For many organizations, and consumers, there is still nervousness and suspicion about the security of cloud services, driven by a gap in confidence with regards to information security and Personally Identifiable Information (PII). The issue is significant for cloud services providers as well as their customers both within the US and internationally, as demonstrated by the invalidation of the Safe Harbor agreement, it replaces the EU-U.S. Privacy Shield program (still being finalized) and the EU General Data Protection Regulations. ISO 27018 provides specific controls for data controllers and processors to identify and clarify the Chain of Responsibility for the protection of PII data. An ISO 27018 assessment reviews documentation such as policies and procedures, and conducts interviews to measure conformance to the ISO 27018 standard. There is no formal certification as in ISO 27001, however Coalfire provides third-party validation of this conformance.

In addition, our team uses CoalfireOne℠ to ensure projects are consistently managed and that compliance challenges are identified early so they can be addressed quickly and cost-effectively. CoalfireOne is designed for collaboration to ensure our clients are an integral part of the assessment process.

The ISO 27001 certification process illuminated opportunities for improvement around our access and security of information that we had not previously focused on in other IT related compliance assessments.

CISO FOR A HOSTING COMPANY

DS_ISO27001_050517

TAKE THE COMPLEXITY OUT OF ASSESSING CONTROLS AND RISK.

North America | Europe

Coalfire.com | info@coalfire.com | 877-224-8077

COALFIRE

About Coalfire

As cybersecurity risk management and compliance experts, Coalfire delivers cybersecurity advice, assessments, testing, and implementation support to IT and security departments, executives, and corporate directors of leading enterprises and public sector organizations. By addressing each organization's specific challenges, we're able to develop a long-term strategy that improves our clients' overall cyber risk profiles. Armed with our trusted insights, clients can get to market faster with the security to succeed. Coalfire has offices throughout the United States and Europe. **Coalfire.com**