ISO 27001

Information Security Management System Standard

AN EXECUTIVE OVERVIEW

PERRY JOHNSON
CONSULTING, INC.

www.pjcinc.com • 1-888-248-0256

ISO 27001:2022

Information Security Management System Standard

AN EXECUTIVE OVERVIEW

Revised 02/23

PERRY JOHNSON CONSULTING, INC.

Detroit

200 East Big Beaver Rd. ÅTroy, Michigan 48083
1-888-248-0256 or (248) 519-2602

Website: www.pjcinc.com Å**Email:** pjc@pjcinc.com

ISO 27001:2022

An Executive Overview

Table of Contents

FOREWORD

ISO 27001 was first published in 2005 and was essentially an ISO issuance of BS7799-2 (more on the origin of this document later). When it was updated in 2013 it had the distinction of being the first ISO published standard to utilize the 10 section structure and core text provided in Annex SL. This alignment with Annex SL was maintained when ISO 27001 was updated in 2022. This means that ISO 27001:2022 can be easily added to a portfolio of certification that could possible include ISO 9001:2015 and ISO 14001:2015.

The new standard has achieved numerous ideals by this latest rewrite, including:

- Simplification of language;
- Consistency with other standards; and
- A flexible approach to the management of processes.

This guide was written to provide information about the ISO 27001:2022 standard, and its applications. Step by step, it outlines the general requirements of ISO 27001:2022, which can be applied to any type of industry or company that has electronic information that must be kept secure. In some cases, these requirements can also be applied to non-electronic information requiring secure storage as well.

Registration to ISO 27001:2022 offers a major competitive edge for organizations that handle electronic data and is emerging as a mandatory requirement in some marketplaces such as defense and healthcare. Far-sighted firms are planning for registration by conducting a thorough investigation of the revised standardôs interpretations.

Of course, not every company that handles sensitive electronic data is the same. The ISO 27001:2022 standard offers flexibility in approach in some areas, but itôs requirements must be implemented in full (unlike other standards where exemptions are permitted). To determine how to approach these various requirements, interested organizations should hire the services of a reputable ISO 27001 consulting firm, with documented ISO 27001 implementation experience.

Firms planning a new registration to adopt ISO 27001:2022 should obtain the aid of an accredited consulting company in implementing the existing requirements of the standard as well as the new interpretations of the standard to their specific situations.

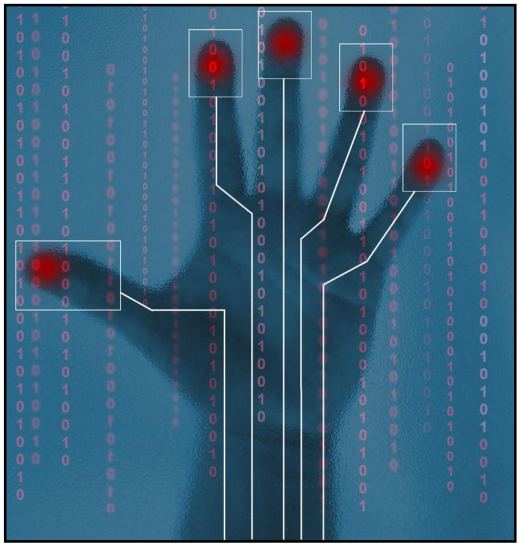
PERRY JOHNSON CONSULTING, INC.
Troy, MI
February 2023

THE USERS OF THIS GUIDE _____

This guide will be useful to managers and other personnel in organizations that meet any of the following criteria:

- Organizations that manage data for any of the myriad of clientele who must have assurance that their data is secure. This includes customers in healthcare, government services, insurance, education, and many others.
- Companies seeking to remain abreast of worldwide information security management system standards development.
- Firms planning to improve their information security management programs
- Companies seeking a competitive advantage in the marketplace
- Firms desiring to make customer satisfaction and customer peace of mind their top priority
- Firms with facilities in the European Union (EU)
- Firms planning to establish facilities in the EU
- Firms planning to export to the EU
- ISO 9001:2015 seeking to add ISO 27001:2022 to their portfolio of certification

WHAT IS ISO 27001?



ISO 27001 is part of a series of information security management systems standards created by the International Organization for Standardization (ISO), a federation of national standards bodies based in Geneva, Switzerland. The American National Standards Institute (ANSI) is the member body representing the United States. All standards are assigned a Technical Committee (TC). JTC 1, Subcommittee 27 is the committee that has responsibility for the ISO 27001 series of standards.

The ISO 27001 information security management standards are not specific to products or services, but apply to information security management processes. While including numerous specified practices, the overall cadre of requirements is sufficiently open to interpretation and there are a number of way to fulfill the requirements.

The latest version of ISO 27001 represented the culmination of several key goals for the ISO. Chief among these was the design to have a common structure for all ISO standards. To achieve this, the ISO appointed a special Joint Technical Coordination Group (JTCG) in 2012 and tasked the JTCG with development of a ñcore textò for the ISO family of standard. The results of their efforts was given the name ñAnnex SL.ò

Annex SL – A Common Structure

Annex SL exists as part of a larger publication called *"ISO Directives Part 1, Consolidated ISO Supplement – Procedures specific to ISO."* This expansive document can be thought of a ñplaybookò for the ISO to follow in the development of standards. As of 2023, nearly every ISO published standard aligns with this core structure and standardized format. We will learn more about Annex SL and the standardized format over the next several pages of this Executive Overview.

The Origin of ISO 27001
(Actually beginning with what is now ISO 27002!)

ISO 27001:2022 draws its roots all the way back to the establishment of the UK Department of Trade and Industry's (DTI) Commercial Computer Security Centre (CCSC). This body was founded in May 1987 with two major objectives. The first of these was to help vendors of information technology security products by establishing a set of internationally recognized security assessment criteria and an associated evaluation and certification scheme. This led to the formation to the ITSEC and the establishment of the ITSEC Scheme.

The second goal of the DTI CCSC was to help prospective users by issuing a set of good security practices. This effort resulted in the ñUsers Code of Practiceò that was published in 1989. This was further revised by the National Computing Centre (NCC), and later a cooperation of users, primarily drawn from the UK, to ensure that the code was both meaningful and practical from a userôs point of view.

The final result was first published as British Standard's guidance document PD 0003, A code of practice for information security management, and following a period of further comment reissued as British Standard BS7799-1:1995.

BS7799-1 received an update in 1999 following further feedback from users and other interested parties. Part 1 of the standard was proposed as an ISO standard via the ñFast Trackò mechanism in October 1999, and published with minor amendments as ISO/IEC 17799:2000 in December 2000.

ISO/IEC 17799:2000 received a significant update in 2005 as ISO/IEC 17799:2005, as a result of the regular cyclical process that ISO standards go through. The most significant change it received at that time was in its listing of controls, which now clearly distinguishes between the requirements, implementation guidance and further information. There was also some rationalization, with the addition of some new controls and existing controls better explained. The revised standard now had 133 controls under 11 headings, as opposed to 127 controls under 10 headings. There were two new major sections ï one putting the controls into a stronger contextual framework of risk assessment and treatment, the other separating out those controls relating to incident management.

In July 2007, a Technical Corrigendum (No. 1) was published by ISO to replace ñ17799ò throughout the original ISO/IEC 17799:2005 standard with the new number ñ27002ò, thus bringing the name of the Code of Practice into line with the other standards in the 27000 series.

Back to ISO 27001

Around the same time that BS7799:1995 was being developed, there were early calls for a useable standard that would address implementation at the organizational level, and that would enable official certification following verification of specified practices. This eventually led to the publication of BS7799-2 in 1999.

The earliest version of BS7799-2 was problematic in that it only gave instruction on how to build an ISMS and not how to operate, maintain and improve it once it had been established. BDD/2 Panel 3 was tasked with creating a new version of BS 7799-2 which would address these issues and facilitate the creation of integrated management systems. The results of their efforts were published in 2002 as BS7799-2:2002.

When it was published, BS 7799 Part 2 was harmonized with the other management system standards (ISO 9001:2000 and ISO 14001:1996). This was accomplished primarily by utilizing the Plan-Do-Check-Act (PDCA) model as part of the management system approach to developing, implementing, and improving the effectiveness of an organization's information security management system.

This principle can be summarized as follows. Plan out every process, implement controls to ensure your process is carried out as planned, institute checks to verify the process is effective, and take action when it is not.

The principle of PDCA model reflected the principles set out in the OECD guidance (OECD Guidelines for the Security of Information Systems and Networks, 2002) governing the security of information systems and networks. In particular, the key ideas of risk assessment, security design and implementation, security management and reassessment.

In 2005, BS 7799-2 finally entered the ISO Fast Track mechanism and emerged as ISO/IEC 27001:2005. There is a lot of similarity between the two standards and two key differences. The first key difference is the adoption of ISO/IEC 17799:2005 as the basis of the standard. The second is the introduction of a new requirement concerning ISMS metrics (process effectiveness measures) and the need to measure the effectiveness of information security controls.

In September 2013, the ISO 27001 and ISO 27002 standards were both revised and issued as the first major standards aligned with the Annex SL framework. These newest standards incorporate a number of key improvements, including the concept of "documented information" which has replaced outdated references to "documents" and "records." Risk based thinking is now pervasive throughout the standard. Finally, the overarching concept of "Interested Parties" broadens the scope of where an organization's requirements and influences on its information security management system might come from.

In 2021 it was decided that both ISO 27001 and ISO 27002 needed to be tweaked, primarily to ensure that the list of mandatory information security controls were consistent and updated to reflect current best practices in an ever evolving marketplace. Both ISO 27001 and ISO 27002 have now completed the full review and approval cycle and have been published as ISO 27001:2022 and ISO 27002: 2002.

The Family of ISO 27000 Standards

In addition to the ISO 27001:2022 and ISO 27002:2022 standards, ISO maintains a long list of available publications for purchase and use in the development of an Information Security Management System. We have highlighted a few of the more important ones below:

- **ISO 27000:2018**, *Information technology – Security techniques – Information security management systems – Overview and Vocabulary*. This document (now in its fourth revision) provides all sanctioned interpretations for the numerous terms used throughout the ISO 27000 series of standards. ISO 27000:2018 also provides helpful information on understanding what an ISMS system is all about, and the various benefits of pursuing implementation of an ISMS system. ISO 27000:2018 is not a certifiable standard, but it can be of great benefit to a company newly starting out in pursuit of ISO 27001:2022 certification.

Å **ISO 27003:2017**, *Information technology – Security techniques – Information security management systems implementation guidance*. This standard, which represents a second edition, provides guidance on best practices for effective implementation of an ISMS system in accordance with ISO 27001:2022 (although it was originally written to address implementation of ISO 27001:2013). It describes the process of securing management approval to implement an ISMS, defines an approach to implement an ISMS (referred to as the ISMS project), and provides guidance on how to plan the ISMS project, resulting in a final ISMS project implementation plan. It is a reference standard in that a company cannot become registered to ISO 27003:2017.

Å **ISO 27004:2016**, *Information technology – Security techniques – Information security management – Monitoring, measurement, analysis and evaluation*. This standard, which represents a second edition, provides practical guidance on developing measures and measurements needed to review the effectiveness of an implemented information security management system (ISMS) and controls or groups of controls. It is a reference standard in that a company cannot become registered to ISO 27004:2016.

Å **ISO 27007:2020**, *Information security, cybersecurity and privacy protection – Guidelines for information security management systems auditing*. This standard, which represents a third edition, provides practical guidance on the auditing of an ISMS. It is intended to be a supplement to the ISO 19011:2018 standard (described below). Furthermore, this guidance is considered non-binding and prospective auditors are not certified to ISO 27007:2020. Indeed, even the Certification Bodies that provide ISO 27001:2022 certification are officially assessed under another standard (ISO 27006:2015).

Additional Relevant or Referenced Standards

- **ISO 19011:2018**, *Guidelines for* A*uditing Management Systems*. This document is a general guideline for the auditing of management systems (quality, environmental, information security, etc.). It applies to first, second and third party audits; auditor qualification criteria; and audit program management. ISO 19011 replaced ISO 10011-1, ISO 10011-2 and ISO 10011-3, along with the three environmental auditing standards: ISO 14010:1996, *Guidelines for Environmental Auditing – General Principles*, ISO 14011:1996, *Guidelines for Environmental Auditing – Audit Procedures – Auditing of Environmental Management Systems*, and ISO 14012:1996, *Guidelines for Environmental Auditing – Qualification Criteria for Environmental Auditors*. ISO 19011:2018 is not a stand-alone certifiable standard.

- **ISO 31000:2018**, *Risk Management – Guidelines*. This document is a general guideline for the successful implementation of Risk Management practices. It is not intended to promote a singular approach to risk management between multiple organizations. Rather, ISO 31000:2018 seeks to provide general guidelines to harmonize risk management processes in existing and future standards. It provides a common approach in support of standards dealing with specific risks and/or sectors, and does not replace those standards. ISO 31000:2018 is not a stand-alone certifiable standard.

REGISTERING TO ISO 27001:2022

ISO 27001:2022 registration is a tangible expression of a firmôs commitment to information security management that is internationally understood and accepted. ISO 27001 registered organizations almost universally realize major increases in the perception of their information security capabilities.

ISO 27001 registration is carried out by certification bodies (commonly called registrars), which are accredited organizations that review the facilityôs information security management system to ensure that it meets the standard and is effective. Once registration is obtained, the registrar conducts regular surveillance audits of the facility to determine if its information security management system continues to meet the standardôs requirements.

As it typically takes 6 to 18 months to complete the ISO 27001 registration process, organizations are advised not to put off registration for too long.

Key Steps to Completing a New Registration

Before an organization can be considered for registration, several preliminary steps should be taken.

The first step is to implement an information security management system that meets ISO 27001:2022 requirements.

To qualify for registration, itôs not enough to just conform to the standard. Organizations must determine what their information security management processes are, and what their intentions are for controlling their processes. Methodologies for the myriad required documents and records (called ñDocumented Information in ISO 27001:2022) must also be determined. Many other questions of approach have to be answered as well, for requirements ranging from competency records to external provider evaluation. Organizations must ensure that the system they establish is robust, effective, transparent, and consistent.

After successfully completing the preliminary steps, a relationship must be established with a registrar. The registrarôs job is to verify whether an organizationôs information security management system has been properly implemented and conforms to ISO 27001:2022 and all other applicable requirements.

Once the services of an accredited registrar have been obtained, a formal application must be filed. When all of the documentation has been submitted, the registrar conducts a two stage audit. The first stage involves an audit of basic documentation including records of a full system internal audit followed by a formal management review. The ñStage 1ò audit will include a variety of preliminary assessments and is intended to ensure that the ISMS is ready for Stage 2 assessment. The ñStage 1ò auditor will identify items that require correction before the ñStage 2ò audit can begin. Once the registrar determines that the Stage 1 basic documentation and data requirements are met, the ñStage 2ò audit may proceed.

The Stage 2 audit is a full system audit that takes place after the Stage 1 corrections are verified by the Stage 2 auditor. Performance data is checked for effectiveness relative to documented objectives. Information security management activities within the facility are checked for conformity to applicable requirements as well as to effectiveness. Other management system activities are checked relative to documented processes and procedures.

During the ñStage 2ò audit, the registrar auditor interviews employees, reviews records, and performs a detailed inspection of the facilityôs information security management system documents. Wherever possible, the auditor will also verify that technical controls are functioning properly by verifying configurations. The purpose of the audit is to ensure that the facilityôs information security management system is functioning adequately and conforms to all ISO 27001:2022 requirements.

Afterward, the registrar reports its findings in an audit report. If any major or minor nonconformities are found, the organization (or auditee) must take corrective action to remedy the cause of the nonconformity. Nonconformities must be remedied within a set time frame, determined by the registrar. Once the registrar has closed out all outstanding nonconformities, a certificate of registration is issued.

To ensure that organizations are following ISO 27001:2022 requirements after registration is obtained, the registrar conducts surveillance audits at least once each year.

Remember: In order to achieve registration to ISO 27001:2022, the organization must completely embrace the standard, which focuses on controls, consistency, and management of risk to critical information.

What to Look For in a Registrar

In selecting a registrar, it is extremely important for every organization to be aware of the relevant qualifications.

A registrar must:

- Be accredited by a national accreditation body, such as the ANAB (ANSI-ASQ National Accreditation Board) of the United States, the Raad voor Accreditatie (RvA) of the Netherlands, or the United Kingdom Accreditation Service (UKAS); to the requirements of both ISO 27006:2015 *Information Technology – Security Techniques – Requirements for bodies providing audit and certification of information security management systems* as well as ISO 17021-1:2015 *Requirements for Bodies providing audit and certification of management systems.* Among other benefits, using an accredited registrar assures the following:
  - The registrar is required to provide a fair and documented process for any disputed findings, client complaints, or other similar situations;
  - The registrar can be reported, and by extension held accountable to the requirements of ISO 27006 and ISO 17021-1 by the accreditation bodies;
  - The registrar must ensure that their auditors are full competent for the audits they perform; and
  - All audits are subject to a wide ranging review process by numerous persons, assuring a fair and unbiased process.
- Maintain a listing of its ISO 27001 qualified auditors;
- Have personnel on its executive (registration) committee or governing board with industry experience and expertise in the appropriate International Accreditation Forum (IAF) Mandatory Document (MD) 1 code ï or an equivalent code such as those found in Standard Industrial Classification (SIC), North American Industry Classification System (NAICS) or European Accreditation of Certification (EAC) codes.

What to Look For in an Auditor

Requirements have been established for the auditors working for accredited ISO 27001 registrars. Before an auditor can evaluate an organizationôs facility to verify whether its information security management system conforms to ISO 27001:2022 requirements, the auditor must satisfy the following conditions:

1) Auditors must have satisfactorily completed ISO 27001 training courses and demonstrated their knowledge of ISO 27001:2022. Certificates are awarded to those auditors who have successfully completed this training;

2) Auditors must understand and comply with the guidance given in ISO 27007:2020*, Information security, cybersecurity and privacy protection — Guidelines for information security management systems auditing* as well as within ISO 19011:2018, *Guidelines for auditing management systems*;

3) They must be recognized and qualified as ISO 27001 auditors under the registrarôs criteria; and,

4) At least one member of an audit team must have relevant industry knowledge in the appropriate IAF ID1 and/or other relevant codes, as determined by the registrarôs qualification process, for each client.

Before hiring the services of a registrar, itôs a good idea to make sure the registrar and its auditors have met the above qualifications.

THE BENEFITS OF ISO 27001:2022

The ISO 27000:2018 standard provides a thorough summary statement on the many benefits of pursuing and achieving ISO 27001:2022 certification. This statement discusses (in part) the following key benefits:

The benefits of implementing an ISMS are realized most significantly in the reduction of information security risks. This means not that such incidents will never happen, but rather that their likelihood is reduced and impact is lessened.

Additional benefits realized from the successful implementation of an ISMS include:

a) A structured framework supporting the process of specifying, implementing, operating and maintaining a comprehensive, cost-effective, value creating, integrated and aligned ISMS that meets the organizationôs needs across different operations and sites;

b) Assistance for management in consistently managing and operating in a responsible manner their approach towards information security management, within the context of corporate risk management and governance, including educating and training business and system owners on the holistic management of information security;

c) Promotion of globally accepted, good information security practices in a non-prescriptive manner, giving organizations the latitude to adopt and improve relevant controls that suit their specific circumstances and to maintain them in the face of internal and external changes;

d) Provision of a common language and conceptual basis for information security, making it easier to place confidence in business partners with a compliant ISMS, especially if they require certification against ISO/IEC 27001 by an accredited certification body;

e) Increase in stakeholder trust in the organization;

f) Satisfying societal needs and expectations; and

g) More effective economic management of information security investments.

Bottom line: An organization that chooses to conform to ISO 27001 will be operating a top-notch information security management system that focuses on informed and competent management decision making, control of risks, and reduced waste.

The Nine Fundamental Principles

ISO 27000:2018, Section 4.2.1 sets forth nine fundamental principles, which have been identified for leading an organization toward the establishment of a robust and reliable information security management system. These Principles are the basis of ISO 27001:2022. They are:

1. Awareness of the need for information security;
2. Assignment of responsibility for information security;
3. Incorporating management commitment and the interests of stakeholders;
4. Enhancing societal values;
5. Risk assessments determining appropriate controls to reach acceptable levels of risk;
6. Security incorporated as an essential element of information networks and systems;
7. Active prevention and detection of information security incidents;
8. Ensuring a comprehensive approach to information security management; and
9. Continual reassessment of information security and making of modifications as appropriate.

ISO 27001:2022 Structure and Clauses

As discussed earlier in this overview, ISO 27001:2022 was among the very first standards to utilize the Annex SL format. This methodology of organizing a standard follows a Plan-Do-Check-Act philosophy and attempts to present requirements is a logical progression.

Non-Auditable clauses of ISO 27001:2022 are:

1 **Scope** ï which provides a general statement about to whom ISO 27001:2022 is intended to apply.

2 **Normative Reference** ï which provides an explanation of the linkage between ISO 27001:2022 and ISO 27000:2018.

3 **Terms and Definitions** ï which establishes the use of ISO 27000:2018 for all official definitions.

Auditable clauses of ISO 27001:2022 are:

4 **Context of the Organization** (4 clauses), which mandate an organization to determine the scope of its system, ascertain interested parties, and in general determine the breadth of their information security management system, which defines and manages processes in order to ensure effective management of secure information.

5 **Leadership** (3 clauses), under which management defines policy, organizational roles, and defines organizational roles and responsibility. It is emphasized that Leadership means a shared responsibility for the management of the quality system.

6 **Planning** (3 clauses), under which the primary requirements related to risk management, as well as security objectives (planning, reporting, etc.) are found.

7 **Support** (5 clauses), which provide requirements pertaining to all of the various resources an organization needs to effectively operate their quality system, including people (competency) communication needs, and documented information (maintained and retained).

8 **Operation** (3 clauses), which provides requirements pertaining to the planning and control of operations, and further controls pertaining to security risks (assessment and treatment).

9 **Performance Evaluation** (3 clauses), which provide requirements pertaining to methods used by Organizations to self-regulate their information security management system and ensure its effectiveness. These clause include requirements Management Review and Internal Audit.

10 **Improvement** (2 clauses), which provides requirements pertaining to the actions that should be taken as a result of evaluations and other output monitoring actions discussed in earlier parts of the standard. Ideas covered here include Corrective Action and Continual Improvement.

ISO 27001:2022 also include a critical list of required controls all found in Annex A and listed as ñTable A.1ò. We will be providing a more complete listing of these controls later in this document. Each of these controls is to be considered mandatory and enforced via a direct reference found in clause 6.1.3 ï ñInformation Security Risk Treatmentò. The controls listed in Table A.1 are also intended to align with the control mechanism given in ISO 27002:2022.

ISO 27001:2022 INFORMATION SECURITY MANAGEMENT SYSTEM REQUIREMENTS

All ISO 27001:2022 clauses are briefly described below.

4 – CONTEXT OF THE ORGANIZATION

4.1 Understanding the organization and its context requires the organization to determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of its information security management system. It is further clarified that determining these issues refers to establishing the external and internal context of the organization considered in Clause 5.3 of ISO 31000:2018.

4.2 Understanding the needs and expectations of interested parties requires the organization to determine the interested parties that are relevant to the information security management system, the relevant requirements of these interested parties, and which of those requirement will be addressed through the information security management system. It is further clarified that the requirements of interested parties may include legal and regulatory requirements and contractual obligations.

4.3 Determining the scope of the information security management system requires the organization to determine the boundaries and applicability of the information security management system to establish its scope, and to consider the external and internal issues referred to in 4.1, the requirements referred to in 4.2, and interfaces and dependencies between activities performed by the organization, and those that are performed by other organizations. It concludes by mandating that the scope be available as documented information.

4.4 Information security management system requires the organization to establish, implement, maintain and continually improve an information security management system including processes needed and their interactions in accordance with the requirements of ISO 27001:2022.

5 – LEADERSHIP

5.1 Leadership and commitment requires top management to demonstrate leadership and commitment with respect to the information security management system by ensuring the information security policy and the information security objectives are established and are compatible with the strategic direction of the organization, ensuring the integration of the information security management system requirements into the organizationôs processes, ensuring that the resources needed for the information security management system are available, communicating the importance of effective information security management and of conforming to the information security management system requirements, ensuring that the information security management system achieves its intended outcome(s), directing and supporting persons to contribute to the effectiveness of the information security management system, promoting continual improvement, and supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility. It is clarified that ñbusinessò references within ISO 27001:2022 can be interpreted broadly to mean those activities that are core to the purposes of the organizationôs existence.

5.2 Policy requires top management to establish an information security policy that is appropriate to the purpose of the organization, includes information security objectives (see 6.2) or provides the framework for setting information security objectives, includes a commitment to satisfy applicable requirements related to information security; and includes a commitment to continual improvement of the information security management system. It goes on to require that the information security policy be available as documented information, be communicated within the organization; and be available to interested parties, as appropriate.

5.3 Organizational roles, responsibilities and authorities requires top management to ensure that responsibilities and authorities for roles relevant to information security are assigned and communicated within the organization. It further requires top management to assign the responsibility and authority for ensuring that the information security management system conforms to the requirements of ISO 27001:2022 and reporting on the performance of the information security management system to top management. Finally, this clause clarifies that top management can also assign responsibilities and authorities for reporting performance of the information security management system within the organization.

6 – PLANNING

6.1 Actions to address risks and opportunities

6.1.1 General requires the organization, When planning for the information security management system, to consider the issues referred to in 4.1 and the requirements referred to in 4.2 and determine the risks and opportunities that need to be addressed to ensure the information security management system can achieve its intended outcome, prevent, or reduce, undesired effects; and to achieve continual improvement. It further requires the organization to plan actions to address these risks and opportunities; and to determine how to integrate and implement the actions into its information security management system processes; and evaluate the effectiveness of these actions.

6.1.2 Information Security Risk Management requires the organization to define and apply an information security risk assessment process that establishes and maintains information security risk criteria that include risk acceptance criteria and criteria for performing information security risk assessments. This process must ensure that repeated information security risk assessments produce consistent, valid and comparable results. Thus process must also identify the information security risks, which includes identifying the information security risk assessment process to identify risks associated with the loss of confidentiality, integrity, and availability for information within the scope of the information security management system, and to identify the risk owners. It further requires the organization to analyze the information security risks, which should include an assessment of the potential consequences that would result if the risks identified were to materialize; an assessment of the realistic likelihood of the occurrence of the risks identified in and a determination of the levels of risk. Finally it requires an evaluation of the information security risks. This must include a comparison of the results of risk analysis with the risk criteria previously established, and a prioritization of the analyzed risks for risk treatment. Retained documented information about the information security risk assessment process is required.

6.1.3 Information Security Risk Treatment requires the organization to define and apply an information security risk treatment process to select appropriate information security risk treatment options, taking account of the risk assessment results, to determine all controls that are necessary to implement the information security risk treatment option(s) chosen, to compare the controls determined above with those in Annex A and verify that no necessary controls have been omitted. *(Please note that we will review Annex A later in this Overview).* It further requires the organization to produce a Statement of Applicability that contains the necessary controls and justification for inclusions, whether the necessary controls are implemented or not, and the justification for exclusions of controls from Annex A. It also requires the formulation of an information security risk treatment process; and to obtain risk ownersô approval of the information security risk treatment plan and acceptance of the residual information security risks. The organization is required to retain documented information about the information security risk treatment process.

6.2 Information Security objectives and planning to achieve them requires the organization to establish information security objectives at relevant functions and levels. The information security objectives must be consistent with the information security policy, be measurable (if practicable), take into account applicable information security requirements, and results from risk assessment and risk treatment. The information security objectives must be monitored, communicated, updated as appropriate, and available as documented information. When planning how to achieve its information security objectives, the organization must determine what will be done, what resources will be required, who will be responsible, when it will be completed, and how the results will be evaluated.

6.3 Planning of Changes requires that when the organization determines the need for changes to the information security management system, that those changes be carried out in a planned manner.

7 – SUPPORT

7.1 Resources requires the organization to determine and provide the resources needed for the establishment, implementation, maintenance and continual improvement of the information security management system.

7.2 Competence requires the organization to determine the necessary competence of person(s) doing work under its control that affects information security performance, to ensure that those persons are competent on the basis of appropriate education, training, or experience, to take actions (where applicable) to acquire the necessary competence, to evaluate the effectiveness of the actions taken; and to retain appropriate documented information as evidence of competence.

7.3 Awareness requires the organization to ensure that persons doing work under the organizationôs control are aware of the information security policy, their contribution to the effectiveness of the information security management system, including the benefits of improved information security performance, and the implications of not conforming with the information security management system requirements.

7.4 Communication requires the organization to determine the internal and external communications relevant to the information security management system, including on what it will communicate, when to communicate, with whom to communicate, how to communicate, with whom to communicate, and how to communicate.

7.5 Documented information

7.5.1 General requires the organizationôs information security management system to include documented information required by ISO 27001:2022, as well as documented information determined by the organization as being necessary for the effectiveness of the information security management system.

7.5.2 Creating and updating requires that when creating and updating documented information, the organization ensures appropriate identification and description (e.g. a title, date, author, or reference number), format (e.g. language, software version, graphics) media (e.g. paper, electronic) and review and approval for suitability and adequacy.

7.5.3 Control of documented information requires documented information required by the information security management system and by ISO 27001:2022 to be controlled to ensure it is available and suitable for use, where and when it is needed. It further requires that documented information be adequately protected (e.g. from loss of confidentiality, improper use, or loss of integrity). It further requires the organization (as it pertains to control of documented information) to address the following activities, as applicable. Distribution, access, retrieval and use, storage and preservation, including preservation of legibility, control of changes (e.g. version control), and retention and disposition. It further required that documented information of external origin determined by the organization to be necessary for the planning and operation of the information security management system be identified as appropriate, and be controlled. Finally it requires documented information retained as evidence of conformity be protected from unintended alterations.

8 – OPERATION

8.1 Operational planning and control requires the organization to plan, implement and control the processes needed to meet information security requirements, and to implement the actions determined in clause 6 by establishing criteria for the processes and implementing control of the processes in accordance with the determined criteria. It further requires the organization to keep documented information to the extent necessary to have confidence that the processes have been carried out as planned. The organization must also control planned changes and review the consequences of unintended changes, taking action to mitigate any adverse effects, as necessary. Finally, the organization must ensure that externally provided processes, products or services that are relevant to the information security management system are controlled.

8.2 Information security risk assessment requires the organization to perform information security risk assessments at planned intervals or when significant changes are proposed or occur, taking account of the criteria established in clause 6. It further requires the organization to retain documented information of the results of the information security risk assessments.

8.3 Information security risk treatment requires the organization to implement the information security risk treatment plan. It further requires the organization to retain documented information of the results of the information security risk treatment.

9 – PERFORMANCE EVALUATION

9.1 Monitoring, measurement, analysis and evaluation requires the organization to determine what needs to be monitored and measured (including information security processes and controls), the methods for monitoring, measurement, analysis and evaluation needed to ensure valid results, who shall monitor and measure, when the monitoring and measuring to be performed, when the results from monitoring and measurement are to be analyzed and evaluated, and who needs to analyze and evaluate the results. It further requires the organization to retain appropriate documented information as evidence of the results. Lastly, this clause requires the organization to evaluate information security performance and the effectiveness of the information security management system.

9.2.1 Internal audit (General) requires the organization to conduct internal audits at planned intervals to provide information on whether the information security management system conforms to the organizationôs own requirements for its information security management system, as well as the requirements of ISO 27001:2022, and to ensure that the information security management system is effectively implemented and maintained.

9.2.2 Internal audit (Program) requires the organization to plan, establish, implement and maintain an audit program(s) including the frequency, methods, responsibilities, planning requirements and reporting, which must take into consideration the importance of the processes concerned and the results of previous audits. The organization is further required to define the audit criteria and scope for each audit, to select auditors and conduct audits to ensure objectivity and the impartiality of the audit process, to ensure that the results of the audits are reported to relevant management, and to retain documented information as evidence of the implementation of the audit program and the audit results.

9.3.1 Management review (General) requires top management to review the organizationôs information security management system, at planned intervals, to ensure its continuing suitability, adequacy, and effectiveness.

9.3.2 Management review (Inputs) requires that management review meetings must include consideration of the status of actions from previous management reviews, any changes in external and internal issues that are relevant to the information security management system, any changes in needs and expectations of interested parties that are relevant to the information security management system, any feedback on the performance of the information security management system, including trends in nonconformities and corrective actions, monitoring and measurement results, audit results, and the fulfilment of information security objectives. It further requires that inputs include a discussion of feedback from interested parties, the results of risk assessment and status of the risk treatment plan, and any opportunities for improvement.

9.3.3 Management review (Outputs) requires the results of management review include decisions related to continual improvement opportunities, and any need for changes to the information security management system. It further requires the organization to retain documented information as evidence of the results of management reviews.

10 – IMPROVEMENT

10.1 Continual improvement requires the organization to continually improve the suitability, adequacy and effectiveness of the information security management system.

10.2 Nonconformity and corrective action requires that when a nonconformity occurs, the organization must react to the nonconformity and, as applicable take action to control and correct it and deal with the consequences. Furthermore, it requires the organization to evaluate the need for action to eliminate the cause(s) of the nonconformity, in order that it does not recur or occur elsewhere, by reviewing the nonconformity, by determining the causes of the nonconformity, by determining if similar nonconformities exist, or could potentially occur, by implementing any action needed, by reviewing the effectiveness of any corrective action taken, and by making changes to the information security management system, if necessary. Furthermore it requires that corrective actions be appropriate to the effects of the nonconformities encountered. This clause also requires the organization to retain documented information as evidence of the nature of the nonconformities and any subsequent actions taken, as well as the results of any corrective action.

Annex A (Normative)

The control objectives and controls listed in the table below are directly derived from and aligned with those given in ISO 27002:2022. These controls are intended to be used in context to clause 6.1.3 discussed earlier in this overview.

5 – Organizational Controls		
5.1	Policies for information security	Information security policy and topic specific policies are required to be defined, approved by management, published and communicated to/acknowledged by relevant personnel and relevant interested parties, as well as reviewed at planned intervals and if significant changes occur.
5.2	Information security roles and responsibilities	These shall be defined and allocated according to the organization needs.
5.3	Segregation of duties	Conflicting duties and areas of responsibility must be segregated.
5.4	Management responsibilities	Management needs to require all personnel to apply information security in accordance with established information security policy, topic specific policies, and the organizationôs procedures.
5.5	Contact with authorities	These shall be established and maintained.
5.6	Contact with special interest groups	Contacts with special interest groups or other specialist security forums and professional associations are to be maintained.
5.7	Threat intelligence	Information on this shall be produced from a collecting and analyzing of information security threats.
5.8	Information security in project management	Information security must be integrated into project management.
5.9	Inventory of information and other associated assets	This shall be developed and maintained, including identification of owners.
5.10	Acceptable use of information and other associated assets	Protocols for the acceptable use and procedures for handling information and other associated assets must be identified, documented, and implemented.
5.11	Return of assets	Personnel and other interested parties as appropriate have to return all organization owned assets in their possession upon change or termination of their employment, contract, or agreement.

5.12	Classification of information	This is required according to the information security needs of the organization based on confidentiality, integrity, availability, and relevant interested party requirements.
5.13	Labeling of information	An appropriate set of procedures for information labeling needs to be developed and implemented in accordance with the information classification scheme adopted by the organization.
5.14	Information transfer	Rules, procedures, or agreements for this activity need to be in place for all types of transfer facilities within the organization and between the organization and other parties.
5.15	Access control	Rules to control physical and logical access to information and other associated assets have to be established and implemented based on business and information security requirements.
5.16	Identity management	The full life cycle of identities has to be managed.
5.17	Authentication information	Allocation and management of authentication information has to be controlled by a management process, including advising personnel on appropriate handling of authentication information.
5.18	Access rights	Access rights to information and other associated assets have to be provisioned, reviewed, modified, and removed in accordance with the organizationôs topic-specific policy on and rules for access control.
5.19	Information security and supplier relationships	Processes and procedures have to be defined and implemented to manage any information security risks associated with the use of suppliers products or services.
5.20	Addressing information security within supplier agreements	Relevant information security requirements has to be established and agreed with each supplier based on the type of supplier relationship.
5.21	Managing information security in the information and communication technology (ICT) supply chain	Processes and procedures must be defined and implemented to manage the information security risks associated with the ICT products and services supply chain.
5.22	Monitoring, review, and change management of supplier services	The organization must regularly monitor, review, evaluate, and manage change in supplier information security practices and service delivery.
5.23	Information security for use of cloud services	Processes for acquisition, use, management, and exit from cloud services must be established in accordance with the organizationôs information security requirements.

5.24	Information security incident management planning and preparation.	The organization has to plan and prepare for these by defining, establishing, and communicating information security incident management processes roles and responsibilities.
5.25	Assessment and decision on information security events	The organization has to assess these events and decide if they are to be categorized as information security incidents.
5.26	Response to information security incidents	Information security incidents must have a response in accordance with the documented procedures.
5.27	Learning from information security incidents	Knowledge gained from information security incidents must be used to strengthen and improve information security controls.
5.28	Collection of evidence	The organization has to establish and implement procedures for the identification, collection, acquisition, and preservation of evidence related to information security events.
5.29	Information security during disruption	The organization has to plan how to maintain information security at an appropriate level during disruptions.
5.30	ICT readiness for business continuity	ICT readiness has to be planned, implemented, maintained, and tested based on business continuity objectives and ICT continuity requirements.
5.31	Legal, statutory, regulatory, and contractual requirements	If such requirements are relevant to information security, the organization's approach to meet these requirements has to be identified, documented, and kept up to date.
5.32	Intellectual property rights	The organization must implement appropriate procedures to protect intellectual property rights.
5.33	Protection of records	Records must be protected from loss, destruction, falsification, unauthorized access, and unauthorized release.
5.34	Privacy and protection of personal identifiable information (PII)	The organization has to identify and meet the requirements including the preservation of privacy and protection of PII according to applicable laws and regulations and contractual requirements.
5.35	Independent review of information security	The organization's approach to managing information security and its implementation including people, processes, and technology has to be reviewed independently at planned intervals or whenever significant changes occur.
5.36	Compliance with policies, rules, and standards for information security	Compliance with the organization's information security policy, topic-specific policies, rules, and standards has to be regularly reviewed.

5.37	Documented operating procedures	Operating procedures for information processing facilities have to be documented and made available to personnel who need them.
6 – People Controls		
6.1	Screening	Background verification checks on all candidates to become personnel have to be carried out prior to joining the organization and on an ongoing basis after hiring taking into consideration applicable laws, regulations, and ethics and must be proportional to business requirements, the classification of the information to be accessed, and any perceived risks.
6.2	Terms and conditions of employment	Employment contractual agreements must state the personnelôs and the organizationôs responsibility for information security.
6.3	Information security awareness, education, and training	Organization personnel and relevant interested parties have to receive appropriate information security awareness, education, and training and must also receive regular updates of the organization's information security policy, topic-specific policies and procedures, as relevant for their job function.
6.4	Disciplinary process	A disciplinary process has to be formalized and communicated to take action against personnel and other relevant interested parties who have committed an information security policy violation.
6.5	Responsibilities after termination or change of employment	Information security responsibilities and duties that remain valid after termination or change of employment have to be defined, enforced, and communicated to relevant personnel and other interested parties.
6.6	Confidentiality or non-disclosure agreements	Confidentiality or nondisclosure agreements reflecting the organization's needs for the protection of information have to be identified, documented, regularly reviewed, and signed by personnel and other relevant interested parties.
6.7	Remote working	Security measures have to be implemented when personnel are working remotely to protect information accessed, processed, or stored outside of the organization's premises.
6.8	Information security event reporting	The organization has to provide a mechanism for personnel to report observed or suspected information security events through appropriate channels in a timely manner.

7 – Physical Controls		
7.1	Physical security perimeters	Security perimeters have to be defined and used to protect areas that contain information and other associated assets.
7.2	Physical entry	Secure areas need to be protected by appropriate entry controls and access points.
7.3	Securing offices, rooms, and facilities	Physical security for offices, rooms, and facilities must be designed and implemented.
7.4	Physical security monitoring	Premises have to be continuously monitored for unauthorized physical access.
7.5	Protecting against physical and environmental threats	Protection against physical and environmental threats, such as natural disasters and other intentional or unintentional physical threats to infrastructure have to be designed and implemented.
7.6	Working in secure areas	Security measures for working in secure areas shall be designed and implemented.
7.7	Clear desk and clear sign	Clear desk rules for papers and removable storage media and clear screen rules for information processing facilities must be defined and appropriately enforced.
7.8	Equipment siting and protection	Equipment has to be sited securely and protected.
7.9	Security of assets off premises	Off-site assets have to be protected.
7.10	Storage media	Storage media must be managed through their lifecycle of acquisition, use, transportation, and disposal in accordance with the organization's classification scheme and handling requirements.
7.11	Supporting utilities	Information processing facilities must be protected from power failures and other disruptions caused by failures in supporting utilities.
7.12	Cabling security	Cables carrying power, data, or supporting information services shall be protected from interception, interference, or damage.
7.13	Equipment maintenance	Equipment has to be maintained correctly to ensure availability, integrity, and confidentiality of information.
7.14	Secure disposal or reuse of equipment	Items of equipment containing storage media have to be verified to ensure that any sensitive data and licensed software has been removed securely or overwritten prior to disposal or reuse.

8 – Technological Controls		
8.1	User end point devices	Information stored on, processed by, or accessible via user endpoint devices has to be protected.
8.2	Privileged access rights	The allocation and use of privileged access rights has to be restricted and managed.
8.3	Information access restriction	Access to information and other associated assets needs to be restricted in accordance with the established topic-specific policy on access control.
8.4	Access to source code	Read and write access to source code, development tools, and software libraries have to be appropriately managed.
8.5	Secure authentication	Secure authentication technologies and procedures must be implemented based on information access restrictions and the topic-specific policy on access control.
8.6	Capacity management	The use of resources has to be monitored and adjusted in line with current and expected capacity requirements.
8.7	Protection against malware	Protection against malware has to be implemented and supported by appropriate user awareness.
8.8	Management of technical vulnerabilities	Information about technical vulnerabilities of information systems in use needs to be obtained, and the organizationôs exposure to such vulnerability has to be evaluated, and appropriate measures taken.
8.9	Configuration management	Configurations, including security configurations, hardware, software, services, and networks have to be established, documented, implemented, monitored, and reviewed.
8.10	Information deletion	Information stored in information systems, devices, or in any other storage media must be deleted when no longer required.
8.11	Data masking	Data masking needs to be used in accordance with the organization's topic-specific policy on access control and other related topic-specific policies, and business requirements, taking appropriate legislation into consideration.
8.12	Data leakage prevention	Data leakage prevention measures must be applied to systems, networks, and any other devices that process, store, or transmit sensitive information.

8.13	Information backup	Backup copies of information, software, and systems must be maintained and regularly tested in accordance with the agreed topic-specific policy on backup.
8.14	Redundancy of information processing facilities	Information processing facilities have to be implemented with redundancy sufficient to meet availability requirements.
8.15	Logging	Logs that record activities, exceptions, faults, and other relevant events have to be produced, stored, protected, and analyzed.
8.16	Monitoring activities	Networks, systems, and applications have to be monitored for anomalous behavior and appropriate actions must be taken to evaluate potential information security incidents.
8.17	Clock synchronization	Clocks of information processing systems used by the organization have to be synchronized to approved time sources.
8.18	Use of privileged utility programs	The use of utility programs that can be capable of overriding system and application controls have to be restricted and tightly controlled.
8.19	Installation of software on operational systems	Procedures and measures have to be implemented to securely manage software installation on operational systems.
8.20	Networks security	Networks and network devices have to be secured, managed, and controlled to protect information in systems and applications.
8.21	Security of network services	Security mechanisms, service levels, and service requirements of network services have to be identified, implemented, and monitored.
8.22	Segregation of networks	Groups of information services, users, and information systems need to be segregated in the organizationôs networks.
8.23	Web filtering	Access to external websites must be managed to reduce exposure to malicious content.
8.24	Use of cryptography	Rules for the effective use of cryptography, including cryptographic key management, must be defined and implemented.
8.25	Secure development lifecycle	Rules for the secure development of software and systems have to be established and applied.
8.26	Application security requirements	Information security requirements must be identified, specified, and approved when developing or acquiring applications.

8.27	Secure system architecture and engineering principles	Principles for engineering secure systems must be established, documented, maintained, and applied to any information system development activities.
8.28	Secure coding	Secure coding principles have to be applied to software development.
8.29	Security testing in development and acceptance	Security testing processes must be defined and implemented in the development lifecycle.
8.30	Outsourced development	The organization must direct, monitor, and review activities related to outsourced system development.
8.31	Separation of development, test, and production environments	Development, testing, and production environments have to be separated and secured.
8.32	Change management	Changes to information processing facilities and information systems have to be subject to change management procedures.
8.33	Test information	Test information must be appropriately selected, protected, and managed.
8.34	Protection of information systems during audit testing	Tests and other assurance activities involving assessment of operational systems must be planned and agreed between the tester and appropriate management.

CONCLUSION

Since its initial release in 2005, the ISO 27001 information security management systems standard has sought to have an enormous impact on the world of information security management.

In the short run, implementing an ISO 27001:2022 information security management system has a major and positive impact on the perception an organization gives its customers of its ability to manage and secure important electronic information. Not to mention ISO 27001:2022 registration can give American businesses unmatched credibility and competitive advantages in the European Union.

In the long run, ISO 27001:2022 implementation and registration will preserve and create domestic and international markets for American businesses in virtually every field where the security of information is paramount. Even now, many major American businesses and government agencies are requiring ISO 27001:2022 registration as a supplier information security assurance qualification.

ISO 27001:2022 furthers a tradition of flexibility, and through its alignment with Annex SL ensures that the organization can easily and seamlessly incorporate as many additional standards (ISO 45001, ISO 50001, etc.) as it sees fit.

THE STANDARD SHOULD BE OBTAINED FROM WWW.ISO.ORG OR WWW.ANSI.ORG.