Understanding ISO 27001

500 Federal Street
Troy, NY 12180
(800) 803-4350

www.greycastlesecurity.com
intel@greycastlesecurity.com

Bring Your Vision to Life

Candice Wold
Security Strategist

GreyCastle security

1. What is ISO 27001?

ISO 27001 is an internationally recognized standard codifying the audit requirements for an Information Security Management System, or ISMS. This standard was the first of the ISO27XXX series first published by the International Organization for Standardization, or ISO (www.iso.org), in October 2005 and revised in 2013.

ISO 27001 is high level, broad in scope, and conceptual in nature. This approach allows it to be applied across multiple types of enterprises and applications. ISO 27001 is the only information security "standard" devoted to information security management audit criteria in a field generally governed by specific operational audit criteria.

As a standard that is primarily conceptual, ISO 27001 is not:

- A technical standard.
- Product or technology driven.
- An equipment evaluation methodology.

ISO 27001 is however:

- A comprehensive minimum baseline of information security management controls that all Information Security Programs SHALL address in some manner. This in essence makes ISO 27001 internationally sanctioned "due diligence."

2. Why ISO 27001?

The information security field has traditionally been based on sound "best practices" and "guidelines". While this cumulative wisdom of the ages is valid, it is also subject to various interpretations and implementations, not always consistent or harmonious. Furthermore, without the risk justification required by ISO 27001 "best practice" is in reality "best guess" devoid of the underlying analysis that makes control implementation both justifiable and defensible. ISO 27001 offers the following benefits:

- An internationally recognized management system that can enhance information security interoperability and trust with trading partners.
- A yardstick to evaluate Information Security Program effectiveness.

- A vehicle to certify “due diligence”.
- An umbrella under which multiple data protection regulations may be managed.

Reasons to pursue an ISO 27001 based Information Security Program also vary:

- For some industries, an ISO 27001 certified operational area may become a de facto requirement.
- For organizations subject to government regulation, ISO 27001 may increase efficiency and eliminate redundancy in complying with multiple information protection regulations through centralized management.
- For data centric organizations, customer perception of an ISO 27001 certified operational area may offer a marketing advantage.
- An ISO 27001 certified operational area provides a high degree of defensibility.

3. Background

ISO 27001 is a direct descendent of the British Standards Institute (BSI) Information Security Management standard BS 7799-2. BSI has long been proactive in the evolving field of Information Security.

In response to industry demands, a working group devoted to Information Security was first established in the early 1990’s, culminating in a “Code of Practice for Information Security Management” in 1993. This work evolved into the first version of the BS 7799 standard released in 1995.

In the late 1990’s, in response to industry demands, BSI formed a program to accredit auditing firms, or “Certification Bodies,” as competent to audit to BS 7799. Simultaneously, a steering committee was formed, culminating with the update and release of BS 7799 in 1998, 1999, 2000, and finally in 2002.

By this time, information security had become headline news and a concern to computer users worldwide. While some organizations utilized the BS 7799 standard, demand grew for an internationally recognized information security standard under the aegis of an internationally recognized body, such as the ISO. This demand led to the updating and release of BS7799-2 as ISO 27001 in October of 2005.

Finally, in September of 2013, ISO 27001 was revised and updated to put more emphasis on measuring and evaluating how well an organization's ISMS is performing. Additionally, a section on outsourcing to third parties was included, reflecting market behavior of organizations relying on third parties for aspects of IT. Further, emphasis was removed on the Plan Do Act Check cycle (though the PDCA is still common practice in ISMS implementation and maintenance) allowing for other continuous improvement methodologies to be utilized. Overall, the changes in ISO 27001 were aimed at aligning with other management system standards such as ISO 9001 and ISO 20000.

4. ISO 27001 versus ISO 27001

Both standards serve distinct purposes, hence it is important to understand the differences between ISO 27001 and ISO 27002.

ISO 27001	ISO 27002
An auditing standard based up auditable requirements	An implementation guide based upon best practice suggestions
A list of management controls an organization shall address	A list of operational controls an organization should consider
Used as a means to audit and certify an organization's Information Security Management System	Used as a means to assess the comprehensiveness of an organization's Information Security Program

5. Control Areas

ISO 27001 defines a management system as organizational structure, policies, planning activities, responsibilities, practices, procedures, processes, and resources. ISO 27001 further defines an ISMS as that part of the overall management system, based on a risk approach, to establish, implement, operate, monitor, review, maintain and improve information security. This comprehensiveness causes an ISO 27001 ISMS to potentially interact with multiple enterprise departments and programs such as:

- Human Resources
- Legal / Compliance
- Suppliers / Procurement
- Business Continuity

- Audit
- Facilities
- Operations
- Physical Security

The ISO 27001 control areas, control objectives and key control attributes are summarized below. See ISO 27001 for complete details.

6. Mandatory Controls

The controls detailed within ISO 27001 sections 4-10 are required for conformance to this standard.

7. Context of the Organization

This is a new clause in ISO 27001 that addresses establishing the context of the ISMS with in the enterprise or entire organization. This clause calls for the identification of organizational objectives in terms of information security, as well as external and internal issues, and interested parties in order to define the scope of the ISMS.

8. Leadership

This clause places requirements on what the standard refers to as “top management” – the person or group of people, who directs and controls the organization at the highest level, to demonstrate leadership and commitment to the ISMS. A specific responsibility includes establishing the information security policy. Further, this clause places the requirements for top management to assign information security responsibilities and authority.

9. Planning

This clause calls for reference to the organizational context (issues) and interested parties (requirements) in establishing the ISMS to determine the risk and opportunities that need to be addressed, with the intended result to be:

- Ensure the ISMS can achieve its intended outcomes
- Prevent or reduce undesired effects
- Achieve continuous improvement

This is can be accomplished through the assessment of information security risk (risk assessment, risk treatment plan and the Statement of Applicability – selection of controls). ISO 27001:2013 has widened the use of risk assessment methodologies in order to identify the risk and opportunities that exist. Following the assessment of risk, a risk treatment plan, which includes the assignment of risk owners and the determination of mitigating controls, is to be carried out.

Further, through this clause, the organization is to establish information security objectives relevant to the business areas (functions) and levels of management of the organization.

10. Support

This clause focuses the requirement of an organization to determine and provide the necessary resources to establish, implement, maintain and continually improve the ISMS. This is met through establishing:

- Competence - necessary skills and knowledge to see that information security activities and actions can in fact be implemented and acted upon.
- Awareness - the policy is understood, contribution to the ISMS can occur, and the implications of nonconformance are understood.
- Communication – external and internal relevant communications are understood.
- Documentation – required documentation from ISO 27001 is created and present as well as all other relevant documentation that the organization deems necessary for the effectiveness of the ISMS.

11. Operation

This clause aims at the organizations ability to execute the plans and processes that are subject of the previous clauses, which include:

- Establishing the processes needed for the organization to meet its information security requirements and implement actions needed to address the information security risk and opportunities
- Conduct regular information security risk assessments
- Implement the information security risk treatment plan

12. Performance Evaluation

This clause focuses on how the organization is assess the performance and effectiveness of the ISMS by identifying how the organization will monitor, measure, analyze and evaluate the organization's information security and effectiveness of its ISMS.

Additionally, this clause identifies the need for an internal audit. The audit program needs to be capable of determining if the ISMS conforms to the requirements of ISO 27001 and determining if the ISMS has been implemented effectively or not.

Finally, the performance evaluation of the ISMS shall include a review by management in planned intervals. Management review includes establishing the review process, planning the review process, reviewing the performance of the ISMS, and generating review outputs and a record of such reviews.

13. Improvement Requirements

ISO 27001 sets the requirement that efforts shall be made to continuously improve and take corrective actions when nonconformities occur. Organizations are to take action to control and correct nonconformities and to deal with the consequences of nonconformities. The cause is to be identified and an evaluation of the need to eliminate or control the cause shall occur. Further, corrective actions need to be implemented to address the cause. These corrective actions are to be reviewed and necessary changes to the ISMS shall occur.

Finally, an organization shall work to improve and enhance the overall performance of the ISMS. This is done through a constant understanding of the context of the organization and the requirements of interested parties to ensure the suitability, adequacy and effectiveness of the ISMS.

14. Discretionary Controls

The controls detailed within ISO 27001 Annex A are the same controls detailed within ISO 27002, but without the implementation guidance provided within ISO 27002. ISO 27001 requires that these Annex A controls be completely addressed, but not necessarily implemented. The business-friendly stance of ISO 27001 allows for risk acceptance based upon organizational risk tolerance criteria established by management. Those Annex A controls not implemented must have documented risk acceptance justification.

Annex A control areas include:

• Information Security Policy	• Access Control
• Organization of Information Security	• Physical and Environmental Security
• Human Resource Security	• Cryptography
• Asset Management	• Operations Security
• Communications Security	• Incident Management
• Systems Acquisition, Development and Maintenance	• Information Security Aspects of Business Continuity Management
• Supplier Relationships	• Compliance

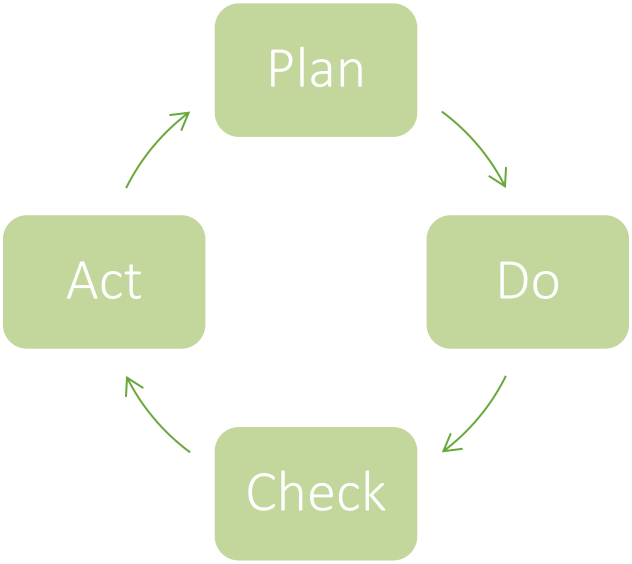
15. How is ISO 27001 Implemented?

A process is considered to be any activity using resources and managed in order to enable the transformation of inputs into outputs. A process approach is when individual processes and their interactions are bundled into a cohesive package, or system, chartered to accomplish something. ISO 27001 is implemented through the creation and maintenance of an Information Security Management System or ISMS chartered with establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an organizations information security.

16. The PDCA Model (Suggested)

ISO 27001:2013 allows for the adoption of an organization's preferred continuous improvement methodology. The most common methodology for implementation and

continuous improvement is the Plan, Do, Check, Act (PDCA) model. The PDCA model is common to other management systems such as those defined within ISO 9001 (Quality) and ISO 14001 (Environment) and is also consistent with OEDC guidelines.



Plan	Establish ISMS
Do	Implement and operate the ISMS
Check	Monitor and review the ISMS
Act	Maintain and improve the ISMS

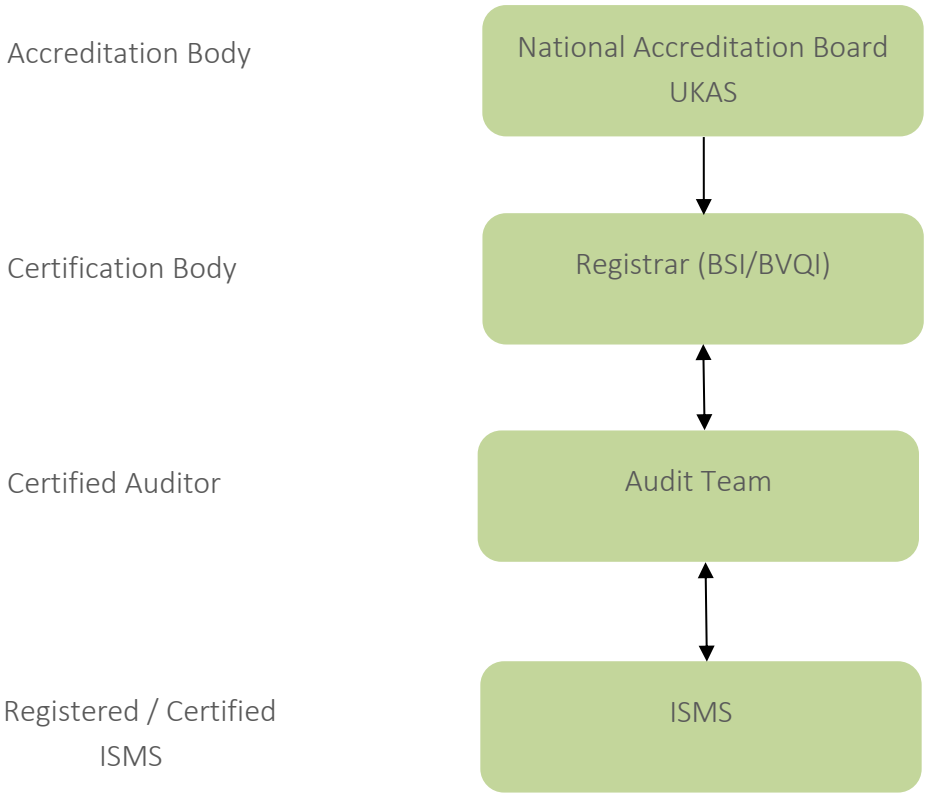
ISMS is a strategic initiative, and this iterative level one process directly maps to the section 4-10 controls. See the companion whitepaper "Understanding ISMS" for further details on the methods employed to implement this process tactically and operationally.

17. How is ISO 27001 Certification Obtained?

ISO itself does not participate in conformance audit activities. However, its standards and guides harmonize conformity assessment worldwide through independent third- party auditors.

18. Certification Model

The certification model starts with the National Accreditation Board of each respective country. Examples are UKAS in the United Kingdom, and RvA in the Netherlands. These respective National Accreditation Boards accredit individual registrars or registration firms as a Certification Body, authorized and competent to audit against ISO 27001 requirements. The Certification Body will audit an organization against ISO 27001, potentially leading to ISO 27001 Certification. Once certified as conformant to ISO 27001, the ISMS become registered, and under registrar governance. The validity of the certification and registration is thus ultimately derived from the National Accreditation Board of the respective country.



19. Conformance Maintenance

The accredited Certification Body that issued the original Certificate of Conformance and maintains the registration must approve changes to the security infrastructure defined within the Scope of Registration. Minor changes may be submitted in writing, furnishing the evaluator with enough detail to determine impact. Major changes may require re-auditing. Surveillance visits are performed annually, and a re-certification audit is required every three years.

20. Process vs. Product

There is misunderstanding in the industry regarding both the approach, and level of effort required to implement either an ISO 27002 based Information Security Program or an ISO 27001 certified operational area. Many organizations simply wish to start with a "standards based" information security infrastructure, unable to immediately justify the extra effort required for certification. This "standards based" infrastructure will nevertheless leave them well poised to proceed toward certification should a business justification emerge. Other organizations are misled into believing that the purchase of a "product" will automatically make them conformant.

20.1 Toolkit Approach

- Can produce a set of ISO 27002 pre-written "policies" or "direction"
- Cannot cover the ISO 27002 controls addressable by "actions" since actions are executed uniquely in each environment.
- Cannot assign a defensible risk-based justification unless coupled with a risk assessment process
- May create a false sense of security for organizations believing possession of "security policies" is all that is required for conformance.
- Cannot speak to the management of the controls required by ISO 27001

20.2 Process Approach

- May utilize a toolkit as a starting point of discussion.
- Takes into account organizational behavior to gain buy-in at all levels.

- Takes into account the organizations legal and regulatory environment.
- Acknowledges and works within the organizations culture and values.
- Produces risk justified security requirements, processes, roles, and activities required to justify the selection of ISO 27002 controls.
- Is defensible.

21. Conclusion

- ISO 27002 is the implementers guide, suggesting what should be done based upon internationally recognized best practice. As a result, it serves as an excellent basis to build an enterprise Information Security Program.
- An Information Security Program oversees the organizations information protection initiative, and may have responsibility over multiple operational areas.
- ISO 27001 is the auditors guide specifying what shall be done based upon Quality Management principles inherent to a management system.
- Operational areas serve as the basis of establishing the scope of an ISO 27001 certification.
- Scope of an ISO 27002 Information Security Program and an ISO 27001 operational area do not have to be the same.

There is an ever-increasing demand for information security certification. This phenomenon will be driven by many factors, including:

- Regulatory requirements, such as HIPAA, GLBA, and SOX which require information security to be managed.
- Marketing incentives, particularly in e-commerce and finance
- Financial incentives, such as insurance premium reductions
- Corporate “due diligence” concerns

All of these examples represent growth opportunities and challenges to all practitioners and students of information security.

22. About Candice Wold

Candice Wold is GreyCastle Security's Security Strategist and Practice Lead for Compliance.

Candice represents GreyCastle Security in the Bay Area and specializes in the information security management frameworks of ISO 27001:2013, SSAE 16, NERC CIP, NIST 800-53, and FISMA. Candice is an ISO/IEC 27001:2103 Certified Lead Auditor and will be assisting our clients with the design and implementation of custom Information Security Management Systems (ISMS) with the goal of ISO 27001 certification.

She enjoys learning about the nuances between the public and private space through the FedRAMP Program and will continue her expertise as cloud service providers continue to offer capabilities in the Federal space.

In her free time, she enjoys competitive running and exploring local breweries. As a breakfast food connoisseur, she has never been known to turn down French toast.