Audit Catalog

CFECERT

• cfecert.co.uk - sales@cfecert.co.uk •

Index

CFE Certification specializes in information security management, business continuity management, IT service management, artificial intelligence management, GDPR compliance, risk management, quality management, and personal data management systems.

We offer a comprehensive range of services including gap analyses, internal audits, supplier audits, compliance assessments, certification processes, and training.

By adhering to international standards, CFE Certification increases stakeholder confidence, strengthens reputation and contributes to the financial growth of institutions and organisations.

As a proud British **CPD** Educational Certification Service member, most of our training courses are CPD-certified, reflecting our commitment to professional development.

CFE Certification is accredited by globally recognised bodies, including the United Kingdom Accreditation Service (**UKAS**), the International Accreditation Service (**IAS**) and the Turkish Accreditation Agency (**TURKAK**), ensuring the highest levels of credibility and compliance.

CFE | Academy CFE | Audit CFECERT

GAP ANALYSIS

Gap analysis is a strategic method used to identify the differences between an organization's current management system practices and the requirements of the targeted standard. This analysis helps detect deficiencies and areas for improvement, providing the organization with a clear roadmap for building a sustainable and auditable structure.

CFECERT conducts gap analyses within the scope of various management system standards such as ISO/IEC 42001, ISO/IEC 27001, ISO/IEC 27701, ISO 9001, ISO 10002, ISO/IEC 20000-1, ISO 22301, ISO 37001, and GDPR.

Benefits of Gap Analysis for Organizations:

- Identifies risk areas and nonconformities within your processes.
- Enables you to progress toward your goals more efficiently and systematically.
- Helps detect deficiencies at an early stage and supports the establishment of an auditable system.
- Provides time and cost advantages in transitioning to the certification process.

PRE-AUDIT

The pre-audit is an optional assessment process tailored to the specific needs of organizations preparing for a certification audit. Serving as a preparatory step for the upcoming certification audit, this process involves reviewing the structure and operation of your management system.

During this stage, key documentation is examined, interviews are conducted with essential personnel, and the level of compliance of your system with the relevant management system standard is evaluated.

The report generated from the pre-audit helps identify potential nonconformities within your system and gives you time to implement necessary improvements before the official certification audit.

For organizations aiming to begin the certification process on a stronger footing, the pre-audit serves as a valuable preparatory step.

INTERNAL AUDIT

An internal audit is a systematic evaluation process conducted within the organization to assess the conformity and effectiveness of the implemented management system against applicable standards. This process enables the early identification of potential deficiencies and the implementation of necessary improvement actions.

Contact Us Now!

+44 (0) 203 9833 166

training@cfecert.co.uk

For management systems established and operated in accordance with ISO standards, conducting internal audits at regular intervals is a mandatory requirement.

Organizations may carry out internal audits using their own resources, or in situations requiring impartiality and technical expertise, they may seek support from external auditors.

With its experienced team of experts in sector-specific requirements, legal regulations, and relevant standards, CFECERT supports your organization in achieving effective results in the internal audit process and strengthening risk management.

SUPPLIER AUDIT

A supplier audit is the process through which organizations assess their suppliers, dealers, branches, and franchise operations in order to ensure the sustainability of product and service quality. These audits are typically referred to as "second-party audits" and aim to evaluate the compliance of all stakeholders within the supply chain with relevant management system standards.

CFECERT designs and conducts supplier audits based on management system principles, tailored to client-specific needs and industry dynamics. In doing so, it strengthens the reliability of your supply chain, enhances process efficiency, and supports effective quality management.

WHY SHOULD YOU CONDUCT REGULAR SUPPLIER AUDITS?

To maintain sustainable quality, safety, and ethical compliance within your supply chain, conducting regular supplier audits is essential. These audits not only assess current performance but also secure the foundations of long-term business partnerships.

With regular supplier audits, you can:

- Identify and mitigate quality, operational, structural, safety, and ethical risks in advance
- Verify that your supplier's quality management system aligns with your own standards and expectations
- Gain comprehensive insight into procurement and operational policies
- Ensure safe, ethical, and responsible working conditions within your supply chain
- Meet legal, environmental, and ethical obligations
- Protect your corporate reputation and brand image

Contact Us Now!

+44 (0) 203 9833 166

training@cfecert.co.uk

CFECERT performs supplier audits in accordance with international management system standards or your organization's internal policies and criteria. We support both the evaluation of current suppliers and the assessment of potential new partners for future collaboration.

CERTIFICATION AUDIT

A certification audit is conducted to assess an organization's compliance with a specific standard or regulation. This audit process consists of two stages. The duration of the audit is determined based on the size of the organization, the number of locations, and the scope of certification.

STAGE 1 AUDIT

The purpose of the Stage 1 audit is to evaluate whether the organization is ready for the Stage 2 audit. During this stage, the auditor reviews management system documentation and assesses the structural characteristics of the organization.

Key elements reviewed in the Stage 1 audit include:

- Whether objectives and key performance indicators have been defined
- The scope of the management system, processes, operations, equipment used, and control points
- Information related to legal requirements, corrective actions, and improvement activities
- Whether internal audits and management reviews have been planned and implemented

The CFE certification audit team uses the findings from Stage 1 to allocate appropriate resources and prepare a detailed plan for the Stage 2 audit. In addition, any documentation gaps that may result in nonconformities during Stage 2 are identified and reported to the organization.

STAGE 2 AUDIT

At this stage, all documented information is reviewed in detail to verify that the management system complies with the full requirements of the standard.

- Key performance objectives and related records are audited through monitoring, measurement, and evaluation
- The organization's policies, internal audit results, management review records, and management responsibilities are assessed
- Operational control processes and their implementation according to planned arrangements are evaluated

The duration of the Stage 2 audit is calculated in accordance with criteria defined by the International Accreditation Forum (IAF).

Contact Us Now!

+44 (0) 203 9833 166

training@cfecert.co.uk

CERTIFICATION PROCESS

YEAR 1 (Initial Certification)

PRE-AUDIT	AUDIT PLAN
This is optional	Plan for audit has to be mutually agreed

AUDIT STAGE 1 AND 2	INITIAL CERTIFICATION
None-conformites must be closed after audit conclusions	Your certificate will be given after the successful completion of the audit processes.

YEAR 2 (1. Surveillance Audit)

AUDIT PLAN	SURVEILLANCE AUDIT 1
	Within 12 months of the initial certification audit.

YEAR 3 (2. Surveillance Audit)

AUDIT PLAN	SURVEILLANCE AUDIT 2
	At least one audit must be carried out in each calendar year.

ISO/IEC 27001 – INFORMATION SECURITY MANAGEMENT SYSTEM

ISO/IEC 27001 is an international standard that enables organizations to establish an effective Information Security Management System (ISMS). This system aims to manage information security risks systematically, based on the principles of confidentiality, integrity, and availability of information assets.

The ISMS helps organizations identify, analyze, and manage the information security risks they face by applying appropriate risk treatment methods such as prevention, mitigation, transfer, or acceptance. Through this risk-based approach, business continuity is ensured, and information security awareness is strengthened across the organization.

In today's environment, the need for information security is not merely a technical requirement but also a strategic priority for building trust with employees, customers, business partners, and stakeholders. Especially with the increasing relevance of data protection regulations such as KVKK, GDPR, DORA, and NIS 2, ISO/IEC 27001 has become even more critical.

Key Benefits of ISO/IEC 27001:

- Ensures the accuracy, integrity, and confidentiality of corporate information
- Minimizes risks related to information assets
- Supports business continuity
- Enhances information security awareness throughout the organization
- Enables compliance with legal and regulatory requirements
- Prevents unauthorized access to information
- Helps protect corporate reputation
- Builds trust among customers and business partners
- Provides competitive advantage
- Reduces unnecessary workload and time loss

Our Services under ISO/IEC 27001:

- Gap Analysis
- Pre-Audit
- Internal Audit
- Supplier Audit
- Certification Audit

Contact Us Now!

+44 (0) 203 9833 166

training@cfecert.co.uk

ISO/IEC 27017 – SECURITY CONTROLS FOR CLOUD SERVICES

ISO/IEC 27017 is an international standard developed to enhance information security in cloud services. It is based on ISO/IEC 27002 and provides additional, cloud-specific controls to protect information stored and processed in cloud environments.

While ISO/IEC 27018 focuses specifically on the protection of personal data, ISO/IEC 27017 offers broader guidance on general information security controls. It is particularly beneficial for cloud service providers delivering services such as Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS), helping them establish a secure and robust information security infrastructure.

Key Benefits of ISO/IEC 27017:

- Establishes a secure and auditable information security framework for cloud service providers
- Identifies, manages, and reduces information security risks
- Ensures compliance with legal and regulatory requirements
- Builds trust with customers receiving cloud services
- Supports corporate reputation and brand reliability
- Offers competitive advantage and opportunities for growth

Our Services under ISO/IEC 27017:

- Gap Analysis
- Pre-Audit
- Internal Audit
- Supplier Audit
- Certification Audit

ISO/IEC 27018 – PROTECTION OF PERSONAL DATA IN CLOUD

ISO/IEC 27018 is an international standard that defines controls and measures for the protection of personal data processed in cloud environments. Based on the information security controls of ISO/IEC 27002 and structured around the privacy framework of ISO/IEC 29100, the standard specifically focuses on mitigating privacy risks related to personal data processing.

ISO/IEC 27018 is applicable to all organizations providing cloud computing services, including public and private sector entities, government agencies, and non-profit organizations, regardless of size or structure.

Difference from ISO/IEC 27017:
While ISO/IEC 27017 focuses on general information security controls for cloud services, ISO/IEC 27018 is specifically centered on the confidentiality and protection of personal data. It plays a critical role in helping cloud service providers that process personal data comply with regulations such as GDPR, KVKK, DORA, NIS 2, and DPA.

Key Benefits of ISO/IEC 27018:
- Establishes information security and privacy controls in cloud environments where personal data is processed
- Enables legal and regulatory compliance for data-processing cloud service providers
- Helps reduce privacy risks and increase customer trust
- Supports reputation building and provides competitive advantage
- Contributes to business continuity and organizational growth strategies

Our Services under ISO/IEC 27018:
- Gap Analysis
- Pre-Audit
- Internal Audit
- Supplier Audit
- Certification Audit

ISO/IEC 27799 – INFORMATION SECURITY MANAGEMENT IN HEALTHCARE ORGANIZATIONS

ISO/IEC 27799 is an international standard that guides the implementation of information security controls for organizations operating in the healthcare sector—such as hospitals, clinics, laboratories, health technology providers, and insurance companies—to ensure the confidentiality, integrity, and availability of personal health data.

This standard builds upon the general security controls of ISO/IEC 27002 and tailors them to the specific requirements of the healthcare environment, offering a specialized information security management structure for entities that process health-related data.

By focusing specifically on the protection of personal health information, ISO/IEC 27799 supports compliance with data protection regulations such as GDPR and DPA. It provides assurance for both data controllers and data processors within healthcare institutions.

Key Benefits of ISO/IEC 27799:
- Ensures effective implementation of an information security management system specific to the healthcare sector

Contact Us Now!
+44 (0) 203 9833 166
training@cfecert.co.uk

- Secures the confidentiality, integrity, and availability of sensitive health data
- Supports risk assessment processes tailored to healthcare-specific threats and vulnerabilities
- Facilitates compliance with legal and international data protection requirements
- Enhances institutional trust, patient satisfaction, and brand reputation
- Provides a competitive edge through secure data management practices
- Helps reduce risks and prevent security breaches

Our Services under ISO/IEC 27799:

- Gap Analysis
- Pre-Audit
- Internal Audit
- Supplier Audit
- Certification Audit

ISO/IEC 27701 – PRIVACY INFORMATION MANAGEMENT SYSTEM

ISO/IEC 27701 is an international extension standard developed as an addition to ISO/IEC 27001, focusing on the management of personally identifiable information (PII). It provides guidance for both data controllers and data processors in managing data privacy effectively.

The standard supports the implementation of a robust privacy information management system (PIMS) aligned with data protection regulations such as KVKK, GDPR, and DPA. It helps organizations build trust and transparency in their personal data handling practices for both internal and external stakeholders.

Applicable to all types and sizes of organizations—including public institutions, private sector companies, government agencies, and non-profit organizations—ISO/IEC 27701 enables structured and secure privacy governance.

Important note:
ISO/IEC 27701 certification can only be granted to organizations that already hold ISO/IEC 27001 certification. Organizations without ISO/IEC 27001 cannot apply for ISO/IEC 27701 certification independently. Therefore, organizations seeking ISO/IEC 27701 certification must already be certified to ISO/IEC 27001 or apply for both standards simultaneously.

Contact Us Now!

+44 (0) 203 9833 166

training@cfecert.co.uk

Key Benefits of ISO/IEC 27701:

- Builds a privacy management system integrated with ISO/IEC 27001
- Identifies and effectively manages risks related to personal data processing
- Ensures sustainable compliance with national and international privacy regulations
- Enhances transparency and trust among stakeholders
- Clearly defines roles, responsibilities, and obligations
- Strengthens compliance in employment contracts and third-party relationships
- Supports corporate reputation and simplifies security operations

Our Services under ISO/IEC 27701:

- Gap Analysis
- Pre-Audit
- Internal Audit
- Supplier Audit
- Certification Audit

SERVICE ORGANIZATION CONTROLS (SOC) SOC 1 & SOC 2 ASSESSMENTS

SOC (Service Organization Control) is an internationally recognized reporting framework used to evaluate the internal control structure and information security practices of organizations, particularly those offering technology-based services.

SOC 1

A SOC 1 report focuses on the impact of a service provider's controls on the financial reporting processes of its clients. It is suitable for companies that need assurance regarding the effectiveness of internal controls over financial reporting.

SOC 2

A SOC 2 report evaluates a service organization's control environment based on the principles of security, availability, processing integrity, confidentiality, and privacy. It clearly demonstrates how user data is processed and protected.

SOC 2 reports are typically intended for service organization management, clients, regulatory bodies, business partners, and other stakeholders who understand technical controls.

SOC 2 assessments are especially important for SaaS companies, cloud service providers, data processors, and other technology-driven service organizations as a critical indicator of trust.

The validity period of a SOC 2 report is 12 months from the date of issuance and is used to document the organization's ongoing performance in security and compliance.

Contact Us Now!

+44 (0) 203 9833 166

training@cfecert.co.uk

DEFINING THE SCOPE OF A SOC ASSESSMENT

Before initiating a SOC 1 or SOC 2 assessment, it is essential to clearly define the scope. This step is critical in aligning expectations with the client and tailoring an appropriate control framework for the service organization.

Key steps in defining the scope include:

- Collecting detailed information on customer platforms, system architecture, service models, and contractual obligations
- Analyzing service processes to determine which parts of the organization (Trust Service Providers – TSPs) fall within the scope
- Evaluating the required controls according to the relevant trust principles (e.g., confidentiality, integrity, availability) and defining disclosure criteria
- Analyzing the design of controls from technical, operational, and managerial perspectives
- For Type 2 assessments, testing the effectiveness of implemented controls over a defined period to produce a comprehensive assurance report

TYPES OF SOC REPORTS: TYPE I AND TYPE II

SOC Type I:

This report evaluates the design and implementation of a service organization's controls at a specific point in time. It does not provide assurance about the ongoing operational effectiveness or consistency of the controls over time.

SOC Type II:

A Type II report assesses both the design and the operating effectiveness of the controls over a specified period (typically 6 to 12 months). Especially within the SOC 2 framework, it offers in-depth assurance regarding the organization's security, confidentiality, and operational practices.

Organizations that successfully complete a SOC audit demonstrate their commitment to information security, privacy, and processing integrity. For clients in sectors that handle sensitive data, a SOC report serves as evidence of trustworthiness and reliability—offering a competitive advantage and unlocking new business opportunities.

PCI DSS – PAYMENT CARD INDUSTRY DATA SECURITY STANDARD

PCI DSS (Payment Card Industry Data Security Standard) is a globally recognized security standard for the protection of payment card data. It is critically important for financial institutions, e-commerce platforms, and all businesses that process payment information, ensuring the confidentiality, integrity, and security of cardholder data.

CFECERT provides expert audit and compliance services under the PCI DSS framework, supporting organizations in **meeting these high-level** security requirements. Our services contribute to protecting customer data, minimizing risk, and ensuring compliance with regulatory expectations.

Key Benefits of PCI DSS Standard:

- Ensures the confidentiality and integrity of cardholder data
- Supports compliance with legal and regulatory requirements (e.g., BDDK, MASAK)
- Reduces the risk of regulatory penalties and reputational damage in case of data breaches
- Enhances customer trust and strengthens brand value
- Demonstrates a strong commitment to security in competitive markets
- Improves the efficiency and security of payment processes
- Strengthens organizational security practices and internal controls
- Accelerates threat detection and incident response capabilities
- Improves the effectiveness of vulnerability and risk management systems
- Supports secure expansion into new markets and business growth
- Offers advantages in cyber insurance coverage and premium costs
- Facilitates technical and operational alignment with card networks and payment systems

Failing to comply with PCI DSS can result in significant penalties, loss of customers, and severe data breaches. In contrast, investing in PCI DSS compliance is a strategic decision that strengthens long-term resilience against cyber threats.

OUR PCI DSS AUDIT SERVICES:

- **Compliance Assessments:** We conduct comprehensive on-site audits to assess your organization's compliance with PCI DSS requirements, ensuring that all controls are implemented effectively and sustainably.

- **Gap Analysis:** We identify discrepancies between your current security practices and PCI DSS standards and guide you in addressing technical and operational gaps.

- **Vulnerability Scanning:** We perform regular scans at the network, system, and application levels to detect potential vulnerabilities and proactively mitigate risks to cardholder data.

- **Penetration Testing:** We simulate-world threat scenarios to test the resilience of your systems against attacks and evaluate your defense capabilities against data breaches.

Contact Us Now!

+44 (0) 203 9833 166

training@cfecert.co.uk

•**Policy and Procedure Review:** We evaluate your information security policies, procedures, and incident response plans to ensure they align with PCI DSS requirements and effectively protect cardholder information.

• CYBER ESSENTIALS & CYBER ESSENTIALS PLUS

Cyber Essentials is a UK government-backed certification scheme that defines a set of baseline security controls to help organizations protect themselves against the most common cyber threats. The program provides a strong starting point for cybersecurity and assesses whether a business's IT infrastructure meets basic security principles.

Cyber Essentials certification allows organizations to demonstrate their cybersecurity reliability. It is applicable to organizations of all sizes and offers an accessible, cost-effective security solution.

Cyber Essentials Plus is the advanced level of the program. In addition to verifying that baseline controls are in place, it includes technical testing, vulnerability assessments, and simulated cyberattacks carried out by independent cybersecurity experts. This level offers deeper assurance and confirms that an organization maintains a stronger cybersecurity posture.

Key Benefits of Cyber Essentials Certification:

•Strengthens your organization's cybersecurity foundation and provides effective protection against common threats
•Enhances risk management and supports early detection of vulnerabilities
•Builds customer trust and reinforces your organization's reputation
•Offers competitive advantage—particularly helpful in public sector tenders and corporate partnerships
•Supports compliance with legal and regulatory requirements
•Improves response and recovery capabilities against cyber incidents
•Helps reduce cybersecurity insurance premiums
•Increases organizational awareness and encourages internal security improvements
•Easy to implement and affordable as a security solution
•Enables alignment with government and public sector standards and provides advantages in audits

Contact Us Now!

+44 (0) 203 9833 166

training@cfecert.co.uk

ISO/IEC 42001 – ARTIFICIAL INTELLIGENCE MANAGEMENT SYSTEM

ISO/IEC 42001 is the first international standard developed for the governance, security, and risk management of artificial intelligence (AI) systems. As AI technologies become increasingly integral to business processes, managing these systems in an ethical, secure, and sustainable manner has become essential.

CFECERT offers audit and consultancy services to support organizations in aligning with ISO/IEC 42001 requirements and ensuring the safe implementation of AI applications. During the certification process, we assess whether your AI systems are managed in accordance with the principles of transparency, accountability, security, and ethics.

We analyze the current state of your AI systems, identify potential gaps based on ISO/IEC 42001, and provide actionable improvement recommendations. Our audits help you demonstrate compliance with internationally recognized AI security and governance frameworks.

Key Benefits of ISO/IEC 42001:

- Strengthens information security governance within AI systems
- Identifies, mitigates, and sustainably manages AI-related risks
- Enhances stakeholder trust and reinforces corporate reputation
- Supports compliance with regulations and ethical principles
- Contributes to faster and more accurate decision-making processes
- Improves incident response capabilities and accelerates improvement cycles
- Optimizes resource management and operational efficiency
- Enables integration with other management systems (e.g., ISO/IEC 27001)
- Encourages a culture of continuous improvement and transparency
- Provides a scalable and flexible governance framework for AI

ISO/IEC 42001 is a strategic step for organizations of all sizes that use or plan to integrate AI technologies. Adhering to this standard not only offers a competitive edge, but also demonstrates a commitment to ethical and responsible AI deployment.

Our Services under ISO/IEC 42001:

- Gap Analysis
- Pre-Audit
- Internal Audit
- Supplier Audit
- Certification Audit

Contact Us Now!

+44 (0) 203 9833 166

training@cfecert.co.uk

CYBER SECURITY RISK ASSESSMENT

At CFECERT, we offer comprehensive Cybersecurity Audit Services to help organizations systematically analyze cyber threats, reduce risks, and ensure compliance with relevant regulations (e.g., EBA, ISO/IEC 27001). These services not only strengthen your technological infrastructure but also support proactive solutions by identifying security vulnerabilities.

Our Cyber Security Audit Services:

- **Risk Assessment:** We conduct a thorough analysis of your IT infrastructure to identify weaknesses and potential threats, and we assess the integrity and resilience of your security framework.

- **Penetration Testing:** Our expert team performs controlled attack simulations on your systems to uncover vulnerabilities before they can be exploited by malicious actors, enabling timely mitigation.

- **GAP Analysis:** We compare your existing cybersecurity measures with industry standards and best practices to identify areas for improvement and provide actionable recommendations to address deficiencies.

- **Incident Response Evaluation:** We evaluate your organization's preparedness for cyber incidents, analyze your incident response processes, and help you establish a fast, effective, and sustainable response structure.

- **Continuous Monitoring and Compliance:** We provide continuous monitoring to keep your systems under surveillance and implement early warning mechanisms against potential breaches. Additionally, we offer consultancy to ensure ongoing compliance with the EBA Framework and other relevant regulations.

Contact Us Now!

+44 (0) 203 9833 166

training@cfecert.co.uk

ISO 9001 – QUALITY MANAGEMENT SYSTEM

ISO 9001 is the most fundamental and widely adopted international standard for quality management systems. It aims to ensure that organizations consistently deliver products and services that meet customer requirements through effective, consistent, and continuously improving processes.

A Quality Management System (QMS) is a structured framework that defines and manages an organization's quality policies, processes, procedures, roles, and responsibilities. It focuses on meeting both customer expectations and regulatory requirements, while establishing a strong foundation for efficiency, sustainability, and continual improvement.

Implementing a QMS in accordance with ISO 9001 not only increases customer satisfaction, but also enhances an organization's competitiveness and supports its growth objectives.

Key Benefits of ISO 9001:

- Ensures standardization, monitoring, and continuous improvement of business processes
- Helps reduce errors, prevent waste, and lower operational costs
- Clarifies internal responsibilities and supports employee training and development
- Enhances customer satisfaction and builds trust
- Strengthens corporate reputation and supports customer acquisition and sales growth
- Fosters a culture of continuous improvement and long-term sustainability

Our Services under ISO 9001:

- Gap Analysis
- Pre-Audit
- Internal Audit
- Supplier Audit
- Certification Audit

Contact Us Now!

+44 (0) 203 9833 166

training@cfecert.co.uk

ISO 10002 – CUSTOMER SATISFACTION MANAGEMENT SYSTEM

ISO 10002 is an international standard that provides a practical guide for organizations to manage customer complaints related to their products and services effectively. It covers the planning, implementation, maintenance, and continual improvement of processes for receiving, evaluating, responding to, and resolving complaints.

By establishing a systematic complaint management framework, organizations not only improve customer satisfaction but also strengthen brand credibility and foster customer loyalty.

The ISO 10002 standard is flexible and can be applied by organizations of any size, sector, or structure. It enables customer feedback to be used as a strategic opportunity for organizational improvement.

Key Benefits of ISO 10002:

- Enables systematic, timely, and effective handling of customer complaints
- Increases customer satisfaction and enhances customer loyalty
- Improves corporate image and reinforces trust perceptions
- Ensures transparency and traceability in complaint processes
- Helps prevent recurrence of issues and service-related failures
- Creates opportunities for continuous improvement in service quality

Our Services under ISO 10002:

- Gap Analysis
- Pre-Audit
- Internal Audit
- Supplier Audit
- Certification Audit

DIGITAL OPERATIONAL RESILIENCE ACT (DORA)

The Digital Operational Resilience Act (DORA) is a comprehensive European Union regulation designed to ensure that financial institutions are resilient against cyber threats, operational disruptions, and digital risks, and can respond effectively to such incidents.

CFECERT provides expert audit and consultancy services to help organizations comply with DORA's stringent operational resilience requirements.

Our DORA Audit Services:

- **Compliance Assessments:** We assess your organization's digital operational resilience in accordance with DORA guidelines, ensuring that your systems, processes, and control mechanisms align with regulatory expectations.

- **Gap Analysis:** We identify discrepancies between your current practices and DORA requirements, and develop actionable strategies to close these gaps and support your compliance process.

- **Risk Management and Incident Response:** We analyze your risk management approach and incident response protocols to ensure that your organization is prepared for digital disruptions and capable of implementing effective crisis management strategies.

- **Continuous Monitoring and Reporting:** To ensure the sustainability of a DORA-compliant structure, we provide continuous monitoring of your operational resilience and conduct periodic evaluations and reporting, updating your framework as needed.

CFECERT supports financial institutions and digital infrastructure service providers in meeting DORA requirements, enhancing operational resilience, and ensuring the security of their critical systems through audit and training services.

NIS 2 DIRECTIVE – NETWORK AND INFORMATION SYSTEMS SECURITY

The NIS 2 Directive [(EU) 2022/2555] is a new regulation adopted by the European Union on December 14, 2022, aimed at enhancing cybersecurity across critical sectors. This directive significantly expands and strengthens the scope of the original NIS Directive (2016/1148).

As the second iteration of the EU's first binding cybersecurity legislation, NIS 2 seeks to improve the digital resilience of essential and important entities across the EU.

Contact Us Now!

+44 (0) 203 9833 166

training@cfecert.co.uk

MAIN OBJECTIVES OF THE NIS 2 DIRECTIVE

1. Enhancing Cybersecurity in Critical Sectors

- Aims to strengthen the cybersecurity resilience of organizations operating in vital sectors such as energy, transportation, finance, healthcare, digital infrastructure, and public administration.
- Expands its scope to include new sectors such as cloud service providers, data centers, online marketplaces, critical product manufacturers, and public institutions.

2. Strengthening Risk Management and Security Practices

- Requires organizations to establish systematic policies for identifying, assessing, preventing, and responding to cyber risks.
- Demands that incident detection, reporting, and response procedures be clearly defined within institutional structures.
- Promotes the creation of cybersecurity governance frameworks and the clear assignment of responsibilities.

BENEFITS OF NIS 2 FOR ORGANIZATIONS

- **Enhanced Cybersecurity Resilience:** Mandates a strong security culture across critical sectors; improves capabilities for threat prevention, detection, and response.

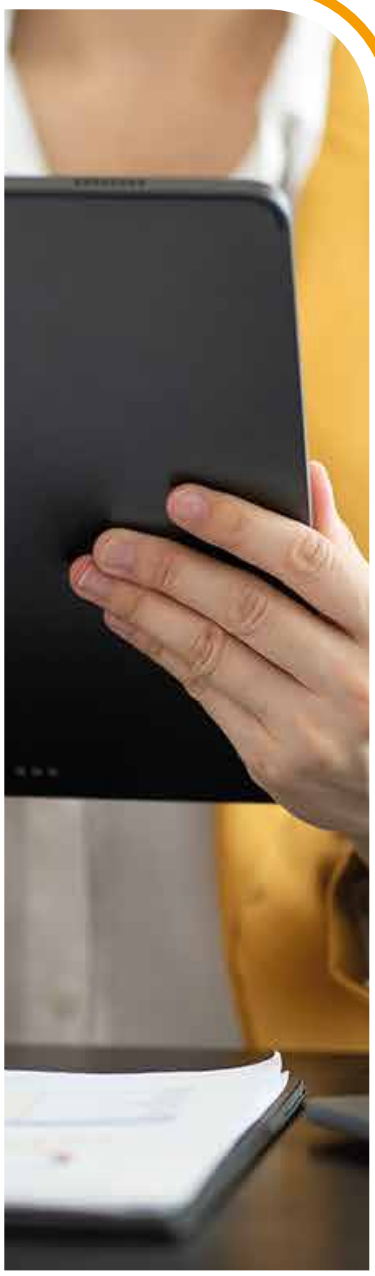
- **Better Protection of Critical Infrastructure:** Reduces the risk of large-scale disruptions in services essential to society and the economy.

- **Increased Trust in Digital Services:** Promotes accountability and transparency, thereby strengthening user confidence in digital services.

ISO 29115 – DIGITAL IDENTITY VERIFICATION MANAGEMENT SYSTEM

ISO/IEC 29115 is an international standard developed to ensure the security of digital identity verification methods and the protection of personal data in digital environments. With the rise of online transactions, financial services, and biometric recognition systems, it provides a robust framework for managing risks in this domain.

The standard defines principles for the classification, management, and verification of digital identity assurance levels. It also helps organizations align with privacy, security, and legal requirements—such as the General Data Protection Regulation (GDPR).



CFECERT offers training and audit services under ISO/IEC 29115 to help organizations align their digital identity verification processes with international best practices. We analyze your current systems, identify gaps with respect to the standard, and guide you in building a secure identity assurance infrastructure.

Key Benefits of ISO/IEC 29115:

- Ensures compliance with public authorities and regulatory requirements
- Enhances institutional reliability and reputation
- Aligns with personal data protection regulations, especially GDPR
- Offers advanced data security and risk mitigation
- Promotes a culture of privacy across the organization
- Streamlines digital identity verification processes and boosts efficiency
- Improves incident management and data breach response capabilities
- Strengthens security in relationships with suppliers and third parties
- Facilitates international data transfer processes
- Supports continuous improvement and auditability
- Increases employee awareness and engagement

Our Services under ISO/IEC 29115:

- Gap Analysis
- Pre-Audit
- Internal Audit
- Supplier Audit
- Certification Audit

EUROPEAN BANKING AUTHORITY (EBA) FRAMEWORK

The European Banking Authority (EBA) provides comprehensive guidelines to help financial institutions and banks across Europe establish strong structures for cybersecurity, IT risk management, and operational resilience.

CFECERT offers tailored audit and consultancy services to support organizations in achieving full compliance with the EBA Framework. Our audit services are designed to help strengthen your digital security infrastructure and ensure alignment with regulatory expectations.

Our Audit Services under the EBA Framework:

- **Compliance Assessments:** We assess your current cybersecurity and IT risk management practices by benchmarking them against EBA's technical evaluation and governance principles.

- **Gap Analysis:** We identify discrepancies between your current structure and EBA standards and develop a roadmap to address gaps efficiently and effectively.

Contact Us Now!

+44 (0) 203 9833 166

training@cfecert.co.uk

- **Risk Management and Penetration Testing:** We conduct in-depth risk assessments and technical penetration tests to identify potential threats and reduce your organization's exposure to cyber risks.

- **Continuous Monitoring and Reporting:** We provide ongoing monitoring of your information systems in line with EBA's periodic audit and reporting requirements, ensuring the sustainability of secure operational structures.

CFECERT delivers reliable and comprehensive audit services to help banks and financial institutions comply with the complex requirements of the EBA Framework and build secure, resilient, and sustainable operational environments.

GDPR – GENERAL DATA PROTECTION REGULATION

The General Data Protection Regulation (GDPR) is one of the European Union's most comprehensive legal frameworks on personal data protection and privacy. It was approved by the European Parliament on June 14, 2016, and came into effect on May 25, 2018.

GDPR is binding not only for organizations operating within the EU, but also for any entity that processes the personal data of EU citizens, regardless of its location.

The regulation's primary aim is to give individuals greater control over their personal data and to ensure that organizations handle such data transparently, securely, and fairly. Under GDPR, organizations are classified as data controllers and/or data processors—each with clearly defined technical and administrative responsibilities.

CFECERT offers tailored audit services—such as gap analysis and supplier audits—to help organizations comply with GDPR. We support your organization in establishing a systematic approach to enhance the sustainability of compliance efforts and prevent potential data breaches.

Benefits Of Gdpr Compliance For Organizations:

- Rebuilds customer trust and strengthens brand reputation
- Ensures consistency in personal data protection practices across the EU
- Simplifies policy management by eliminating the need to comply with separate national regulations
- Saves time and reduces costs by centralizing compliance efforts
- Ensures GDPR compliance across supplier relationships
- Clarifies the responsibilities between data controllers and data processors
- Increases legal and technical awareness within the organization
- Enables sustainable risk management against data breaches

Contact Us Now!

+44 (0) 203 9833 166

training@cfecert.co.uk

Our Gdpr Compliance Services:

- GDPR Gap Analysis
- Supplier Audit

ISO 37001 – ANTI-BRIBERY MANAGEMENT SYSTEM

ISO 37001 is an international management system standard developed to help organizations establish a preventive, systematic, and sustainable framework to address bribery risks. It supports legal compliance while also promoting the development and maintenance of an ethical business culture.

ISO 37001 provides requirements and guidance for establishing, implementing, monitoring, reviewing, and continually improving an anti-bribery management system. It is applicable to organizations of all sizes and sectors, and can be implemented either independently or integrated into existing management systems.

The scope of the standard extends beyond internal organizational processes to include relationships with business partners, suppliers, employees, and other stakeholders.

Key Benefits Of Iso 37001:

- Defines requirements based on international best practices for anti-bribery management
- Demonstrates an organization's commitment to preventing bribery, reassuring management, investors, customers, and employees
- Facilitates compliance with national and international legal frameworks
- Reinforces ethical values, transparency, and accountability
- Increases stakeholder trust and supports corporate reputation
- Provides a competitive advantage in public tenders and international partnerships

Our Services Under Iso 37001:

- Gap Analysis
- Pre-Audit
- Internal Audit
- Supplier Audit
- Certification Audit

Contact Us Now!

+44 (0) 203 9833 166

training@cfecert.co.uk

BS 10012 – PERSONAL INFORMATION MANAGEMENT SYSTEM (PIMS)

BS 10012 is a British standard developed to help organizations effectively manage the collection, processing, storage, and deletion of personal data. It provides a best practice framework for a Personal Information Management System (PIMS) and supports a systematic approach to data protection.

BS 10012 has been updated to align with European data protection legislation, such as the General Data Protection Regulation (GDPR), and is consistent with other information security standards like ISO/IEC 27001. This integration helps reduce duplication of effort and allows for more efficient use of resources.

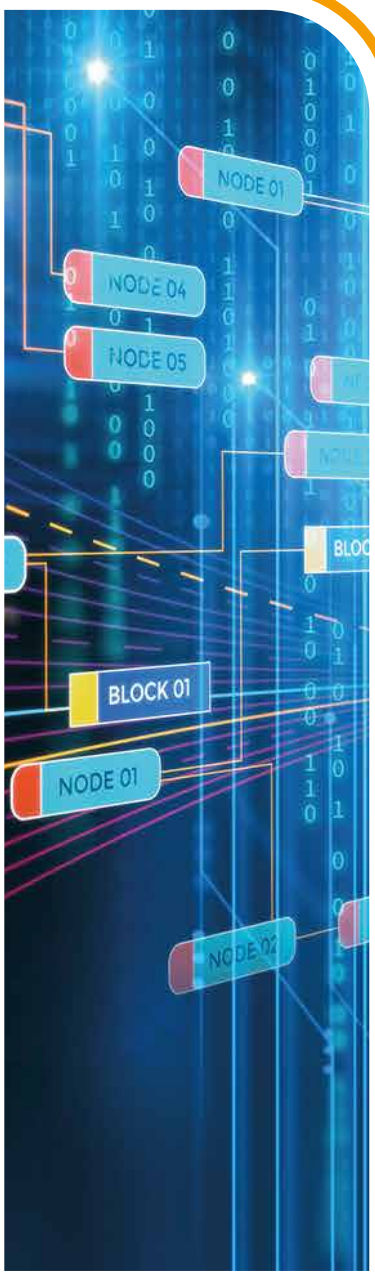
With this standard, organizations can maintain regulatory compliance while offering assurance to stakeholders regarding personal data security. It also helps ensure that data processing activities are transparent, controlled, and auditable.

Key Benefits of BS 10012:

- Ensures the secure processing, storage, and transfer of personal data
- Supports ongoing compliance with GDPR and similar regulations
- Enables integration with other information security systems, such as ISO/IEC 27001
- Promotes a strong culture of data protection and internal awareness
- Reduces the risk of data breaches and enhances incident response capabilities
- Provides assurance to stakeholders that personal data is managed responsibly and transparently
- Enhances operational efficiency and consistency in compliance efforts

Our Services under BS 10012:

- Gap Analysis
- Pre-Audit
- Internal Audit
- Supplier Audit
- Certification Audit



ISO/IEC 20000-1 – IT SERVICE MANAGEMENT SYSTEM

ISO/IEC 20000-1 is an international management system standard that enables the planning, delivery, monitoring, and continual improvement of IT services. It supports organizations in managing service processes more efficiently and reliably, while aiming to enhance customer satisfaction.

Implementing an IT service management system ensures that all service-related processes are evaluated as a whole. This structure allows for measurable service quality, optimized resource usage, and guaranteed service continuity.

The standard is based on globally recognized best practices and supports the alignment of IT services with business objectives.

Key Benefits of ISO/IEC 20000-1:

- Increases the quality, reliability, and continuity of services
- Enhances customer satisfaction while reducing complaints and risks
- Facilitates the monitoring, measurement, and evaluation of service processes
- Promotes more effective use of resources
- Enables auditable cooperation with service providers
- Strengthens organizational reputation and trust in service delivery
- Supports a culture of continual improvement

Our Services under ISO/IEC 20000-1:

- Gap Analysis
- Pre-Audit
- Internal Audit
- Supplier Audit
- Certification Audit

Contact Us Now!

+44 (0) 203 9833 166

training@cfecert.co.uk

ISO 22301 – BUSINESS CONTINUITY MANAGEMENT SYSTEM

ISO 22301 is an international management system standard developed to help organizations maintain continuity of operations in the face of unexpected events, crises, and disasters. It provides a systematic framework for establishing, implementing, monitoring, and continuously improving business continuity plans.

A Business Continuity Management System (BCMS) analyzes the organization's critical processes, resources, and external dependencies to ensure that essential services can continue with minimal disruption during an incident.

For organizations operating in sectors where interruptions are unacceptable—such as public services, transportation, healthcare, and infrastructure—ISO 22301 certification is often not just a choice, but a necessity.

Key Benefits of ISO 22301:

- Enhances organizational resilience against unexpected events
- Minimizes risk by preventing loss of revenue and service interruptions
- Ensures maintenance of customer service levels through continuity planning
- Supports timely and effective decision-making by management
- Improves response and recovery capabilities in the face of disruptions
- Builds competitive advantage and strengthens stakeholder trust
- Facilitates compliance with legal and regulatory requirements (e.g., KVKK, GDPR)
- Establishes an auditable and secure infrastructure supported by internal and external reviews

Our Services under ISO 22301:

- Gap Analysis
- Pre-Audit
- Internal Audit
- Supplier Audit
- Certification Audit

Contact Us Now!

+44 (0) 203 9833 166

training@cfecert.co.uk

ISO 14001 – ENVIRONMENTAL MANAGEMENT SYSTEM

ISO 14001 is an international environmental management system standard that helps organizations systematically manage their environmental impacts. The standard provides a framework for developing environmental policies, identifying environmental risks, reducing environmental impact, and ensuring compliance with legal requirements.

Applicable to organizations of all types and sizes, ISO 14001 promotes the continual improvement of environmental performance and guides those committed to achieving sustainability goals.

Beyond protecting the environment, ISO 14001 also strengthens corporate reputation and provides assurance to stakeholders that environmental responsibilities are being addressed seriously.

Key Benefits of ISO 14001:

- Enhances corporate reputation and credibility
- Enables monitoring, measurement, and control of environmental impacts
- Increases compliance with environmental legislation and regulations
- Improves environmental performance across the supply chain
- Reduces environmental risks and helps protect executives, shareholders, and assets
- May reduce public liability insurance costs
- Facilitates access to environmentally conscious partners and customers

Our Services under ISO 14001:

- Gap Analysis
- Pre-Audit
- Internal Audit
- Supplier Audit
- Certification Audit

Contact Us Now!

+44 (0) 203 9833 166

training@cfecert.co.uk

ISO 45001 – OCCUPATIONAL HEALTH AND SAFETY MANAGEMENT SYSTEM

ISO 45001 is an international management system standard designed to protect employees and visitors from work-related injuries, occupational illnesses, and hazardous conditions. It enables the sustainable management of healthy and safe working environments.

The standard provides a systematic structure for eliminating workplace hazards, reducing occupational health and safety (OHS) risks, raising employee awareness, and improving overall performance. It is applicable to organizations of all sectors and sizes.

By implementing ISO 45001, organizations go beyond legal compliance—enhancing employee engagement, workforce productivity, and corporate reputation.

Key Benefits of ISO 45001:

- Provides a healthy and safe working environment for employees
- Helps prevent workplace accidents and occupational diseases
- Increases awareness and minimizes risky behaviors among employees
- Prevents workforce loss and production downtime, resulting in cost savings
- Enhances production performance by ensuring process safety and continuity
- Supports systematic and sustainable compliance with legal regulations
- Reduces the risk of penalties during audits and inspections
- Contributes to a positive image in terms of corporate social responsibility and employer branding

Our Services under ISO 45001:

- Gap Analysis
- Pre-Audit
- Internal Audit
- Supplier Audit
- Certification Audit

Contact Us Now!

+44 (0) 203 9833 166

training@cfecert.co.uk

ISO 50001 – ENERGY MANAGEMENT SYSTEM

ISO 50001 is an international management system standard developed for organizations seeking to improve energy efficiency, reduce costs, and minimize environmental impact. The standard covers the establishment of energy policies, setting objectives, preparing action plans, and monitoring performance.

With ISO 50001, organizations can systematically manage their energy consumption, implement energy-efficient technologies, eliminate waste, and make their operations more sustainable. The standard is also compatible with energy regulations such as the UK-based Energy Savings Opportunity Scheme (ESOS).

Key Benefits of ISO 50001:

- Enables transparent monitoring and management of energy flows
- Structures continuous energy efficiency monitoring processes
- Allows for evaluation of energy-related procurement and design activities
- Identifies energy-saving opportunities through data analysis
- Reduces energy costs and greenhouse gas emissions
- Increases employee awareness and supports a culture of sustainability
- Ensures compliance with legal and regulatory requirements
- Enhances corporate image and demonstrates environmental responsibility
- Strengthens competitive advantage and may offer tax benefits
- Supports business modernization and accelerates transformation initiatives

Our Services under ISO 50001:

- Gap Analysis
- Pre-Audit
- Internal Audit
- Supplier Audit
- Certification Audit

Contact Us Now!

+44 (0) 203 9833 166

training@cfecert.co.uk

ISO 22000 – FOOD SAFETY MANAGEMENT SYSTEM

ISO 22000 is an international management system standard developed to ensure that organizations across the entire food chain produce safe food. Globally applicable, this standard focuses on systematically ensuring food safety at every stage—from farm to fork.

It provides a scalable framework for all organizations involved directly or indirectly in the food chain, regardless of size or structure. This includes farmers, feed producers, processors, manufacturers, retailers, distributors, transportation and storage services, and hygiene service providers.

The aim of the standard is not only to ensure legal compliance but also to encourage organizations to adopt higher-level food safety management practices. It is designed to be practical even for small businesses.

Key Benefits of ISO 22000:

- Provides a competitive advantage in domestic and international markets
- Enables rapid and effective control of food safety risks
- Reduces production errors and resource waste
- Lowers costs and increases efficiency
- Prevents foodborne illnesses
- Strengthens communication with suppliers, auditors, customers, and all stakeholders
- Ensures systematic compliance with food safety regulations
- Increases reliability in official inspections and reduces the risk of nonconformities

Our Services under ISO 22000:

- Gap Analysis
- Pre-Audit
- Internal Audit
- Supplier Audit
- Certification Audit

Contact Us Now!

+44 (0) 203 9833 166

training@cfecert.co.uk

ISO 28001 – SUPPLY CHAIN SECURITY MANAGEMENT SYSTEMS

ISO 28001 is an international management system standard developed to identify, assess, and control security risks across all stages of the supply chain. It aims to establish a resilient, planned, and secure structure for product delivery, capable of withstanding potential disruptions and breakdowns.

The standard is intended for organizations operating across every link of the supply chain—from production and transportation to warehousing and customs operations. It provides a critical framework for companies that seek to ensure timely, complete, and secure delivery.

ISO 28001 builds upon the requirements of ISO 28000 by elaborating and operationalizing them, offering organizations an effective security management model. It is also aligned with the Authorized Economic Operator (AEO) criteria of the World Customs Organization and supports compliance with national supply chain security programs in many countries.

Key Benefits of ISO 28000:

- Enables systematic identification and mitigation of security vulnerabilities within the supply chain
- Facilitates the establishment of structures that ensure supply continuity during crises
- Supports secure transportation, shipment, and customs operations in international logistics
- Provides customers with a reliable commitment to secure and timely delivery
- Offers a more practical and operational management model based on the ISO 28000 framework
- Eases compliance with international security requirements such as AEO (Authorized Economic Operator)
- Enhances credibility with trade partners, government bodies, and customs authorities

Our Services under ISO 28001:

- Gap Analysis
- Pre-Audit
- Internal Audit
- Supplier Audit
- Certification Audit

Contact Us Now!

+44 (0) 203 9833 166

training@cfecert.co.uk

NOTES

CFECERT CFE | Audit CFE | Academy

CONTACT US NOW

London Office

6 Bevis Marks,
London EC3A 7BA,
United Kingdom

+44 (0) 203 9833 166

Istanbul Office

Parima Plaza, Floor 14, No: 8,
Eski Çırpıcı Yolu Street,
Maltepe Neighborhood, 34010
Zeytinburnu – Istanbul, Turkey

+90 (212) 951 0703

Have a Question?
info@cfecert.co.uk

Looking for Certification Services?
certification@cfecert.co.uk

Explore Our Training Courses
training@cfecert.co.uk

cfecert.com