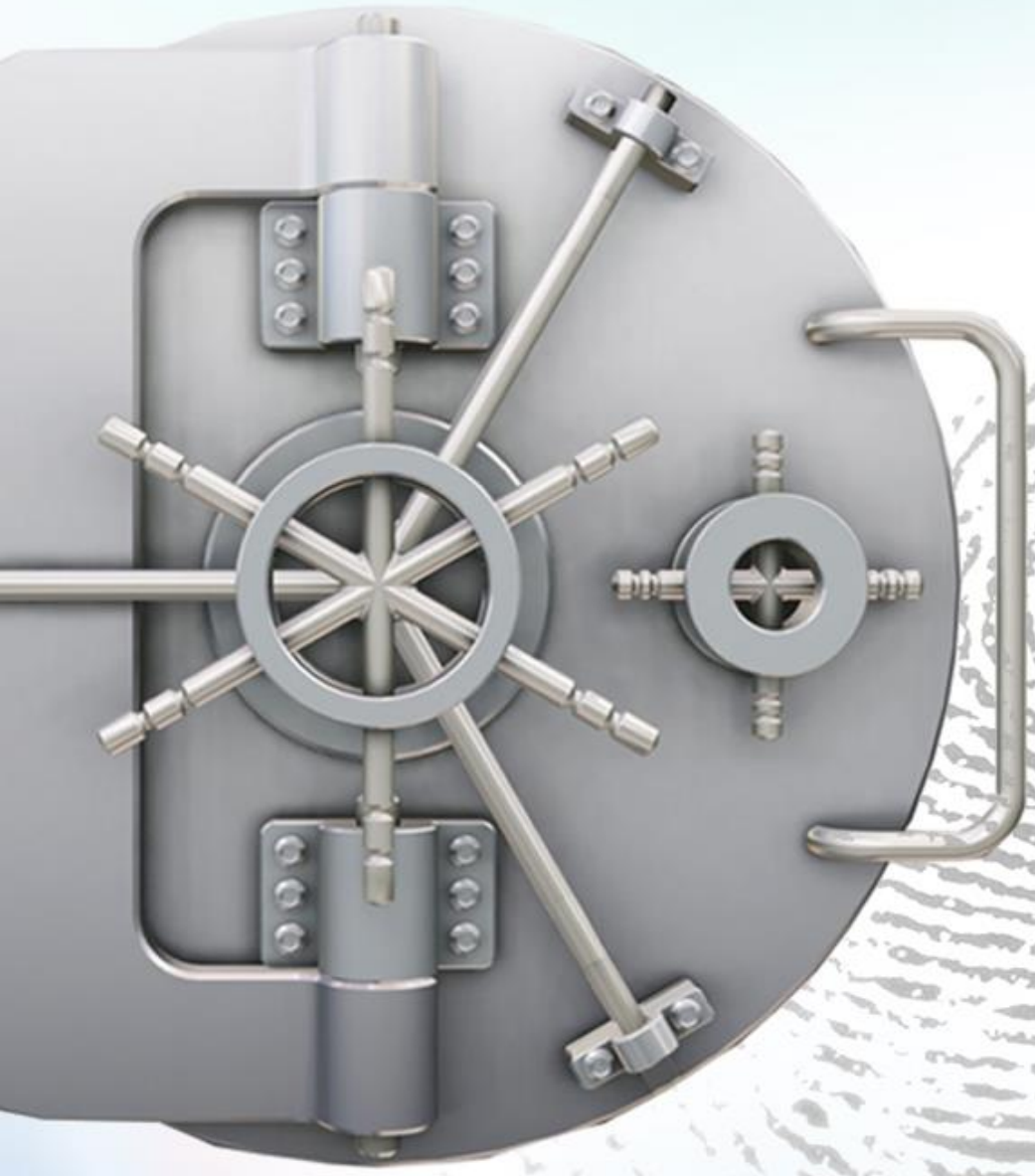
We Do Everything ISO 27001!

ecfirst | Perfecting the Art of Active Cyber Defense

ISO 27001

Training ♦ Consulting ♦ Certification



- Exec Brief
- Services
- 1-Day Workshop
- Policy
- CSCS™
- Testimonials
- About ecfirst

ISO 27001: An Exec Brief

A Global Information Security Standard

The ISO 27000 series is an important global information security framework that can be applied to address multiple regulations and standards and is applicable to organizations of all types, industries and sizes. Your organization may be impacted by regulations such as the Health Insurance Portability and Accountability Act (HIPAA) and possibly other regulations such as the Payment Card Industry's Data Security Standard (PCI DSS) or U.S. State requirements. An important reference and an excellent framework in the world of information security is the ISO 27000 standard.

The ISO 27000 family of information security standards includes:

- ISO 27001 (ISMS – Information Security Management System)
- ISO 27002 (Security Clauses, Categories & Controls)
- ISO 27003 (Guidance in implementing ISMS)
- ISO 27004 (ISMS measurement and metrics; effectiveness of ISMS)
- ISO 27005 (ISRM - Information Security Risk Management)

Why Adopt ISO 27000?

Organizations need to address several compliance mandates, both federal and States. Further, organizations also work with business associates, some may be in the United States, and others may be international firms. The ISO 27000 is the only global enterprise security standard that may be used as a framework for an organization's information security strategy. This increases efficiency and brings about consistency in the implementation of an enterprise security program. It also increases an organization's credibility about its security program.

ISO 27000 is a comprehensive security standard that may be used as a framework to address federal and state mandates. It enables an organization to ensure that its business associates are consistent in their approach to security. The ISO 27000 series provides best practice recommendations on information security management, risks and controls. So if your organization is required to comply with regulations such as the PCI DSS, HITECH Act, HIPAA or other national (federal) or stating requirement then you can seriously consider the ISO 27000 to provide an exceptional framework to address security related regulatory mandates.

The bottom-line is that adopting the ISO 27000 establishes *instant credibility* that the enterprise is basing its security strategy on the *most comprehensive*, global standard. It

ISO 27001: An Exec Brief

delivers efficiency by ensuring all compliance mandates are addressed with one standard. It *enables consistency* as all business associates address the organization's security requirements in the context of one global standard.

Benefits of ISO 27000

- **Compliance**. Selecting a control framework that not only complies with HIPAA and SOC2 but provides extra safeguards clearly demonstrates that gaps identified by the OIG audit are being seriously addressed.
- **Risk mitigation**. Provide the organization with a structured approach to information security management to enable them to secure their information assets. The management system considers risks to the confidentiality, integrity and availability of the data as well as business risks associated with non-compliance and data breaches.
- **Client retention**. Security questionnaires completed fully and appropriately; clients less likely to defect to a competitor that doesn't have the same certification.
- **Reputation**. Demonstrate compliance with an internationally recognized standard and the ability to satisfy customer security requirements. Become known for secure management of confidential and sensitive information.
- **Decreased costs**. Invest now to save later; consider the Information Security Management System to be an insurance policy. Help identify the true cost and ROI of risk mitigation.
- **Business alignment**. A Management System allows the information security initiative to be aligned perfectly with business strategic objectives and places information security as a high, visible priority in strategic thinking and project planning. This includes aligning security practices across all locations and subsidiaries.
- **Improved tools & procedures**. Enhance information security through adoption of best practices and implementation of best in class security products.
- **Marketing edge**. Demonstration of commitment to information security and provide a competitive differentiator when tendering for business and contracts. Demonstrate compliance with an internationally recognized standard and the ability to satisfy (and surpass) customer security requirements.
- **Resource utilization**. The formal procedural structure of a Management System helps optimize human resources, technical resources and financial resources.

ISO 27001: An Exec Brief

A Phased Approach to Adopt ISO 27000

It should be noted that implementing and maintaining ISO 27001 is not a technology project, it is essentially about change management: changing the way staff approach data protection and the culture change that is required to improve the compliance maturity of the company.

The adoption of ISO 27000 as the framework for enterprise security should be a strategic decision for an organization.

Organizations should seriously consider a phased approach to adopt the ISO 27000, global information security standard, as its framework for protecting client and enterprise data.

- **Phase 1** Leadership commitment and communication
- **Phase 2** Planning & Gap Analysis
- **Phase 3** Implement the Management System processes
- **Phase 4** Complete “Statement of Applicability” and implement appropriate controls
- **Phase 5** Stage 1 Audit – compare Management System with ISO 27001 requirements
- **Phase 6** Stage 2 Audit - compare Management system with actual operations and controls
- **Phase 7** Certification Audit

Discuss with ecfirst how we can enable your organization to adopt the ISO 27000 global information security standard.

ISO 27001 Solutions

Organizations are increasingly considering applying the family of ISO 27000 international security standards to comply with various U.S. federal and state regulations such as HIPAA, HITECH, as well as standards such as the PCI DSS. The ISO 27000 series is a global standard that provides a comprehensive framework that organizations can adopt to address compliance requirements and establish a resilient information infrastructure.

ecfirst Brings Deep Experience & Expertise with ISO 27000

ecfirst's fast-paced, one-day private training workshop on the ISO 27000 series, its policy templates, quick reference cards, and deep consulting expertise embodied in its signature methodology, *biz*SHIELD^{tm}, are enabling organizations to easily adopt the ISO standard. The ecfirst *biz*SHIELD^{tm} is a signature methodology is specifically focused on the ISO 27000 series and includes the following core components:

- A fast paced, instructor-led, one-day Getting Started with the ISO 27000 (ISO 27001 and ISO 27002) training delivered at your site.
- A one-day workshop on Getting Started with ISO 27799 that tailors the ISO 27001 Standard for the Healthcare industry
- ISO 27001 Security Policy Templates that can easily be tailored to enable your organization to establish a comprehensive library of policies.
- The healthcare industry's first HIPAA to ISO 27001 Mapping Framework document.
- Managed Compliance Services Program (MCSP) for Information Security Management Systems that enables your organization to leverage deep ecfirst ISO expertise and yet pay a fixed monthly fee for a 36-month period and access a range of services at a fixed price.
- ISO 27000 Webcast – Applying the ISO 27000 Standard to Address Federal and State Regulations.

Certified Security Compliance Specialist ™ (CSCS™)

CSCS™ CERTIFIED SECURITY COMPLIANCE SPECIALIST

A two-day in-depth certification program, that addresses **ISO 27000, ISO 27001, ISO 27002, PCI DSS, HITECH, FISMA** and a lot more.

ISO 27001 Solutions

Our Commitment to You

1. Manage the implementation of ISO 27001 in your environment leveraging whenever possible existing information security processes, practices and capabilities
2. Document all information requested and establish time-line for critical next steps
3. Respond with required information and communicate with all involved parties on activities and status
4. Establish framework for complete knowledge transfer to enable your organization to improve processes and capabilities

ISO 27000 & ISO 27799 Training & Certification

ecfirst has several options for ISO 27000 training - from a tailored 60-minute webcast to a two-day CSCS™ certification program. Schedule our one-day training workshop, *"Getting Started with ISO 27000,"* to learn more about the ISO 27001 and ISO 27002 information security standards and understand how these may be applied to address compliance requirements.

1. Examine the ISO 27000 information security framework and its core components.
2. Review the ISO 27001 security standard and understand key terminology, definitions and the overall organization.
3. Step through the clauses defined in the comprehensive ISO 27002 standard.
4. Understand how compliance requirements of State regulations such as those from Massachusetts and California, as well as federal requirements such as HIPAA and HITECH can be addressed with the ISO 27000 Information Security Management System.
5. Identify critical steps for organizations to get started with the ISO 27000.

Partial Clients List

EY Building a better working world
verizon
SLALOM CONSULTING
Hexaware TECHNOLOGIES
KONICA MINOLTA
CBORD
imprivata
PointClick Cloud Without Compromise

ISO 27001 1-Day Workshop

The ecfirst ISO 27001 Workshop is a one day program that addresses the key aspects of this important global information security standard. This workshop specifically examines the following standards:

- ISO 27000
- ISO 27001
- ISO 27002
- ISO 27799

The ecfirst ISO 27001 Workshop also features case studies and a breakout session to ensure attendees understand critical areas emphasized in this global standard.

Bring this valuable 1-day ISO 27001 workshop to your site today!

Learning Objectives

From this ISO 27001 training program you will:

- Examine the core requirements of the ISO 27001 standard.
- Understand the core elements of an Information Security Management System (ISMS).
- Walk through several sample security policy templates that an organization may use to address regulatory requirements.
- Examine the clauses, categories, and controls defined in the ISO 27002 standard.
- Examine the objective and core requirements of the ISO 27799 standard.

Target Audience

The 1-day ISO 27001 training program is of value to compliance professionals and managers, security officers, security practitioners, privacy officers and senior IT professionals.

On-Site Training

The 1-day ISO 27000 program is delivered worldwide, at the client's site. ecfirst will customize the session to meet your organization's specific requirements and time frames. Call ecfirst at **+1.515.444.1221** today to discuss details about the program.

ISO 27001 1-Day Workshop

Course Outline

Module 1: The ISO 27000 Standard

- Introduction
- Terminology
- Definitions

Module 2: The ISO 27001 Standard

- Introduction
- Definition - ISMS
- Scope
- The PDCA Model
- Framework Organization
  - Definition
  - Requirements

Module 3: The ISO 27002 Standard

- Introduction
- Scope
- Introductory Clause
- Clauses, Categories & Controls
  - Definition
  - Requirements

Case Study I: ISO/IEC 27799 Healthcare Information Security
ISO 27799:2008 defines guidelines to support the interpretation and implementation in health informatics of ISO/IEC 27002 and is a companion to that standard.

Breakout Session: SOA Development
SOA should outline the measures to be taken in order to reduce risks of the clause of the standard. These are based on 'Controls'.

Case Study II: ISO 27001 Certification
Effective communication at all stages is vital to the success of the ISMS and achieving conformance/certification.

ISO 27001 Policy Templates

The ecfirst ISO 27001 policy templates enables organizations to easily and quickly develop customized policies that are based on the ISO 27001 Standard. Your organization also has the option to use the ecfirst On-Demand Consulting program where ecfirst then does all policy customizations as required. ecfirst has considerable experience developing customized policies for its clients.

ISO 27001 Policies	Description
Information Security Policies	
Management Direction for Information Security	Provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.
Policies for Information Security	Ensure a set of policies for information security are defined, approved by management, published, and communicated to employees and relevant external parties.
Review of the Policies for Information Security	Ensure review of the information security policies at regular planned intervals or whenever significant changes occur to the organizational environment.
Organization of Information Security	
Internal Organization	Establish a management framework to initiate and control the implementation and operation of information security within the organization.
Information Security Roles and Responsibilities	Appropriately allocate responsibility for information security at the organization.
Segregation of Duties	Reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.
Contact with Authorities	Maintain appropriate contact with relevant authorities.
Contact with Special Interest Groups	Maintain contact with special interest groups focused on information security.
Information Security in Project Management	Address information security in project management, regardless of the type of project.
Mobile Devices and Teleworking	Ensure the security of teleworking activities and security while using mobile devices.
Mobile Device Policy	Establish precautions to be taken when using mobile computing devices, including wireless devices such as laptops, tablets, smart phones, etc.
Teleworking	Ensure that a policy, operational plans, and procedures are developed and implemented for teleworking activities.

ISO 27001 Policy Templates

ISO 27001 Policies	Description
Human Resource Security	
Prior to Employment	Ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered.
Screening	Ensure that appropriate background checks are carried out for members of the workforce.
Terms and Conditions of Employment	Ensure that all members of the workforce agree to terms and conditions of employment including information security requirements.
During Employment	Ensure that employees and contractors are aware of and fulfill their information security responsibilities.
Management Responsibilities	Ensure that members of the workforce are aware of security threats and concerns, their responsibilities and liabilities, and are equipped to support the organizational security policy.
Information Security Awareness, Education and Training	Ensure that relevant members of the workforce receive appropriate information security education and training.
Disciplinary Process	Establish the disciplinary process for employees that have violated organization security policies or have committed a security breach.
Termination and Change Of Employment	Protect the organization's interests as part of the process of changing or terminating employment.
Termination or Change of Employment Responsibilities	Manage the termination of all members of the workforce in an orderly manner regarding information and information processing facilities.
Asset Management	
Responsibility for Assets	Identify organizational assets and define appropriate protection responsibilities.
Inventory of Assets	Achieve and maintain appropriate protection of organizational assets.
Ownership of Assets	Ensure that all information and assets are owned by a designated part of the organization.
Acceptable Use of Assets	Develop rules for the acceptable use of assets.
Return of Assets	Ensure the return of the organization's assets from all members of the workforce upon termination of employment, contract, or agreement.
Information Classification	Ensure that information receives an appropriate level of protection in accordance with its importance to the organization.
Classification of Information	Appropriately classify the information at the organization.
Labeling of Information	Properly label the classified information.

ISO 27001 Policy Templates

ISO 27001 Policies	Description
Handling of Assets	Develop procedures for handling assets and implement in accordance with the information classification scheme.
Media Handling	Prevent unauthorized disclosure, modification, removal or destruction of information stored on media.
Management of Removable Media	Prevent unauthorized disclosure, modification, removal, or destruction of assets.
Disposal of Media	Ensure the secure and safe disposal of media when it is no longer required and the adherence to documented procedures.
Physical Media Transfer	Establish procedures for the handling and storage of information that protects the information from unauthorized disclosure or misuse.
Access control	
Business Requirements of Access Control	Limit access to information and information processing facilities.
Access Control Policy	Establish, document, and review an access control policy based upon business and security requirements for access.
Access to Networks and Network Services	Ensure that users are only provided with access to the network and network services that they have been specifically authorized to use.
User Access Management	Ensure authorized user access and prevent unauthorized access to systems and services.
User Registration and De-registration	Ensure that the organization follows a formal user registration and de-registration procedure for granting and revoking access to all information systems and services.
User Access Provisioning	Implement a formal user access provisioning process to assign or revoke access rights for all user types to all systems and services.
Management of Privileged Access Rights	Restrict and control the allocation and use of privileges.
Management of Secret Authentication Information of Users	Control allocation of secret authentication information through a formal management process.
Review of User Access Rights	Review user's access rights at regular intervals.
Removal or Adjustment of Access Rights	Ensure access rights to all organization information are removed upon termination of employment, contract, or agreement, or adjusted upon change.
User Responsibilities	Make users accountable for safeguarding their authentication information.

ISO 27001 Policy Templates

ISO 27001 Policies	Description
Use of Secret Authentication Information	Ensure users follow the organization's practices regarding the use of secret authentication information.
System and Application Access Control	Prevent unauthorized access to systems and applications.
Information Access Restriction	Restrict access to information and application system functions by users and support personnel in accordance with the organization's Access Control Policy.
Secure Log-on Procedures	Control access to operating systems by implementing a secure log-on procedure.
Password Management System	Ensure the systems for managing passwords are interactive and provide quality passwords.
Use of Privileged Utility Programs	Restrict and tightly control the use of utility programs that might be capable of overriding system and application controls.
Access Control to Program Source Code	Restrict access to program source code.
Cryptography	
Cryptographic Controls	Ensure proper and effective use of cryptography to protect the confidentiality, authenticity, and/or integrity of information.
Policy on the Use of Cryptographic Controls	Develop and implement a policy on the use of cryptographic controls for protection of the organization's information.
Key Management	Implement key management program to support the organization's use of cryptographic techniques.
Physical and Environmental Security	
Secure areas	Prevent unauthorized physical access, damage, and interference to the organization's information and information processing facilities.
Physical Security Perimeter	Protect the organization's information and information processing facilities through the use of physical security perimeters.
Physical Entry Controls	Utilize appropriate entry controls in secure areas.
Securing Offices, Rooms, and Facilities	Ensure that physical security is included in the design of offices, rooms, and facilities.
Protecting Against External and Environmental Threats	Implement physical protection of the organization's facilities from external and environmental threats, such as natural disasters, malicious attacks, or accidents.

ISO 27001 Policy Templates

ISO 27001 Policies	Description
Working in Secure Areas	Ensure the design and application of physical protection and guidelines for working in secure areas.
Delivery and Loading Areas	Ensure that information processing facilities are isolated from areas of public access and that public access to delivery and loading areas is controlled.
Equipment	Prevent loss, damage, theft or compromise of assets and interruption to the organization's operations.
Equipment Siting and Protection	Ensure that equipment is sited to protect against and reduce risks from environmental threats and hazards, and opportunities for unauthorized access.
Supporting Utilities	Protect the organization from power failures and other disruptions caused by failures in supporting utilities.
Cabling Security	Protect power and telecommunications cabling from interception or damage.
Equipment Maintenance	Maintain organization's equipment so as to ensure its continued availability and integrity.
Removal of Assets	Ensure prior authorization for equipment, information, and software taken offsite.
Security of Equipment and Assets Off-premises	Ensure that the organization applies appropriate security to its equipment when it is used offsite.
Secure Disposal or Re-use of Equipment	Ensure that all items containing any form of storage media have had sensitive data and licensed software removed, securely overwritten, or permanently destroyed.
Unattended User Equipment	Protect unattended equipment appropriately.
Clear Desk and Clear Screen Policy	Protect papers, removable media, and screen viewing from inappropriate or unauthorized access.
Operations Security	
Operational Procedures and Responsibilities	Ensure correct and secure operation of information processing facilities.
Documented Operating Procedures	Ensure that the operating procedures are documented, maintained, and made available to all users who need them.
Change Management	Control and document the changes to information processing facilities and systems.
Capacity Management	Monitor capacity requirements in support of required system performance.

ISO 27001 Policy Templates

ISO 27001 Policies	Description
Separation of Development, Testing, and Operational Environments	Create separate development, test, integration, staging, and production environments to reduce the risk of unauthorized access or changes to production systems.
Protection from Malware	Ensure that information and information processing facilities are protected against malware.
Controls against Malware	Implement detection, prevention, and recovery controls to protect against malicious code, and augment user awareness about these mechanisms.
Backup	Protect against data loss.
Information Backup	Create and regularly test backups of information, software, and system images.
Logging and Monitoring	Record events and generate evidence.
Event Logging	Produce, maintain, and regularly review logs that record user activities, exceptions, faults, and information security events.
Protection of Log Information	Protect logging facilities and log information against tampering and unauthorized access.
Administrator and Operator Logs	Log, protect, and regularly review system administrator and system operator activities.
Clock Synchronization	Ensure that the clocks of all relevant information processing systems at the organization are synchronized to an official or industry best practice source.
Control of Operational Software	Ensure the integrity of operational systems.
Installation of Software on Operational Systems	Implement procedures to control the installation of software on operational systems.
Technical Vulnerability Management	Prevent exploitation of technical vulnerabilities.
Management of Technical Vulnerabilities	Reduce risks resulting from exploitation of published technical vulnerabilities.
Restrictions on Software Installation	Establish and implement rules governing the installation of software by users in the organization.
Information Systems Audit Considerations	Minimize the impact of audit activities on operational systems.
Information Systems Audit Controls	Ensure that audit requirements and activities do not disrupt business processes.

ISO 27001 Policy Templates

ISO 27001 Policies	Description
Communications Security	
Network Security Management	Ensure the protection of information in networks and its supporting information processing facilities.
Network Controls	Manage and control networks to protect information in systems and applications.
Security of Network Services	Identify security mechanisms, service levels, and management requirements of all network services.
Segregation in Networks	Segregate groups of information services, users, and information systems on the organization's networks.
Information Transfer	Maintain the security of information transferred within an organization and with any external entity.
Information Transfer Policies and Procedures	Implement controls and procedures that protect the transfer of information.
Agreements on Information Transfer	Establish agreements for the exchange of information and software between the organization and external parties.
Electronic Messaging	Protect information included in electronic messages.
Confidentiality or Non-disclosure Agreements	Ensure that the requirements for confidentiality or non-disclosure agreements are identified, regularly reviewed, and documented so that they reflect the organization's needs for the protection of information.
System Acquisition, Development, and Maintenance	
Security Requirements of Information Systems	Ensure that information security is an integral part of information systems across the entire lifecycle. This also includes the requirements for information systems which provide services over public networks.
Information Security Requirements Analysis and Specification	Ensure that information security-related requirements are included in the business requirements for new information systems and enhancements to existing information systems.
Securing Application Services on Public Networks	Ensure that the information involved in application services passed over public networks is protected from fraudulent activity, contract dispute, and unauthorized disclosure and modification.
Protecting Application Services Transactions	Ensure that information involved in application service transactions is protected to prevent incomplete transmission, misrouting, unauthorized message alteration, unauthorized disclosure, and unauthorized message duplication or replay.
Security in Development and Support Processes	Ensure that information security is designed and implemented within the development lifecycle of information systems.

ISO 27001 Policy Templates

ISO 27001 Policies	Description
Secure Development Policy	Ensure that the rules for the development of software and systems are established and applied to developments within the organization.
System Change Control Procedures	Develop formal change control procedures to control the implementation of changes.
Technical Review of Applications after Operating Platform Changes	Develop a process whereby business critical applications are reviewed and tested whenever operating systems are changed to ensure there is no adverse impact on the organization's operations or security.
Restrictions on Changes to Software Packages	Ensure that tight controls are in place regarding changes to software packages.
Secure System Engineering Principles	Ensure that the principles for engineering secure systems are established, documented, maintained, and applied to any information system implementation efforts.
Secure Development Environment	Ensure that secure development environments for system development and integration efforts that cover the entire system development lifecycle are established and appropriately protected.
Outsourced Development	Ensure that processes are in place to supervise and monitor outsourced software development.
System Security Testing	Ensure that the testing of security functionality carried out during development.
System Acceptance Testing	Ensure that acceptance testing programs and related criteria are established for new information systems, upgrades and new versions.
Test Data	Ensure that test data is protected.
Protection of Test Data	Ensure that test data is selected carefully, protected, and controlled.
Supplier Relationships	
Information Security in Supplier Relationships	Ensure protection of the organization's assets that is accessible by suppliers.
Information Security Policy for Supplier Relationships	Ensure that information security requirements for mitigating the risks associated with supplier's access to the organization's assets are agreed upon with the supplier and documented.
Addressing Security within Supplier Agreements	Ensure that agreements address all relevant information security requirements with suppliers/third parties who may access, process, store, communicate, or provide IT infrastructure components for the organization.
Information and Communication Technology Supply Chain	Ensure that agreements with suppliers include requirements to address the information security risks associated with information and communications technology services and product supply chain.

ISO 27001 Policy Templates

ISO 27001 Policies	Description
Supplier Service Delivery Management	Maintain an agreed level of information security and service delivery in line with supplier agreements.
Monitoring and Review of Supplier Services	Ensure that supplier service delivery is regularly monitored, reviewed, and audited.
Managing Changes to Supplier Services	Manage changes to the provision of services taking into account the criticality of business systems and processes.
Information Security Incident Management	
Management of Information Security Incidents and Improvements	Ensure that a consistent and effective approach is in place to manage information security incidents, including communication on security events and weaknesses.
Responsibilities and Procedures	Establish management responsibilities and procedures to ensure a quick, effective and orderly response to information security incidents.
Reporting Information Security Events	Report information security events through appropriate management channels as quickly as possible.
Reporting Information Security Weaknesses	Ensure that all members of the organization's workforce are aware of the requirement to note and report any observed or suspected security weaknesses in systems or services.
Assessment of and Decision on Information Security Events	Develop processes that assess and classify information security events.
Response to Information Security Incidents	Document procedures that detail responses to information security incidents.
Learning from Information Security Incidents	Ensure that the information gained from information security incidents is utilized to identify recurring and/or high impact incidents.
Collection of Evidence	Define procedures for the identification, collection, acquisition and preservation of data from information security incidents which can serve as evidence.
Information Security Aspects of Business Continuity Management	
Information Security Continuity	Information security continuity should be embedded in the organization's business continuity management systems.
Planning Information Security Continuity	Ensure that the organization determines its requirements for information security and the continuity of information security management in adverse situations such as a crisis or disaster.
Implementing Information Security Continuity	Establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation.

ISO 27001 Policy Templates

ISO 27001 Policies	Description
Verify, Review, and Evaluate Information Security Continuity	Establish processes to regularly test and update business continuity plans.
Redundancies	Ensure availability of information processing facilities.
Availability of Information Processing Facilities	Ensure that information processing facilities are implemented with redundancy sufficient to meet availability requirements.
Compliance	
Compliance with Legal and Contractual Requirements	Develop processes and implement controls to avoid breaches of legal, statutory, regulatory, or contractual obligations related to information security and related requirements.
Identification of Applicable Legislation and Contractual Requirements	Ensure that all legislative, statutory, regulatory, and contractual requirements related to information systems are identified, documented, and updated.
Intellectual Property Rights	Ensure compliance with all intellectual property rights requirements and the use of proprietary software products.
Protection of Records	Ensure that important organizational records are protected.
Privacy and Protection of Personally Identifiable Information	Safeguard the privacy of personally identifiable information as required by legislative, regulatory, or contractual obligations.
Regulation of Cryptographic Controls	Develop and use cryptographic controls in compliance with all relevant agreements, laws, and regulations.
Information Security Reviews	Ensure that information security is implemented and operated in accordance with existing organizational policies and procedures.
Independent Review of Information Security	Ensure independent review of information security controls at planned intervals or when significant changes occur.
Compliance with Security Policies and Standards	Ensure compliance of information processing systems and procedures with the organization's security policies and standards, and related requirements.
Technical Compliance Review	Ensure that regular reviews are conducted on information systems for compliance with information security and policy standards.

Certification

CSCS™
CERTIFIED SECURITY COMPLIANCE SPECIALIST

Increasingly, businesses are challenged with both securing their digital assets and the information infrastructure as well achieving full compliance with numerous legislations and regulations that impact their industry. Healthcare, financial, government and other verticals are required to constantly monitor the changing dynamics of their infrastructure to mitigate risks and vulnerabilities as well as ensure compliance with international as well as U.S. federal and state legislations and industry best practices. Further, United States federal information systems and those of their business associates must meet specific certification and accreditation security guidelines.

CSCS™ Program Covers Major Information Security Regulations & Standards
The CSCS™ Program is the first and only program in the world that provides a comprehensive treatment of major information security regulations and standards. You can expect to learn and understand core requirements of the following from the CSCS™ program:

- ISO Standards including 27001, 27002, 27799
- PCI DSS
- FISMA
- NIST Standards
- HIPAA and HITECH: U.S. Healthcare Regulations
- U.S. State Regulations on Information Security

The Certified Security Compliance Specialist™ (CSCS™) credential is a job-role based designation. This program is designed to enable professionals to understand, prioritize and ultimately assist organizations achieve compliance with information security-based regulations.

Compliance is big business. Legislation (including guidelines and standards) such as PIPEDA, HIPAA, HITECH and standards such as the ISO 27000 are a requirement for organizations to comply with. A key objective for organizations worldwide is to integrate security best practices and be in compliance. Skilled professionals who understand regulatory compliance requirements and information security are valued across several industries, especially healthcare, financial and the government.

Certification

The Certified Security Compliance Specialist™ (CSCS™) is a unique program of its type in the compliance and security industry - indeed the first of its type in the world. It is laser-beam focused on thoroughly examining compliance requirements and establishing best practices that can be applied in securing today's digital business information infrastructure.

Organizations are quickly moving to a digital ecosystem that is governed by strict regulatory compliance requirements. Validate your compliance security skills and knowledge and distinguish yourself with the credential, Certified Security Compliance Specialist™ (CSCS™).

Distinguish Yourself in the Marketplace – Get the CSCS™ Credential!
Just having a background in Information Technology (IT) or information security is not sufficient anymore for the challenges of business today. Employers are looking for individuals who not only have IT skills but also understand compliance regulations that impact their industry and business – because these are priorities that must be met.

Learning objectives

From this compliance and security training program you will:

- Learn about FISMA, NERC CSS, and the HIPAA Security Rule.
- Step through the core requirements of PCI DSS.
- Analyze the international security standard, ISO's 27001, ISO 27002, ISO 27799 and others.
- Learn about authentication requirements in published guidance documents
- Examine California's SB 1386, SB 541, AB 1950, AB 1298, AB 211 and other U.S. State information security related regulations.
- Understand the security life cycle process for U.S. federal information systems. This is an important requirement for business associates worldwide.
- Review international regulations including PIPEDA, PIP, European Union's DPD and EC Directive, Australia's Privacy Act, and the UK's Data Protection Act, Freedom of Information Act.
- Step through processes for conducting a comprehensive risk analysis and vulnerability assessments.
- Review key contingency compliance requirements for developing the framework for disaster recovery and emergency mode operation plans.

Certification

Prerequisite Requirements

- To be certified as a CSCS™, the candidate must attend the two-day CSCS™ training session delivered by ecfirst or any of its Authorized Partners. For a list of scheduled dates and locations, please visit www.ecfirst.com.
- It is strongly recommended that the candidate pass a major security certification exam such as CISSP, CISA or CISM or have equivalent knowledge and experience.

Target Audience

The complete two-day CSCS™ program is of value to compliance professionals and managers, information security officers, security practitioners, privacy officers and senior IT professionals.

The CSCS™ Exam

The Certified Security Compliance Specialist™ (CSCS™) exam is delivered at the conclusion of the CSCS™ instructor-led 2-day program. The CSCS™ exam validates knowledge and skill sets in information security for the following legislations, standards and frameworks:

Examination Areas	Percentage of Exam
Financial Regulations (e.g. PCI DSS)	20%
Digital Healthcare & Security (e.g. HIPAA, HITECH, ISO 27799)	20%
International Security Standards (e.g. ISO 27000, Other International)	20%
U.S. National and State Standards (e.g. FISMA, State laws)	20%
Business Continuity Planning (e.g. BIA, NIST guidelines)	20%
Total	**100%**

Certification

Exam Name	Exam Number	Number of Questions	Time Allowed	Passing Score
CSCS-1	CSC-101	60	60 Minutes	75%

The first four sections of the CSCS™ exam focus in the area of "security" for regulatory compliance. The last section of the exam emphasizes the "availability" principle that is required by legislations.

CSCS™ exam questions are developed with the intent of measuring and testing practical knowledge and application of general concepts and standards in the area of *regulatory compliance and information security.* All questions are multiple choice and are designed with one BEST answer.

Every CSCS™ exam question has a stem (question) and five options (answer choices). The candidate is asked to choose the correct or best answer from the options. The stem may be in the form of a question or incomplete statement. In some instances, a scenario or description problem may be included. These questions normally include a description of a situation and require the candidate to answer one or more questions based on the information provided.

The candidate is cautioned to READ the question carefully. Many times a CSCS™ exam question will require the candidate to choose the appropriate answer that is MOST LIKELY or BEST. In each instance, the candidate is required to read the question carefully, eliminate known incorrect answers and then make the best choice possible.

All questions should be answered. Grades are based solely on the number of questions answered correctly; so do not leave any questions blank. At the conclusion of each exam, test questions are reviewed. Questions identified as being ambiguous or having technical flaws will either not be used in the grading process or will be given multiple correct answer keys.

Certification

Course Outline

Day One

Module 1: State of Cybersecurity
- Current Cyber Assessment
- Cyber Attack Liefecycle

Module 2: Regulations: Getting Started
- 21 CFR Part 11
- SOX, FTC, SOC2
- PIP & PIPEDA

Module 3: GDPR
- GDPR Impacts
- Fundamental Concepts
- GDPR Facts, Benefits & Requirements
- Right to Erasure
- Preparing for GDPR Enforcement

Module 4: ISO/IEC 27K Series
- ISO 27000 - Information Security Management Systems
- ISO 27001 - Security Domains
- ISO 27002 Standard

Module 5: Healthcare Information Security
- HIPAA Security & HITECH Legislations
- Breach Notification
- Administrative, Physical & Technical Safeguards

Day Two

Module 6: PCI DSS
- Control Objectives
- Defined Requirements
- Critical References

Certification

Module 7: U.S. State Regulations

- 23 NYCRR 500
- California's SB 1386, SB 541, and SB 24
- California's AB 1950, AB 1298, & AB 211
- Massachusetts's 201 CMR 17.00
- Data Breach Challenges
- Encryption Requirements

Module 8: U.S. Federal Regulations

- FISMA
- FIPS
- COOP
- FedRAMP

Module 9: NIST Frameworks and Guidance

- Special Publications
- Phases & Tasks
- COOP
- Key Guidance References

Recognition for Other Security Certifications Earned

This is an excellent program for professionals that have earned credentials such as CISSP, CISM, CISA, Security+, MCSE, and CBCP.

CISSP, CISM, CISA, Security+, MCSE and CBCP certified professionals will find that the CSCS™ program adds significant depth to their knowledge of compliance requirements related to information security. These compliance requirements directly impact the security priorities and initiatives across all types of organizations and business.

CISSPs

As (ISC)² CISSPs participate in this two-day instructor-led program and pass the CSCS™ exam, they are then responsible to document their time at Continuing Professional Education (CPE), for possible eligibility for additional CPEs. The CSCS™ program offers 16 CPEs for CISSPs.

Certification

Exam Fee

The Certified Security Compliance Specialist™ (CSCS™) exam fee is $495.00.

Requirements for Maintaining CSCS™ Certification

CSCS™ must comply with the following requirements to retain certification:

- Comply with the ecfirst Code of Professional Ethics.
- Re-certify once every three (3) years. Information on re-certification exams are announced at www.ecfirst.com. Re-certification exam fee is $395.00.

Revocation of CSCS™ Certification

ecfirst may, at its discretion after due and thorough consideration, revoke an individual's CSCS™ certification for any of the following reasons:

- Violating any provision of the ecfirst.com Code of Professional Ethics
- Falsifying or deliberately failing to provide relevant information
- Intentionally misstating a material fact
- Engaging or assisting others in dishonest, unauthorized or inappropriate behavior at any time in connection with the CSCS™ exam or the certification process

Training Options

The two-day Certified Security Compliance Specialist™ (CSCS™) program is delivered worldwide. Call ecfirst at +1.515.460.3481 today to discuss details about locations and schedules.

CSCS™ program attendees may pursue additional career development with the Certified HIPAA Professional (CHP) program. Mention you have passed the CSCS™ exam and receive 20% off the instructor-led tuition fee for the CHP program.

On Site Training

Bring ecfirst training, certification and executive briefs to your site. ecfirst will customize the session to meet your specific requirements and time frames.

Testimonials

"When GHX began discussing our march toward HIPAA compliance, there was a general consensus about where we had to be - in three years, but there was also a notable lack of agreement on how we might get there. After thoughtful consideration (and amazing good fortune) we chose to seek the services of ecfirst as our "implementation partners" to assist our efforts with HIPAA using ISO 27000 as the framework."

"I'm happy to say, it was the best choice we could have made. Their ISO 27000 experience, comprehensive approach, and practical guidance, have put us solidly on the road to achieving our goal, within our window. For GHX, achieving compliance is huge effort, and having a dependable ally was critical to our success."
Patt Anderson, *Compliance Manager*
GHX

"I really liked the detailed overview of ISO 27001/27002, and the heads up on the upcoming ISO 2700X standards. I liked the note about a written comprehensive InfoSec program being needed."
Jim Brady, *Manager, Data Center Services*
Cedars-Sinai Medical Center

"I attended the ISO 27001/2 webcast. It was excellent."
Sishir Reddy, *CEO*
Episource LLC

"The ISO 27000 brief was very helpful as my organization works to implement ISO 27000 for our security framework. I have been CHP and CHSS™ certified by ecfirst for several years and value ecfirst's expertise. I am interested in the CSCS™ certification and will be looking into ecfirst's training program for this certificate."
Judi Hofman, *CAP, CHP, CHSS*
Privacy/Information Security Officer
Cascade Healthcare Community

"I found the program to give me a wonderful framework with the ISO 27000 to enhance our security program under HIPAA and HITECH. The tools will be very helpful in the continued effort to move our program forward."
Lori A Beeby, *Information Systems Director*
Community Hospital – McCook

ecfirst

Perfecting the Art of Active Cyber Defense

Client Reference

"I just wanted to take a moment and say thank you. Thank you and the ***excellent team*** at ecfirst for ***hard work***, late hours and ***diligence*** during the first round of our HITRUST certification, and now working on our annual risk management and HIPAA compliance assessment."

"From HIPAA compliance, cybersecurity pen tests, to the HITRUST certification engagement, we have found ecfirst to be an ***exceptional partner*** that labored incredibly hard for us, with us. The ecfirst insight and diligence to ensuring HITRUST certification mandates are met led to us completing our engagement on budget and time. We look forward to deeper collaboration with ecfirst in the cybersecurity space in the future. I continue to recommend ecfirst highly and often!"

BRG Berkeley Research Group

Chip Goodman | Vice President of Information Technology

"The ecfirst team literally helped us build our HIPAA practices from ground up since 2012, allowing us to offer secure HIPAA-compliant eHealth and health IT solutions to our customers across the U.S. We are actively taking the logical next step in working with ecfirst to pursue the HITRUST certification in order to further expand our market. We see the partnership with ecfirst as an ***integral part*** of our business strategy and have been ***extremely satisfied*** with the ***quality and value*** of the services that ecfirst has rendered."

BrightOutcome COLLABORATIVE SYMPTOM MANAGEMENT

DerShung Yang | Founder & President

"Provant Health partnered with ecfirst to build a plan and assist in executing it with the goal of achieving HITRUST certification. Ali Pabrai and his team were ***flexible, collaborative*** and most importantly patient as we worked to educate our management team and key employees on the meaning and value of HITRUST. I'd recommend ecfirst to any company who wants to understand HITRUST or work on assessing and remediating their processes and systems in preparation for certification."

provant health life. changing.

Tom Basiliere | Chief Information Officer

Robert Acosta | Bob.Acosta@ecfirst.com | +1.949.793.5700

Perfecting the Art of *Active* Cyber Defense

1000s of Clients | Clients in all 50 States | Clients on 5 Continents

Corporate Office

295 NE Venture Drive

Waukee, IA 50263

United States

Kris Laidley

Inside Sales Support Coordinator

ecfirst/HIPAA Academy

Phone: +1.515.987.4044 ext 25

Email: Kristen.Laidley@ecfirst.com

Robert Acosta

National Sales Director

ecfirst/HIPAA Academy

Phone: +1.949.793.5700

Email: Bob.Acosta@ecfirst.com

www.ecfirst.com