ISO advisory services

An internationally recognized approach to management systems

Overview of ISO

The International Organization for Standardization (ISO) was founded to facilitate the international coordination and unification of industrial standards and has published more than 22,000 standards addressing almost all aspects of technology and manufacturing.

ISO International Standards ensure that products and services are safe, reliable, consistent, and comprise good quality materials and construction. For businesses, these frameworks are strategic tools that reduce costs by minimizing waste and errors while increasing productivity. They help companies access new markets, level the playing field for developing countries, and facilitate free and fair global trade via common practice benchmarks and expectations.

Overview of our ISO advisory approach

Coalfire helps organizations secure financial, health, sensitive, intellectual, employee, and third-party information; promote quality internally; manage IT service providers and service requirements; and establish robust business continuity procedures. We prepare your organization for formal certification or alignment against internationally recognized standards including, but not limited to:

- ISO management systems
- The Cloud Security Alliance Security Trust and Assurance Registry (CSA STAR) Information System Security Management and Assessment Program (ISMAP)

- Trusted Information Security Assessment Exchange (TISAX)
- French Health Data Standard (Hébergeur de Données de Santé)
- SS-584 Multi-Tier Cloud Security (MTCS)

ISO advisory services

Coalfire's specialists provide expert advice that enables your organization to better understand and prepare for the ISO certification process, while allowing you to stay focused on your business.

Document development and risk management

We meet with your governance, risk, and compliance team to determine management system core documents. As required by ISO standards, we draft work products in response to the mandatory security, quality, or privacy governance requirements. We also augment your organization's internal process owners to establish appropriate policies and procedures that meet security, quality, or privacy control objectives justified for inclusion in your management system, as appropriate. Following the management framework prescribed within ISO 31000, we implement a systemic risk management process for analyzing the business in assessing your security, quality, or privacy objectives (e.g., the confidentiality, integrity, and availability of information; overall sensitivity of data supporting these processes).

Annual internal audit

In accordance with ISO 19011, we execute an independent, periodic internal audit against your program's security, quality, or privacy requirements, as well as the controls justified for inclusion within the management system's boundary. As part of the requirements, we inquire, observe, and/or inspect documentation to support governance and control procedures established by your organization.

Management review

Following completion of the risk assessment and internal audit inputs, we facilitate the resulting review of the management system with senior and operations management personnel who are key internal interested parties to the program's establishment. We develop a recurring, supporting agenda presentation template to meet ongoing requirements for this periodic management review activity.

External audit support

We help you identify and select an accredited certification body registrar that will assess your organization against in-scope certification requirements. Our advisory team educates you on audit processes and expectations to help you prepare for audit engagements.

During the certification audit, we assist with responding to inquiries related to advisory work products made by the appointed lead auditor in interviews and walkthroughs on your organization's behalf. For any identified findings or nonconformities, we assist with root cause analysis and the development of corrective action plans resulting from the external certification audit.

Effectively prepare for ISO certification.

Learn more about Coalfire's ISO advisory services.
Coalfire.com | 877-224-8077

COALFIRE.

About Coalfire

The world's leading organizations – including the top five cloud service providers and leaders in financial services, healthcare, and retail – trust Coalfire to elevate their cyber programs and secure the future of their business. Number one in compliance, FedRAMP®, and cloud penetration testing, Coalfire is the world's largest firm dedicated to cybersecurity services, providing unparalleled technology-enabled professional and managed services. To learn more, visit Coalfire.com.

DS_SOCAdvisory_051723