



## ISO 27002: An Overview

### ISO

- ISO stands for the International Organization for Standardization; based in Geneva, Switzerland
- ISO is the world's largest developer of standards - over 17,000 created to date
- Best known standard is ISO 9000 series - standard for quality

### ISO 27000 Series

- A series of 14 standards (several currently in draft) that address IT security (see table)
- ISO 27001 is the 'core' standard and is certifiable - organizations can get 'ISO 27001 certified' (like ISO 9000)
- Over 4,000 organizations worldwide have been certified; for a list of certified organizations refer to <http://www.iso27001certificates.com/>
- Primary source of certifications has been in AsiaPac, with Europe a strong second; adoption in the US has been steadily increasing
- ISO 27001 provides a high-level list of controls that should be implemented to support the defined processes; this list, along with implementation guidance, is detailed in ISO 27002

### Core Security Standards Managed by ISO

Standard	Title
27000	Information security management systems - fundamentals and vocabulary (draft)
27001	Specification for an Information Security Management System (focuses on process)
27002	Code of Practice for Information Security Management
27003	Information security management system implementation guidance (draft)
27004	Information security management measurements (draft)
27005	Information security risk management (draft)
27006	Requirements for bodies providing audit and certification of information security management systems
27007	Guidelines for information security management systems auditing
27011	Information security management guidelines for telecommunications (draft)
27031	Specification for ICT readiness for business continuity (draft, title not yet approved)
27032	Guidelines for cybersecurity (draft)
27033	IT network security (draft)
27034	Guidelines for application security (draft)
27799	Security management in health using ISO/IEC 27002 (draft)

### ISO 27002

- Started out as British Standard 7799 (BS 7799)
- Originally adopted by ISO as 'ISO 17799'; renamed to 'ISO 27002' in August of 2007 (name change only - the rest of the standard was unchanged)
- Provides a framework of recommended security controls for protecting information
- Important definitions from ISO 27002

Term	Definition
Asset	Anything that has value to the organization
Control	Means of managing risk, including policies, procedures, guidelines, practices, or organizational structures, which can be of administrative, technical, management, or legal nature. NOTE: Control is also used as a synonym for safeguard or countermeasure.
Information security event	An identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant
Information security incident	An information security incident is indicated by a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security
Risk	Combination of the probability of an event and its consequence
Risk management	Coordinated activities to direct and control an organization with regard to risk. NOTE: Risk management typically includes risk assessment, risk treatment, risk acceptance, and risk communication
Threat	A potential cause of an unwanted incident, which may result in harm to a system or organization
Vulnerability	A weakness of an asset or group of assets that can be exploited by one or more threats

## ISO 27002

- ISO 27002 consists of Level 1 Clauses (e.g. 4.), Level 2 Categories (e.g. 4.1) and Level 3 Controls (e.g. 4.1.1)
- There are 11 Clauses, including one introductory clause; Clause 4, Risk Assessment and Treatment, is considered introductory since it has no controls defined
- The following table lists all the Clauses along with a brief description of the control areas it covers and the number of Categories (Cats) and Controls (Cons) in the Clause

Clause	Covers	Cats	Cons
4. Risk Assessment and Treatment	How an organization should utilize a risk-management approach to security	2	0
5. Security Policy	How an organization should define, implement, and manage a security policy	1	2
6. Organization of Information Security	Management responsibilities; coordination of activities, roles and responsibilities and interaction with internal and external individuals and parties	2	11
7. Asset Management	How organizations should handle critical assets, including inventorying, classification, ownership	2	5
8. Human Resources Security	Management and employee roles and responsibilities for security in regards to employment	3	9
9. Physical Security	Access to facilities, environmental controls and physical assets	2	13
10. Communications and Ops Management	Operating procedures, change management, outsourcing, backup, network security, media handling, information exchange, eCommerce, monitoring	10	32
11. Access Control	User access control, authentication, network access controls, mobile computing	7	25
12. Information Systems Acquisition, Development, Maintenance	Application controls, IT system acquisition, crypto, development and testing, data leakage, vulnerability management	6	16
13. Information Security	Security incident handling, forensics Incident Management	2	5
14. Business Continuity	Business continuity as a function of security	1	5
15. Compliance	Regulatory and internal compliance, PII	3	10

Note: All ISO standards documents (including the ISO 27000 Series) are copyrighted documents. If you have or purchase a copy you may not distribute it. For ISO 27002 you can quote the Clause, Category and Control titles, but none of the underlying detailed descriptions.

## Benefits of ISO 27002

- ISO 27001 is the only internationally recognized IT security standard that an organization can receive certification for; ISO 27002 provides the control framework for this certification
- ISO 27002 is recognized and adopted worldwide, providing organizations with strong credibility when doing business internationally
- ISO 27002 is the only framework that provides a detailed list of specific controls; most IT security standards (e.g. CoBIT, ITIL) focus primarily on management processes
- Implementing an ISO 27002 framework can allow an organization to cover a wide range of internal and regulatory requirements (e.g. PCI, SOX, HIPAA) with a single centralized set of security controls, reducing the cost and complexity of regulatory compliance
- By eliminating redundant controls with an ISO framework, organizations can significantly reduce their security spending

## Comparing Security Frameworks

- The ISO 27000 Series is one of several possible security standards an organization can adopt. Other common standards include ITIL, CoBIT, COSO and NIST 800-53
- The ISO 27000 Series is generally recognized as the most complete and best recognized worldwide
- Organizations can adopt a different framework standard and still utilize ISO 27002 as a comprehensive controls framework
- The Burton Group published a detailed analysis of all major IT security standards, and found that ISO series, combined with COSO, provides the best choice for most organizations ('Enterprise Security Control Standards: Which Ones and Where They Apply', The Burton Group, Version 2, Oct 01, 2007)

### ITIL - (Information Technology Infrastructure Library)

- A collection of documents that define best practices for a wide range of IT practices (not just security)
- 'Security Management Guide' is the IT security component of ITIL, but is generally not recommended as an IT security standard
- Heavily based on ISO 17799 (now 27002)

### CoBIT - (Control Objectives for Information and related Technology)

- Broadly focused on implementation rather than management and policy domains
- Relies on COSO to provide top-level risk management guidance
- Attempts to address much broader IT activities such as tying IT security to business requirements

### COSO - (The Committee of Sponsoring Organizations of the Treadway Commission)

- A high-level control framework that requires management to look at risk-related issues and implement risk management processes
- Very general; does not define specific processes or controls
- Closely tied to SOX
- Primarily adopted in US

### NIST 800-53 - (US National Institute for Standards and Technology Recommended Security Controls for Federal Information System)

- A detailed list of controls created by the US government to define a control framework for federal agencies
- Not widely accepted outside of US

## Glossary of Terms

The lists of words and definitions contained in this section have been taken directly from the ISO 17799 Glossary of Information Security Terms and Phrases and can be reached at <http://www.17799central.com/a.htm>

### A

**ACCESS CONTROL:** Access control refers to the rules and deployment mechanisms which control access to information systems, and physical access to premises. The entire subject of Information Security is based upon Access Control, without which Information Security cannot, by definition, exist.

**ADMISSIBLE EVIDENCE:** Admissible evidence is evidence that is accepted as legitimate in a court of law. From an Information Security perspective, the types of evidence will often involve the production of a system's log files.

**ANTI-VIRUS SOFTWARE:** Software designed to detect, and potentially eliminate, viruses, as well as repair or quarantine files which have already been infected by virus activity.

**AUDIT LOG:** Computer files containing details of amendments to records, which may be also used in the event of system recovery being required. Enabling this feature usually incurs some system overhead, but it does permit subsequent review of all system activity.

**AUDIT TRAIL:** A record or series of records, which allows the processing carried out by a computer or clerical system to be accurately identified. Often enables verification of the authenticity of amendments, including details of the users who created and authorized them.

**AUDITOR:** The person employed to verify, usually independently, the quality and integrity of the work that has been undertaken within a particular area.

**AUTHENTICATION:** Authentication refers to the verification of the authenticity of either a person or of data. Authentication techniques usually form the basis for all forms of access control to systems or data.

**AVAILABILITY:** Ensuring that information systems and the necessary data are available for use when they are needed.

### B

**BACK DOOR:** A back door is the name given to a 'secret' access route into the system.

**BACKUP:** The process whereby copies of files are taken in order to allow restoration of the original should the need arise.

**BCP:** This is a business continuity planning: the activity to ensure that the essential business functions of an organization are able to continue in the event of an unforeseen event.

**BIOMETRIC CONTROLS:** Security access control systems which authenticate users by means of physical characteristics (eg: fingerprints, voice, and retina).

**BS 7799:** The British Standard for Information Security which was re-issued in 1999 in two parts. Part 1 is the Code of Practice for Information Security Management and Part 2 specifies the information security management system.

**BSI:** The British Standards Institution, publishers of BS 7799 and literally thousands of other standards and supporting documents.

**BUSINESS ASSETS:** As it relates to Information Security this refers to any information upon which the organization places a measurable value.

### C

**CERT:** The Computer Emergency Response Team (CERT) is generally recognized as the internet's official emergency team.

**CERTIFICATION AUTHORITY:** A trusted third-party clearing house that issues digital signatures and digital certificates.

**CIA:** Confidentiality, Integrity and Availability are often considered to be the three basics of information security.

**CIPHER:** A cipher is the generic term used to describe a means of encrypting data or information.

**CLEAR-DESK POLICY:** The policy of an organization which instructs personnel to clear their desks at the end of each day.

**COMPUTER VIRUS:** Computer viruses comprise programming code which is purposely written to inflict an unexpected result upon a third party.

**CONTINGENCY PLANNING:** Contingency planning is the process of planning for the unexpected or perhaps the possibility of circumstances changing.

**COPY PROTECTION:** This term is commonly used to describe techniques used by software developers to help prevent illegal use of products.

**CRACKER:** A cracker is either a person who attempts to gain unauthorized access to a computer system, or a program used to 'crack' some code (to reveal perhaps a password).

**CYBERCRIME:** This is an activity which uses network access to commit a criminal act.

### D

**DATA CLASSIFICATION:** This is the conscious decision to assign a level of sensitivity to data.

**DATA ENCRYPTION:** This is a means of scrambling data so that it can only be read by those holding a key (or password).

**DECRYPTION:** The process by which encrypted data is restored to its original form.

**DENIAL OF SERVICE (DoS):** This is an internet attack against a website which results in, or is intended to result in, the user being denied normal service.

**DES:** This is the Data Encryption Standard: a data encryption standard used for the scrambling of data.

**DIGITAL CERTIFICATE:** This is basically the electronic version of an ID card. It establishes your credentials and authenticates your connection when using the internet or a network.

**DIGITAL SIGNATURE:** This is an electronic equivalent of a person's signature, usually used to validate the authenticity of the sender of a message.

**DMZ:** Short for De-Militarized Zone, this is usually a separate part of an organization's network, deliberately separate from the main corporate network/system in some way.

**DONGLE:** A device, usually physical, which is commonly used by developers to prevent unlicensed use of their software.

## E

**ELECTRONIC EAVESDROPPING:** This is the intentional surveillance of data.

**ENCRYPTION:** The process by which data is scrambled - temporarily re-arranged into an unreadable or unintelligible form for confidentiality, or integrity purposes.

## F

**FIREWALLS:** These are security devices, used to restrict access in network environments, and are often placed between networks (e.g. between the internet and a corporate network) or on a users PC.

## G

**GRASS LINE:** A UK slang term for the telephone hotline operated by the Federation Against Software Theft.

## H

**HACKER:** An individual whose objective is to penetrate the security defenses of a computer system or network.

## I

**IDENTITY HACKING:** The practice of posting on the internet anonymously, or more usually giving completely false personal credentials with intent to deceive.

**IDS: INTRUSION DETECTION SYSTEMS:** These are software applications designed to monitor network activity using a variety of techniques.

**IMPACT ANALYSIS:** The identification of threats to business assets and assessment of what impact such threats could have.

**INCURSION:** The penetration of the system by an unauthorized source.

**INFOWAR:** The use of information and information systems as weapons in a conflict in which the information/systems themselves are the targets.

**ISO:** The International Organization for Standardization is a group of national standards bodies whose aim is to establish, promote, and manage standards.

**INFORMATION SECURITY POLICY:** This is an organizational document, preferably ratified by senior management and distributed throughout an organization, which defines the baseline security requirements of the organization in generic terms.

## K

**KEY DISK:** A copy protection device sometimes supplied with the original software, the idea being that the disk must be present for the software to work.

## L

**LOCKOUT:** A technique used to stop an unauthorized attempt to gain access to a system (e.g. after three attempts to enter a password).

**LOGIC BOMB:** This is a piece of program code buried within another program and designed to perform a malicious act.

**LOGICAL SECURITY:** Software safeguards, such as passwords, access rights, and so on.

## M

**MACRO-VIRUS:** A virus containing a malevolent macro.

**MALICIOUS CODE:** A program or part of a program which is deliberately coded in order to cause an unexpected, undesired event.

**MASQUERADING:** The act of identifying yourself as someone else, perhaps in an email or message board.

**MOCKINGBIRD:** This is a type of Trojan Horse virus program which intercepts communications between users and hosts and provides system-like responses, whilst usually storing the users responses for later (sometimes malicious) use.

## N

**NDA: NON-DISCLOSURE AGREEMENT:** This is a legally binding document which protects the confidentiality of ideas, designs, plans, or other commercial material.

**NETWAR:** An alternative term for Infowar.

**NON-REPUDIATION:** Usually a system which ensures a high degree of certainty that another party is the actual party it claims to be.

## O

**OPERATING SYSTEM HARDENING:** This involves the removal of all non-essential tools, utilities and other systems administration options, on the basis that these could be in support of an attack.

## P

**PAYLOAD:** This is the active or deliverable part of a virus.

**PENETRATION:** Intrusion or unauthorized entry into a system.

**PENETRATION TESTING:** The act of testing or experimenting by attempting to gain unauthorized entry into a system.

**PHYSICAL SECURITY:** The physical protection controls used to safeguard the organization's systems.

**PKI: PUBLIC KEY INFRASTRUCTURE:** This is the use and management of public cryptographic keys.

**PRIVILEGED USER:** A user who by virtue of function has been assigned enhanced powers within the computer system.

**PROTO-HACKER:** A person who has risen above the tinkering level, but does not yet have the necessary skills to crack a major computer system.

## Q

**QUARANTINE:** This is usually the removal of an infected file from its current location, encrypting it,

and locking it in a pre-designated quarantine area from which it cannot be accessed except by the anti-virus program and certain system tools.

## R

**READ-ONLY:** A disk, file, data, document, or ROM chip items which can be viewed, possibly copied, but not changed.

**ROTATION OF DUTIES:** The concept that by rotating staff around the pre-defined jobs any unauthorized activity will be more likely to be detected.

**RSA:** A public-key encryption and authentication algorithm devised by Rivest, Shamir and Adleman.

## S

**SACRIFICIAL HOST:** A server located outside the firewall usually to provide a service that might otherwise compromise the local system's security.

**SAMURAI:** A hacker who hires himself out to other parties with legitimate reasons to need such expertise.

**SECURITY OFFICER:** Usually the person who takes primary responsibility for the security related affairs of the organization.

**SEGREGATION OF DUTIES:** The discrete allocation of tasks among different employees in order to contain the scope for error or fraud.

**SHOULDER SURFING:** Looking over someone's shoulder as they enter their password.

**SLAG:** To run a destructive program that leaves computer systems files, records, and data, utterly useless.

**SMURF:** An attack that exploits features of the IP protocol within the TCP/IP protocol.

**SOCIAL ENGINEERING:** Extraction of information, usually verbally, by impersonating a legitimate third party or by using other social interactions.

**SOFTLIFTING:** The theft (piracy) of software for personal use.

**SPOOFING:** Another term for identity hacking.

**STEALTH BOMB:** Malicious program code that is disguised as something else.

## T

**TECHNO-CRIME:** Criminal activity which uses technology as the subject of the crime itself.

## U

**UPS:** This is a hardware unit which is used to enable uninterruptible power supply.

## V

**VISITOR PASSWORD:** A generic password for visitors, with extremely limited access.

## W

**WHITE-HAT HACKER:** A hacker who performs hacking for legitimate reasons.

## Frequently Asked Questions

---

**Q: Can you clarify the difference between ISO 27001 & ISO 27002**

A: ISO 27001 is a specification for a set of processes that an organization should implement to effectively manage security. It also defines, at a high level, a comprehensive list of controls that should be in place to support these processes. ISO 27002 expands on the high level controls framework defined in ISO 27001 by providing detailed information on all controls, along with implementation guidance.

**Q: Do I have to implement both ISO 27001 & ISO 27002?**

A: No; an organization can leverage the controls framework defined in ISO 27002 to support any kind of security management strategy or system.

**Q: Does an organization need to implement everything covered in ISO 27002?**

A: No; the framework was designed to be as comprehensive as possible. Its expected that an organization will implement only the areas that apply to their specific requirements.

**Q: If an organization wants to get ISO 27001 certified, does it have to do so for the entire organization?**

A: No; an organization can define a limited scope of certification so it can implement it incrementally. For example, an organization can certify one division at a time.

**Q: Does ISO 27001/27002 only apply to specific industries?**

A: No; ISO 27001/27002 were designed to apply to any organization that is concerned about IT security. There are, however, efforts underway to develop industry-specific guidance for implementing ISO security frameworks.

**Q: Does the ISO 27000 Series only provide value to large organizations?**

A: No; utilizing an ISO 27000 framework can benefit any organization concerned about information security. It is especially useful for smaller organizations, since they don't have to 're-invent the wheel' to develop and implement a comprehensive security framework.

**Q: Do I have to go through the effort to get ISO 27001 certified?**

A: No; any organization can leverage the ISO 27002 controls framework without going through the effort of becoming ISO 27001 certified.

**Q: Can ISO 27002 by itself solve an organization's security problems?**

A: No; ISO 27002 defines a comprehensive controls framework that should be implemented in support of a broader security management system or strategy. The ISO 27000 Series recommend that organizations take a risk management approach to IT security; once an organization understands its risks, it can utilize ISO 27001 and 27002 to address those risks.

**Q: Is ISO 27002 mutually exclusive with other IT security standards?**

A: No; ISO 27001/27002 can be utilized to detail process and control implementation guidance in support of a higher-level standard such as COSO.

**Q: At what level of an organization should ISO 27000 Series be implemented?**

A: Most practitioners recommend that the drivers for an ISO 27000 framework need to originate and be supported at the highest levels of an organization. While ISO 27002 can be an effective control framework at any level, it gains its maximum value when implemented from the top down.

**Q: Is EMC/RSA ISO 27001 certified?**

A: Not currently, but we have begun the planning to eventually obtain our certification. We will most likely obtain our certification incrementally, with different groups being certified one at a time, until our entire organization is certified.

**Q: Is ISO 27001 certification a one-time process?**

A: No; an organization must pass a bi-annual audit to remain certified.

### Other Resources

- ISO Home Page - <http://www.iso.org>
- Independent site that discusses and promotes ISO 27000 Series - <http://www.iso27001security.com/>
- How ISO 27000 Works - <http://www.gammasl.co.uk/bs7799/works.html>
- ISO 27000 standards in plain English - <http://www.praxiom.com/index.htm#ISO%2017799%20LIBRARY>
- ISO 27001 certifications worldwide- <http://www.iso27001certificates.com/>



**The Security Division of EMC**