

Compliance Frameworks

This information is reproduced with permission from [The Institute of Internal Auditors](#), and is taken from Section 15 (Appendix D) of the *Global Technology Audit Guide (GTAG): Information Technology Controls*.

[15.1 COSO](#)

[15.2 CICA CoCo](#)

[15.3 CICA IT Control Guidelines](#)

[15.4 ITGI Control Objectives for Information and Related Technology \(CobiT\)](#)

[15.5 ISO 17799 \(Code of Practice for Information Security Management\)](#)

[15.6 ISF Standard of Good Practice for Information Security](#)

[15.7 Generally Accepted Information Security Principles \(GAISP\)](#)

[15.8 AICPA/CICA Trust Services, Principles and, Criteria](#)

[15.9 IIA Systems Assurance and Control \(SAC\)](#)

[15.10 Corporate Governance](#)

[15.11 Other Related Issues](#)

The process of identifying and assessing the IT controls necessary to address specific risks is aided considerably by the organization's adoption of a formal control framework. This framework should apply to, and be used by, the whole organization — not just internal auditing. Although many frameworks exist, no single framework covers every possible business type or technology implementation. The most common frameworks are identified below.

15.1 COSO

Formed in 1985, COSO is an independent private-sector initiative that studied the factors that can lead to fraudulent financial reporting and developed recommendations for public companies and their independent auditors, the SEC and other regulators, and educational institutions. COSO produced the *Internal Control – Integrated Framework*, a widely accepted tool for both management and auditors, in September 2004, and it published *Enterprise Risk Management – Integrated Framework* in fall 2004. Details of both frameworks can be found at the [COSO web site](#).

15.2 CICA CoCo

The Canadian Institute of Chartered Accountants (CICA) produced the *Criteria of Control Framework (CoCo)* in 1992 to address public and institutional concerns that the traditional view of control was no longer effective in preventing corporate failures. The mission of CoCo is to improve organizational performance and decision making through better understanding of control, risk, and governance. Moreover, the framework provides a basis for making judgments about the effectiveness of control.

In 1995, *Guidance on Control* was produced, which describes the CoCo framework and defines control in a way that goes beyond the traditional internal control over financial reporting. The CoCo model is a way of focusing on the future of an organization to ensure it is in control by having a clear sense of shared purpose, collective commitment to achieve that purpose, the resources it needs to do the job, and the ability to learn from experience.

15.3 CICA IT Control Guidelines

The *IT Control Guidelines*, published by the CICA, is a reference source for evaluating IT controls. It is organized in a manner that is easy to use and written in straightforward business language.

15.4 ITGI Control Objectives for Information and Related Technology (CobiT)

Established in 1998, the IT Governance Institute (ITGI) provides guidance on current and future issues related to IT governance, security and assurance. The ITGI's leading guidance publication is *Control Objectives for Information Technology* (CobiT). ITGI's CobiT provides a reference framework and common language across the entire information systems life cycle for IS and business leaders and IS audit, control, and security practitioners. CobiT is one of the most popular and internationally accepted set of guidance materials for IT governance.

15.5 ISO 17799 (Code of Practice for Information Security Management)

ISO/IEC 17799:2000(E), promulgated by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), defines information security principles that ultimately can provide assurance to trading partners and regulators that an organization's information is protected properly. Derived from the British Standards Institution's BS 7799 standard, the Code of Practice for Information Security Management is built around specific security elements required within 10 areas, including physical and environmental security, communication and operational management, and access control. Although as a code of practice, ISO/IEC 17799:2000 provides guidance and recommendations, it is not intended to be a specification, and care should be taken to ensure that claims of compliance are not misleading. The original BS 7799 standard has two parts:

- Part 1 is the Code of Practice and is identical to ISO/IEC 17799:2000.
- Part 2 is a specification for implementing an information security management system (ISMS).

To comply with BS 7799 Part 2 (BS 7799-2:2002) an organization's installed ISMS must conform to the set of requirements described in the standard, which are in the form of *shall* statements. Third-party bodies have been accredited to certify, or register, organizations to BS 7799-2:2002.

15.5.1 What Is Information Security?

BS 7799 treats information as an asset, which like other important business assets, has value to an organization and consequently needs to be protected. Information security protects information from a wide range of threats to ensure business continuity, minimize business damage, and maximize return on investments and business opportunities.

Information can exist in many forms: printed or written on paper, stored electronically, transmitted by post or using electronic means, shown on films, or spoken in conversation. Whatever form the information takes, or means by which it

is shared or stored, BS 7799 indicates that it always should be protected appropriately.

Information security is characterized within BS 7799 as the preservation of:

- Confidentiality – ensuring that information is accessible only to those authorized to have access.
- Integrity – safeguarding the accuracy and completeness of information and processing methods.
- Availability – ensuring that authorized users have access to information and associated assets when

required.

Information security is achieved by implementing a suitable set of controls from BS 7799, which could be policies, practices, procedures, organizational structures, and software functions. These controls should be established to ensure the specific security objectives of the organization are met.

15.5.2 How to Establish Security Requirements

BS 7799 states that it is essential that an organization identify its security requirements. There are three main sources:

- Assessing risks to the organization. BS 7799 does not prescribe a methodology.
- The legal, statutory, regulatory, and contractual requirements that an organization, its trading partners, contractors, and service providers have to satisfy.
- The particular set of principles, objectives, and requirements for information processing that an organization has developed to support its operations.

15.5.3 Assessing Security Risks

BS 7799 suggests that security requirements be identified by a methodical assessment of security risks. Expenditure on controls should be balanced against the business harm likely to result from security failures. The process of assessing risks and selecting controls may need to be performed a number of times to cover different parts of the organization or individual information systems, and it is important to review security risks and implemented controls periodically.

15.5.4 Selecting Controls

Once security requirements have been identified, controls from BS 7799 should be selected and implemented to ensure risks are reduced to an acceptable level. Controls should be selected based on the cost of implementation in relation to the risks being reduced and the potential losses if a security breach occurs. Non-monetary factors, such as loss of reputation, should also be taken into account. For more information on BS 7799, see [BS7799-ISO17799 Security Standards](#).

15.5.5 Topics Addressed in BS 7799

1. Scope.
2. Terms and definitions.
3. Security policy:
 - 3.1. Information security policy document.

- 3.2. Review and evaluation.
- 4. Security organization:
 - 4.1. Information security infrastructure.
 - 4.2. Security of third-party access.
 - 4.3. Outsourcing.
- 5. Asset classification and control:
 - 5.1. Accountability for assets.
 - 5.2. Information classification.
- 6. Personnel security:
 - 6.1. Security in job definition and resourcing.
 - 6.2. User training.
 - 6.3. Responding to security incidents and malfunctions.
- 7. Physical and environmental security:
 - 7.1. Secure areas.
 - 7.2. Equipment security.
 - 7.3. General control.
- 8. Communications and operations management:
 - 8.1. Operational procedures and responsibilities.
 - 8.2. System planning and acceptance.
 - 8.3. Protection against malicious software.
 - 8.4. Housekeeping.
 - 8.5. Network management.
 - 8.6. Media handling and security.
 - 8.7. Exchanges of information and software.
- 9. Access control:
 - 9.1. Business requirement for access control.
 - 9.2. User access management.
 - 9.3. User responsibilities.
 - 9.4. Network access control.
 - 9.5. Operating system access control.
 - 9.6. Application access control.
 - 9.7. Monitoring system access and use.
 - 9.8. Mobile computing and teleworking.
- 10. Systems development and maintenance:
 - 10.1. Security requirements of systems.
 - 10.2. Security in application systems.
 - 10.3. Cryptographic controls.
 - 10.4. Security of system file.
 - 10.5. Security in development and support processes.
- 11. Business continuity management:
 - 11.1. Business continuity management process.
- 12. Compliance:
 - 12.1. Compliance with legal requirements.
 - 12.2. Reviews of security policy and technical compliance.
 - 12.3. System audit considerations.

15.6 ISF Standard of Good Practice for Information Security

The Information Security Forum (ISF) *Standard of Good Practice for Information Security* aims at managing the risks associated with every aspect of information systems, irrespective of an organization's market sector, size, or structure. The standard prepared by ISF's global working groups is a publicly available document split into five key areas: security management, critical business applications,

computer installations, networks, and systems development. For more information and details, see the [ISF web site](#).

15.7 Generally Accepted Information Security Principles (GAISP)

The Generally Accepted Information Security Principles (GAISP) culls best practice from all other similar frameworks. Developed in 1991 as the Generally Accepted System Security Principles, GAISP provides a comprehensive hierarchy of guidance for securing information and supporting technology, including:

- **Pervasive Principles** – board-level guidance.
- **Broad Functional Principles** – designed for executive- level information management (exposure draft distributed September 1999).
- **Detailed Principles** – guidance for operational information security management (under development).

GAISP is now being developed by the [Information Systems Security Association \(ISSA\)](#), which can provide details.

15.7.1 Pervasive Principles

The Pervasive Principles address the confidentiality, integrity, and availability of information. They provide general guidance to establish and maintain the security of information and supporting technology.

- **Accountability Principle** – Information security accountability and responsibility must be defined clearly and acknowledged.

Rationale – Accountability characterizes the ability to audit the actions of all parties and processes that interact with information. Roles and responsibilities should be clearly defined, identified, and authorized at a level commensurate with the sensitivity and criticality of information. The relationship between all parties, processes, and information must be defined clearly, documented, and acknowledged by all parties. All parties must have responsibilities for which they are held accountable.

- **Awareness Principle** – All parties with a need to know — including, but not limited to, information owners and information security practitioners — should have access to available principles, standards, conventions, or mechanisms for securing information and information systems, and should be informed of applicable threats to the security of information.

Rationale – This principle applies between and within organizations. Awareness of information security principles, standards, conventions, and mechanisms enhances and enables controls and can help to mitigate threats. Awareness of threats and their significance also increases user acceptance of controls. Without awareness of the necessity for particular controls, controls, users can pose a risk to information by ignoring, bypassing, or overcoming existing control mechanisms. The awareness principle applies to unauthorized and authorized parties.

- **Ethics Principle** – Information should be used and information security should be administered in an ethical manner.

Rationale – Information systems pervade our societies. Rules and expectations are evolving with regard to the appropriate provision and use of information systems and the security of information. Use of information and information systems should match the expectations established by social norms and obligations.

- **Multidisciplinary Principle** – Principles, standards, conventions, and mechanisms for securing information and information systems should address the considerations and viewpoints of all interested parties.

Rationale – Information security is achieved by the combined efforts of information owners, users, custodians, and information security personnel. Decisions made with due consideration of all relevant viewpoints and technical capabilities can enhance information security and receive better acceptance.

- **Proportionality Principle** – Information security controls should be proportionate to the risks of modification, denial of use, or disclosure of information.

Rationale – Security controls should be commensurate with the value and vulnerability of information assets. Consider the value, sensitivity, and criticality of the information, as well as the probability, frequency, and severity of direct and indirect harm or loss. This principle recognizes the value of approaches to information security ranging from prevention to acceptance.

- **Integration Principle** – Principles, standards, conventions, and mechanisms for the security of information should be coordinated and integrated with each other and with the organization's policies and procedures to create and maintain security throughout an information system.

Rationale – Many information security breaches involve the compromise of more than one safeguard. The most effective control measures are components of an integrated system of controls. Information security is most efficient when planned, managed, and coordinated throughout the organization's system of controls and the life of the information.

- **Timeliness Principle** – All accountable parties should act in a timely, coordinated manner to prevent or respond to breaches of, and threats to, the security of information and information systems.

Rationale – Organizations should be able to coordinate and act swiftly to prevent or mitigate threat events. This principle recognizes the need for the public and private sectors to jointly establish mechanisms and procedures for rapid and effective threat-event reporting and handling. Access to threat-event history could support effective response to threat events and may help prevent future incidents.

- **Assessment Principle** – The risks to information and information systems should be assessed periodically.

Rationale – Information and security requirements vary over time. Organizations periodically should assess the information, its value, and the probability, frequency, and severity of direct and indirect harm or loss. Periodic assessment identifies and

measures the variances from available and established security measures and controls, such as those articulated in the GAISP, as well as the risk associated with such variances. It also enables accountable parties to make informed information risk management decisions about accepting, mitigating, or transferring the identified risks with due consideration of cost effectiveness.

- **Equity Principle** – Management shall respect the rights and dignity of individuals when setting policy and when selecting, implementing, and enforcing security measures.

Rationale – Information security measures implemented by an organization should not infringe upon the obligations, rights, and needs of legitimate users, owners, and others affected by the information when exercised within the legitimate parameters of the mission objectives.

15.8 AICPA/CICA Trust Services, Principles and, Criteria

The American Institute of Certified Public Accountants (AICPA) Assurance Services Executive Committee and the CICA Assurance Services Development Board developed the Trust Services Principles and Criteria to address the risks and opportunities of IT. Trust Services Principles and Criteria set out broad statements of principles and identify specific criteria that should be achieved to meet each principle. The principles are broad statements of objectives. Criteria are benchmarks used to measure and present the subject matter, and against which the practitioner can evaluate the subject matter. In the Trust Services Principles and Criteria, the criteria are supported by a list of illustrative controls. The Trust Services Principles and Criteria are organized into four broad areas:

- **Policies** – The organization has defined and documented its policies relevant to the particular principle.
- **Communications** – The organization has communicated its defined policies to authorized users.
- **Procedures** – The organization uses procedures to achieve its objectives in accordance with its defined policies.
- **Monitoring** – The organization monitors the system and takes action to maintain compliance with its defined policies.

Following are summaries of the Trust Services Security, Availability, Processing Integrity, Privacy, Confidentiality, and Certification Authority Principles and Criteria. The Trust Services Principles and Criteria can be used to deliver branded SysTrust and WebTrust engagements, which are assurance services designed for a wide variety of IT-based systems. Upon attainment of an unqualified assurance report, the organization would be entitled to display a SysTrust or WebTrust Seal and accompanying auditor's report. In addition, the framework can be used to provide advisory and consulting services. For a detailed listing of the Trust Services Principles and Criteria, see <http://www.aicpa.org/trustservices>.

15.8.1 Security Principle – The system is protected against unauthorized access (both physical and logical).

In e-commerce and other systems, the respective parties must ensure that information provided is available only to those individuals who need access to complete the transaction or services or to follow up on questions or issues that may

arise. Information provided through these systems is susceptible to unauthorized access during transmission and while it is stored on the other party's systems. Limiting access to the system components helps prevent potential abuse of the system, theft of resources, misuse of software, and improper access to, or use, alteration, destruction, or disclosure of information. Key elements for protecting system components include permitting authorized access and preventing unauthorized access to those components.

15.8.2 Availability Principle – The system is available for operation and use as committed or agreed.

The availability principle refers to the accessibility to the system, products, or services as advertised or committed by contract or by service-level and other agreements. This principle does not, in itself, set a minimum-acceptable performance level for system availability. Instead, the minimum performance level is established by mutual agreement (contract) between the parties.

Although system availability, functionality, and usability are connected, the availability principle does not address system functionality (the specific functions a system performs) and system usability (the ability of users to apply system functions to specific tasks or problems). It does address system availability, which relates to whether or not the system is accessible for processing, monitoring, and maintenance.

15.8.3 Processing Integrity Principle – System processing is complete, accurate, timely, and authorized.

Processing integrity exists if a system performs its intended function in an unimpaired manner, free from unauthorized or inadvertent manipulation. Completeness generally indicates that all transactions and services are processed or performed without exception, and that transactions and services are not processed more than once. Accuracy includes assurances that key information associated with the submitted transaction will remain accurate throughout the processing of the transaction and that the transaction or services are processed or performed as intended. The timeliness of the provision of services or the delivery of goods is addressed in the context of commitments made for such delivery. Authorization includes assurances that processing is performed in accordance with the required approvals and privileges defined by policies governing system processing.

The risks associated with processing integrity are that the party initiating the transaction will not complete the transaction or provide the service correctly and in accordance with the desired or specified request. Without appropriate processing-integrity controls, the buyer may not receive the goods or services ordered, may receive more than requested, or may receive the wrong goods or services altogether. However, if appropriate processing-integrity controls exist and are operational within the system, the buyer can be reasonably assured of receiving the correct goods and services in the correct quantity and price by the promised date.

Processing integrity addresses all of the system components including procedures to initiate, record, process, and report the information, product, or service that is the subject of the engagement. The nature of data input in e-commerce systems typically involves the user entering data directly over Web-enabled input screens or forms, whereas in other systems, the nature of data input can vary significantly. Because of this difference in data-input processes, the nature of controls over the completeness and accuracy of data input in e-commerce systems may be somewhat different than for other systems.

Processing integrity differs from data integrity because it does not imply automatically that the information stored by the system is complete, accurate, current, and authorized. If a system processes information from sources outside of the system's boundaries, an organization can establish only limited controls over the completeness, accuracy, authorization, and timeliness of the information submitted for processing. Errors that may have been introduced into the information and control procedures at external sites typically are beyond the organization's control. When the information source is excluded explicitly from the description of the system that defines the engagement, it is important to detail that exclusion in the system description. In other situations, the data source may be an inherent part of the system being examined, and controls over the completeness, accuracy, authorization, and timeliness of information submitted for processing would be included in the scope of the system as described.

15.8.4 Privacy Principle and Components – Personal information is collected, used, retained, and disclosed in conformity with the commitments in the organization's privacy notice and with the AICPA/CICA Trust Services Privacy Criteria.

The Privacy Principle contains 10 components⁶ and related criteria that are essential to the proper protection and management of personal information. These privacy components and criteria are based on fair information practices included in privacy laws and regulations of various jurisdictions around the world and many recognized good privacy practices. The privacy components are:

- **Management** – The organization defines, documents, communicates, and assigns accountability for its privacy policies and procedures.
- **Notice** – The organization provides notice about its privacy policies and procedures and identifies the purposes for which personal information is collected, used, retained, and disclosed.
- **Choice and consent** – The organization describes the choices available to the individual and obtains implicit or explicit consent with respect to the collection, use, and disclosure of personal information.
- **Collection** – The organization collects personal information only for the purposes identified in the notice.
- **Use and retention** – The organization limits the use of personal information to the purposes identified in the notice and for which the individual has provided implicit or explicit consent. The organization retains personal information only as long as necessary to fulfill the stated purposes.
- **Access** – The organization provides individuals with access to their personal information for review and update.
- **Disclosure to third parties** – The organization discloses personal information to third parties only for the purposes identified in the notice and with the implicit or explicit consent of the individual.
- **Security** – The organization protects personal information against unauthorized access, both physical and logical.
- **Quality** – The organization maintains accurate, complete, and relevant personal information for the purposes identified in the notice.
- **Monitoring and enforcement** – The organization monitors compliance with its privacy policies and procedures and has processes to address privacy-related complaints and disputes.

15.8.5 Confidentiality Principle – Information designated as “confidential” is protected as committed or agreed.

The confidentiality principle focuses on information designated “confidential.” There is no widely recognized definition of *confidential information*, unlike personally identifiable information, which many countries currently are defining through regulation. In the course of communicating and transacting business, partners often exchange information they require to be maintained on a confidential basis. In most instances, the respective parties wish to ensure that the information they provide is available only to those individuals who need access to complete the transaction or resolve any questions that arise. To enhance business partner confidence, it is important to inform the partner about the organization’s confidentiality practices, including those for providing authorized access to, use of, and sharing of information designated as confidential.

Information that may be subject to confidentiality includes:

- Transaction details.
- Engineering drawings.
- Business plans.
- Banking information about businesses.
- Inventory availability.
- Bid or ask prices.
- Price lists.
- Legal documents.
- Client and customer lists.
- Revenue by client and industry.

Unlike personal information, there are no defined rights for accessing confidential information to ensure its accuracy and completeness. Interpretations of what is considered confidential information can vary significantly from business to business and are driven by contractual arrangements in most cases. As a result, those engaged in business relationships need to understand what information will be maintained on a confidential basis and what, if any, rights of access or other expectations an organization might have for updating that information to ensure its accuracy and completeness.

Information that is provided to another party is susceptible to unauthorized access during transmission and while it is stored on the other party’s computer systems. For example, an unauthorized party may intercept business partner profile information and transaction and settlement instructions while they are being transmitted. Controls such as encryption can be used to protect the confidentiality of this information during transmission, while firewalls and rigorous access controls can help protect the information while it is stored on computer systems.

15.8.6 Certification Authority (CA) Principle

The certification authority discloses its key and certificate life cycle-management business and information privacy practices and provides its services in accordance with these practices. This includes the concepts of CA business-practice disclosures, service integrity, and environmental controls.

15.9 IIA Systems Assurance and Control (SAC)

The IIA provides the SAC model The SAC model sets the stage for effective

technology risk management by giving companies a framework to guide an evaluation of the e-business control environment. SAC recognizes the importance of governance — both within an organization and between business partners — to ensure effective security, auditability, and control of information. SAC provides current information to understand, monitor, assess, and mitigate technology risks. SAC examines risks in all business system components, including customers, competitors, regulators, and partners. Full details of the model can be found at <http://www.theiia.org/eSAC/index.cfm>, with a detailed discussion of the model at <http://www.theiia.org/ITAudit/index.cfm?act=itaudit.archive&fid=411>.

15.10 Corporate Governance

15.10.1 OECD Principles of Corporate Governance

The [OECD Principles of Corporate Governance](#), amended in April 2004, set out a framework for good practice that has been agreed to by all 30 OECD member countries and has become a generally accepted standard. Originally issued in 1999, the principles are designed to assist governments and regulatory bodies in drawing up and enforcing effective rules, regulations, and codes of corporate governance. In parallel, they provide guidance for stock exchanges, investors, companies, and others that have a role in the process of developing good corporate governance. Although the OECD principles do not provide specific guidance on IT controls, other OECD units provide further guidance and research on information security and privacy.

15.10.2 EU Commission

The European Commission's Action Plan on [Company Law and Corporate Governance](#) was released in May 2003 to strengthen corporate governance mechanisms in public interest entities. The EU's Corporate Governance initiatives do not address IT issues specifically, but activities of the [Information Society directorate](#) address many specific IT control issues.

15.10.3 United Kingdom's Combined Code and Turnbull Guidance

The Combined Code and Turnbull guidance were the United Kingdom's approach to corporate governance. Like Sarbanes-Oxley, they are not specific on the issue of IT controls, but are focused on the whole internal control framework. More details can be found from [IIA-UK and Ireland](#).

15.10.4 King Report on Corporate Governance for South Africa 2002 (King II)

Similar to the Combined Code and the Turnbull guidance, this code of practice is intended for organizations in South Africa. Copies of the reports can be [accessed online](#).

15.10.5 Other Corporate Governance Requirements

Many other countries have similar corporate governance requirements. A comprehensive list and copies of these can be found at the [European corporate governance institute web site](#).

15.11 Other Related Issues

15.11.1 IT Infrastructure Library (ITIL)

The IT Infrastructure Library (ITIL) is a generic approach to IT service management, providing a set of best practices, drawn from public and private sectors

internationally. Originating in the United Kingdom, it is supported by a qualification scheme, accredited training organizations, and implementation and assessment tools. The best-practice processes promoted in ITIL support and are supported by the British Standards Institution's Standard for IT Service Management (BS 15000). While ITIL does not claim specifically to be a framework for IT control, its use needs to be recognized and taken into account when determining which control framework to apply. Further information can be obtained from [ITIL](#).

15.11.2 ISO 9000:2000

While ISO 9000 relates specifically to the requirements of quality management, it does contain elements that contribute to IT control in respect to the control and documentation of processes. Although it does not constitute a complete IT control framework, ISO 9000 can provide elements that contribute to the strength of IT controls for implementing strong processes. More information on the standard can be obtained from [ISO](#).

15.11.3 National Quality Institute (NQI) Canadian Framework for Business Excellence

The Canadian Quality Criteria/Framework for Business Excellence, developed by the National Quality Institute (NQI), is a framework for improvement. Based on the Quality Principles, the original private-sector criteria has been adapted for the public sector, as well. In addition, they form the evaluation basis for the Manitoba Quality Awards and Canada Awards for Excellence programs and are used by Canadian organizations of all sizes and in all sectors. More information can be obtained from [Qnet](#).

15.11.4 Carnegie Mellon University Software Engineering Institute (CMU/SEI) OCTAVE

[Operationally Critical Threat, Asset, and Vulnerability Evaluation \(OCTAVE\)](#) is a self-directed, risk-based, strategic assessment and planning technique for organizations that want to understand their information security needs. A small team of people from an organization's operational, or business, units and the IT department work together to address the security needs of the enterprise. This team draws on the knowledge of many employees to define the current state of security, identify risks to critical assets, and set a security strategy. OCTAVE focuses on organizational risk and strategic, practice-related issues, balancing operational risk, security practices, and technology. Separate methods are available for large and small organizations.