Sri Lanka Institute of Information Technology

Report on ISO 27001 Implementation for an Organization

Group Assignment

IE3102 - Enterprise Standards for Information Security

Submitted by:

Student Registration Number	Student Name
IT20028046	Gunathilaka S.B.M.B.S. A
IT19108100	Herath H.M.C.S.B

Date of submission
30th of September 2022

Contents

Introduction

Formally known as ISO/IEC 27001, it is a part of the leading international standards for information security.The International Electrotechnical Commission (IEC) and the International Organization for Standardization (ISO) worked together to publish it in 2013, and it was made available to the public at that time (IEC). 2019 saw an alteration to the overall structure.

The implementation of an information security management system is strongly encouraged by ISO 27001. (ISMS). This method intends to combine information security with a coherent management system in order to produce a united set of controls, which is something that a lot of fast emerging companies could initially lack.

The fact that ISO 27001 assesses assets that aren't necessarily related to information technology makes this standard seem more attainable to a greater number of businesses.

It is intended to produce a risk-focused company management system that is conducive to any sort of information asset protection. It can secure information assets stored in IT systems, on hard copy or digital media, and even in the minds of individuals. Not intended for use as a technological security standard.

The specification specifies the following:

- The mandatory "requirements "(often known as the "management system clauses") that follow the ISO Directives Part 1 Annex SL framework; and

- Annex A – an example set of risk-selectable controls typically used to help reduce risks to a tolerable level.

Why is ISO 27001 important?

Information is something that every business generates, stores, and disseminates, and all of it is valuable. Safeguarding the company's assets and generating a substantial return on investment, the implementation of a globally recognized information security management system is a no-brainer.

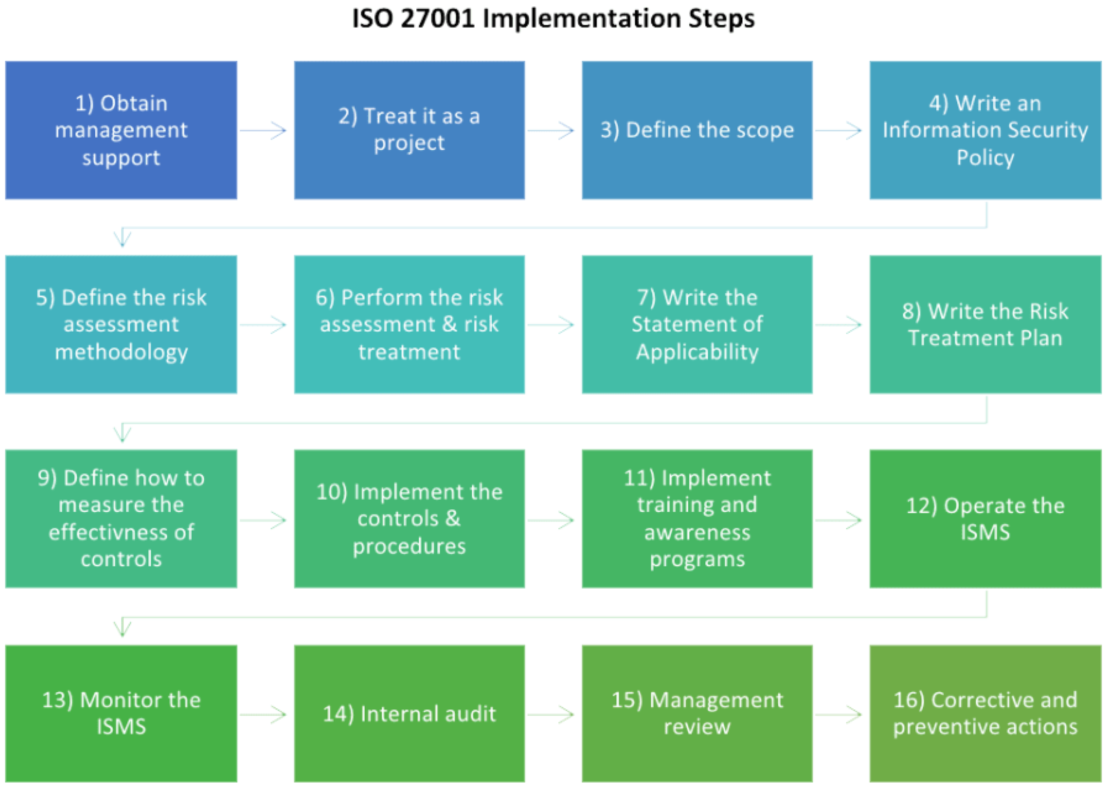
Among the possible advantages are:

- Ability to function in governed markets that demand provable data protection.
- Having that official recognition to use as a selling point when trying to attract new customers.
- By reducing information security management processes and concentrating security controls where they are most needed to prevent major threats, operational costs can be reduced.
- Reducing information and cyber incident response costs is a priority.
- There is clearer evidence of compliance with laws and regulations, and the penalties for breaking them are milder.

Who provide ISO 27001 certification?

These certification bodies train their auditors to conduct certification audits and verify that all certifications comply to a uniformly high degree of accreditation. Typically, a directory of such businesses can be found on the official website of the local accreditation organization. The United Kingdom Accreditation Service (UKAS) is in charge of regulating certified certifying bodies in the United Kingdom.

Implementation steps


ISO 27001 Implementation Steps
1) Obtain management support
2) Treat it as a project
3) Define the scope
4) Write an Information Security Policy
5) Define the risk assessment methodology
6) Perform the risk assessment & risk treatment
7) Write the Statement of Applicability
8) Write the Risk Treatment Plan
9) Define how to measure the effectivness of controls
10) Implement the controls & procedures
11) Implement training and awareness programs
12) Operate the ISMS
13) Monitor the ISMS
14) Internal audit
15) Management review
16) Corrective and preventive actions

Obtain management support

Whoever the person or team working on implementing this standard should not forget to get the help of the management, it's not a serious thing, but we cannot work without their help. According to experts, this is one of the significant reasons to fail the iso27001 project. If we look from the management perspective, they don't assign enough people to the project or the employees working on that project don't get enough salary and other facilities. The upcoming sections will provide some guides to learn how to convince your management and measure how much it will cost.

Treat it as a project

Implementing an ISMS(Information Security Management System)based on iso27001 is a complex task which takes at least a few months.for this activity, many employees are involved from various departments, and for large-scale organizations will take a year or more than a year.

So we can clearly see it's not a simple task, and we should define a time frame that includes what we are going to do in each time segment, what the plan is, and who is involved in this.in other words, we must apply project management by considering this a project unless you will never succeed from this project.

Define the scope

If the organization is more prominent, it always gives a positive result if we implement iso27001, one part of the organization, and it will reduce the risk of the project to a significantly lower level. If the company is more minor (we can decide if the organization is small by considering employee count and if employees are less than 50 we can decide it's a small organization), it is easier to implement iso27001 to the whole company in the given scope.

Write an Information Security Policy

Hence the top-level internal document is the information security policy. There are no restrictions like it should be very explicit content. But it is necessary to give the baseline requirements to our organization to fill its basic security. Since the document is not very comprehensive, it should contain what the things it wants to achieve are and how to handle them. This document doesn't require all the company's security information, and pointing out enough points is enough.

The information security policy document must contain the below areas.

- Objectives: the primary and most critical objectives to be achieved by the information security
- requirements section: supply the contractual, legal and statutory requirements and reference those requirements
- regarding risk management: evaluate the suggested information security controls, and reference the evaluation process.
- responsibilities: there are some responsibilities bound with ISMS (implementation, maintenance, monitoring, reporting)
- communication: the people who affect this policy.
- Support: adherence to the policies and commitment to the procedures with resources.

Define the risk assessment methodology

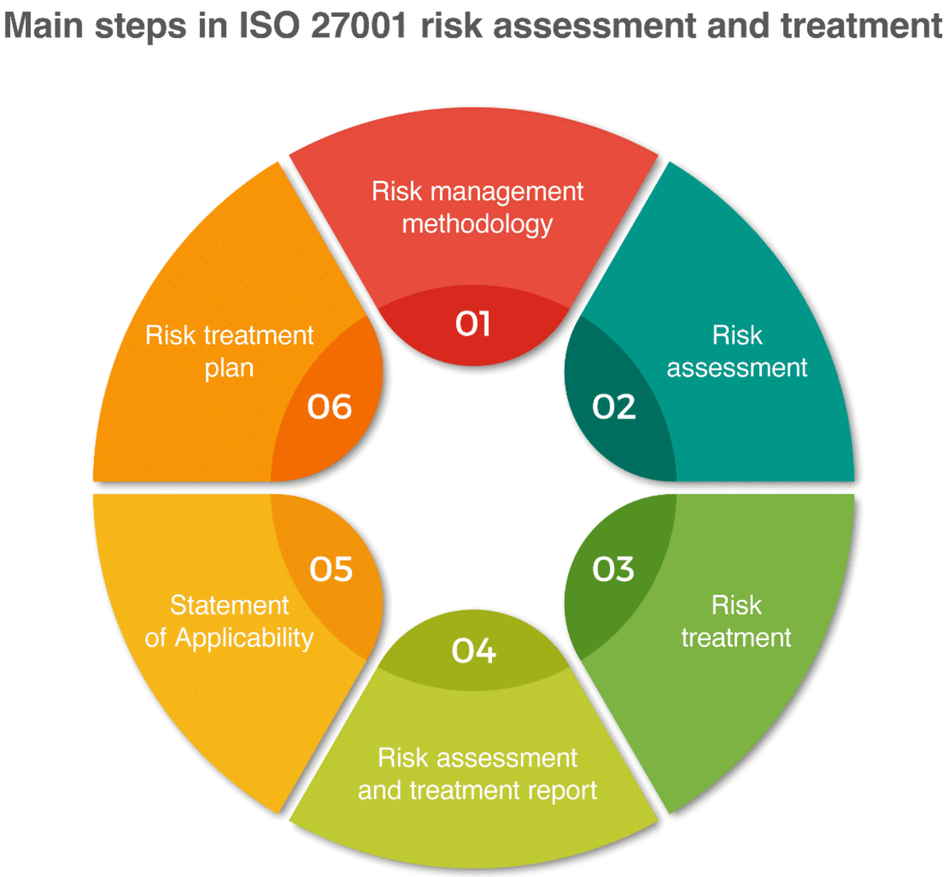
Risk assessment is one of the complex tasks in the implementation process. This stage requires identifying risks, probability, and impact and deciding the risk tolerance level. These things should be clearly defined. Otherwise, it gives inaccurate outputs.

This process contains two parts: risk assessment and risk treatment. The primary purpose is to implement security controls in order to mitigate or avoid potential security problems. This ISO 27001 specifies 114 security controls for Annex A.

Risk assessment and treatment contain several steps.

- Risk management methodology
- Risk assessment

- Risk treatment
- Risk assessment and treatment report
- Statement of Applicability
- Risk treatment plan


Main steps in ISO 27001 risk assessment and treatment
01
Risk management methodology
02
Risk assessment
03
Risk treatment
04
Risk assessment and treatment report
05
Statement of Applicability
06
Risk treatment plan

Perform the risk assessment & risk treatment

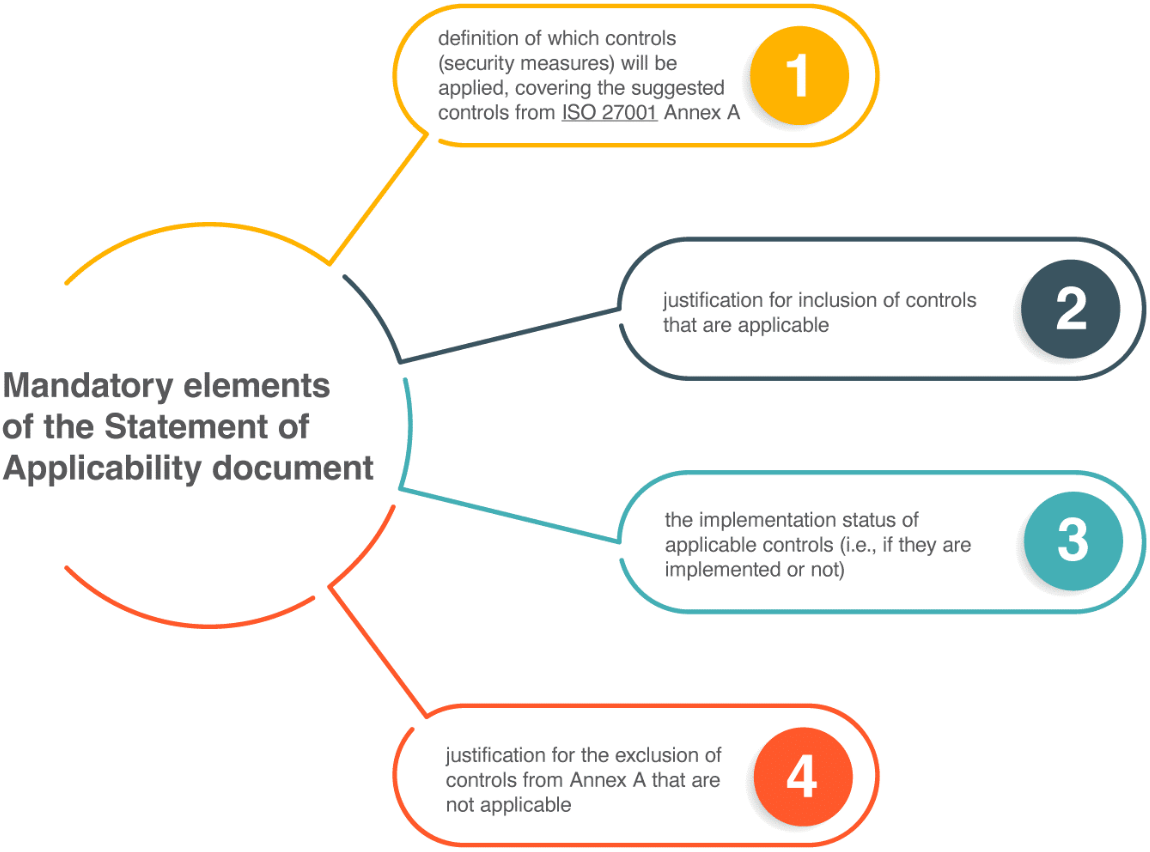
In this stage, the main task is to implement the security controls that came up with the risk treatment plan in the previous stage. it will take a couple of days to a couple of months. It depends on the scale of the organization, and we should manage that much effort carefully. At the end of this risk assessment part, we should get a clear idea of the internal and external threats to the organization's data.

In the risk treatment, we are focusing on the process of decreasing the risk level to the risk tolerance level. in other words, we have to mitigate the risks to the acceptable level.

For doing this, we can use security controls from Annex A.as an output has to be written a comprehensive report containing all the steps we have taken during this activity. Also, we have to get approval for the residual risk.

Write the Statement of Applicability

After completing the previous stage, it means you have completed the risk assessment and treatment then you can easily select the security controls that you exactly want from the ISO 27001 Annex A.the output of this stage we call SoA(Statement of Applicability). The purpose of creating this document is to list all the security controls, whether they are suitable or not, the reasons for that decisions, and how we can implement those controls in the organization. To implement the ISMS, we have to have the authorization of management, and it is necessary to hand over this SOA document


Mandatory elements of the Statement of Applicability document
1
definition of which controls (security measures) will be applied, covering the suggested controls from ISO 27001 Annex A
2
justification for inclusion of controls that are applicable
3
the implementation status of applicable controls (i.e., if they are implemented or not)
4
justification for the exclusion of controls from Annex A that are not applicable

Write the Risk Treatment Plan

Writing a risk treatment plan is the beginning of the process, which builds security controls to protect the organization's tangible and intangible information assets. After implementing the security controls, we need to verify those controls are effective.to measure it, we can check whether the staff can operate and work with those controls without negatively affecting performance. It is also better to develop a process to determine, review and maintain the skills required to obtain the ISMS objectives.

Define how to measure the effectiveness of controls

Most of the time, organizations with a management system do not give enough attention to this phase, but there is a special point in this phase. To ensure the employees are fulfilling the objectives, we have to measure their work. Therefore we have to have a proper way to measure the progress of objectives we have set on ISMS.this measurement needs to be done for all ISMS operations, including the security processes and controls.

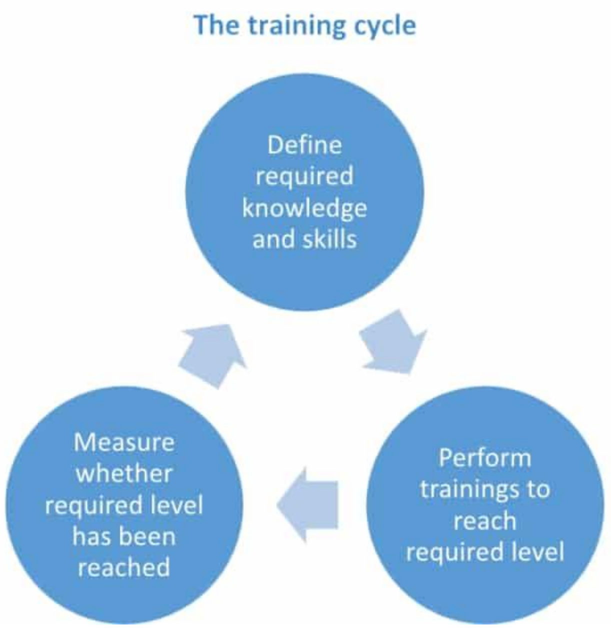
This is one of the most complex tasks in the iso27001 implementation process because, in this phase, we will introduce a new set of activities to the organization so we have to spend more time and effort on it. Hence we need new policies and procedures there will be resistance from the employees. This resistance can be decreased using training and awareness.

Implement the security controls

Implementing security controls can be harder than you think. This is where we must implement all the documents and technology needed, and with the new implementations, the current security process also needs to change.

Implement training and awareness programs

To maintain the proper functionality in our organizations, we must implement policies and procedures for our employees. Before implementing those, we have to inform employees about why we need policies and procedures and train them. With this training and awareness, we can successfully follow the ISO27001 standard.


The training cycle
Define required knowledge and skills
Perform trainings to reach required level
Measure whether required level has been reached

Operate the ISMS

This is where these principles of this standard will be a daily basis action of the organization. Certification auditors want to see logs and records, which include what activities was happened, so it is very important to keep records and logs when operating the ISMS.using records, we can keep track of what is happening and are all the employees achieving their desired objectives.

Monitor and measure the ISMS

When the ISMS is in operation, how do we know what is happening in the ISMS right now? What types of incidents are happening? Are all the procedures give the expected outputs? We can see these things by monitoring and measuring. Here, we have to check whether the ISMS is giving the necessary outputs to achieve our objectives by monitoring and measuring the system. When we are doing those processes, we know what is going wrong and can devise suitable preventive actions.

Internal audit

Most of the time, employees do something wrong and keep doing it because they don't know it is wrong. On the other hand, they don't want to find out about it or fix it. Being unaware can lead to existing problems which can damage the organization's information assets.to find out these kinds of problems we have to go among the employees. For that, we can conduct an internal audit.the purpose of this is to do things correctly and securely that won't lead to problems.

Management review

Hence the top management doesn't have to understand technical details; they don't need to know details such as configuring firewalls etc., but they definitely need to be aware of things happening with the ISMS. If employees do their tasks well and if the ISMS is able to gain the expected results, fulfilling the suggested requirements, etc.

Based on this, top management makes very important decisions such as approving a budget for security improvements, Business continuity, aligning security with business strategy, etc.

Corrective and preventive actions

In this stage, we are trying to fix everything which was incorrect before fixed, and all the threats to the organization's data are now prevented or controlled.so In iso27001, it requires systematically implementing controls. We need to find the root causes and solve them, and later we need to verify that those root causes are no longer there.

SECURITIES CONTROLS PER ISO 27001

Technical controls are provided by software, hardware, and firmware components that are introduced to the system in information systems. Backups and antiviral software, among others.

Organizations can implement controls by setting standards and expectations for personnel, equipment, software, and systems. the BYOD Policy and the Access Control Policy, for instance.

The company implements legal controls to ensure that its operations and behavior comply with and uphold all applicable laws, rules, contracts, and other similar legal documents. a service level agreement (SLA), a non-disclosure agreement (NDA), etc.

Equipment or technologies that physically interact with people and objects are frequently employed to apply physical controls. Locks, alarms, and CCTV cameras are examples of case.

Human resource controls are accomplished by providing people with the information, training, education, and/or experience they need to do their tasks safely. Internal ISO 27001 audits execute training and efficient security training as needed.

Who needs to do what in order to have ISO 27001 Information Security Management System up and running?

Although ISO 27001 does not dictate who must fill what positions, it is nonetheless necessary to delegate authority over some aspects of the ISMS to make sure it meshes with your company's values and practices and that information risks are being properly mitigated.

When discussing stakeholders, it is typical to distinguish between direct and indirect parties as well as primary, secondary, and even tertiary stakeholders. The ISMS can still have internal stakeholders despite this.

Primary Stakeholders

Because ISO 27001 is primarily concerned with the security of a company's management system, important stakeholders should be at the highest levels of management.

Primary stakeholders like yourself may include:

- Executive support and representation
- A senior executive with a risk management interest, such as a Chief Risk Officer (CRO) or Senior Information Risk Officer (SIRO), whose responsibilities include information risk.
- A manager or managers of the ISMS, using titles such as "Chief Information Security Officer" or "Information Security Manager" or others that make sense given the established conventions and terminology of your firm.
- A "lead implementer" or other resource who will be in charge of ISMS implementation.

Secondary Stakeholders

A secondary stakeholder is someone who will be accountable for a specific aspect of the ISMS. Experts from within the company, as well as any prospective outside partners or vendors, will be needed for this.

Possible secondary stakeholders include the following, depending on the scope and character of your business:

- Authorities in the fields of information and cybersecurity, as they relate to the work of your firm.
- Data security and technical support
- Definition of Human Resources
- Security in the form of a diagram; we may call this one "Facilities" or something
- Adherence to regulations and access to legal advice
- Verification from within
- The ISMS should work in tandem with the representatives of the business departments responsible for your important business processes. To do this, it will be crucial to include business managers at all levels of the firm.
- Supplier and partner representatives are granted access to sensitive information.

Top Management

ISO 27001 is essentially a business management system aimed at managing the security of an organization's information assets and lowering information risks to an acceptable level.

It is exceedingly unlikely that an ISMS rollout and operation will be successful, efficient, and effective without the backing of higher management.

ISO 27001 specifies some clauses that are the responsibility of upper management:

- Leadership and commitment – Top management commitment to the integration of information security within the organisation and its processes
- Assistance - Providing Adequate and Qualified ISMS Resources
- Management review - an assurance that the ISMS's efficacy will be reviewed at least once a year by the organization's upper management.

Information Security / Governance Staff

The ISMS's general administration and its components rely heavily on the information security and governance staff accountable for them.

These are the types of workers whose primary responsibility is ensuring the safety and proper management of sensitive data. But if your company is small, it's likely that this will be a single person who has a day job as well.

ISMS.online can deliver knowledge, competence, and confidence without the ISMS becoming a cumbersome overhead in the absence of expert-level resources.

IT department or supplier(s)

Because of the increasing reliance on and importance of IT systems, networks, and applications for information storage, processing, and transmission, it will be vital to ensure that the ISMS involves proper interaction with IT departments and/or suppliers from the start.

Your IT department or its vendors will most likely design, develop, implement, and manage the majority of the technological measures required to secure your information assets.The management of expectations and the division of labor for technical aspects of information and cybersecurity will have a substantial impact on the ISMS's performance.

Internal Auditor(s)

To ensure that the ISMS is able to reduce information risks to an acceptable level, a business must conduct internal audits, as is required by ISO 27001 and all other ISO management system standards.

Audits of the ISMS management clauses (4-10) and the Annex A controls are required at least once per year and must be performed during the certification period (3 years for UKAS accredited certifications).

You can't check your own work, therefore it's important to pick an internal auditor who has the experience and training to do a thorough job of checking everything over.

Whether you're looking for a simple guide to ISO 27001:2013 Internal Audits or a full Virtual Coach service, we have you covered.

Data Protection Officer

The majority of businesses have a Data Protection Officer whose job it is to guarantee that sensitive data, such as employee and customer records, is handled properly. Typically, such information will concern both an organization's employees and its customers.

As a result, implementing the required information and cybersecurity controls and standards to maintain such data is critical.

Other statutes and rules, such as the UK Data Protection Act (2018) and the General Data Protection Regulation (GDPR), do necessitate the appointment of a Data Protection Officer, although ISO 27001 does not. Furthermore, ISO 27001's controls over elements like as compliance clearly suggest the need for such a position.

References

- https://www.itgovernance.co.uk/blog/iso-27001-checklist-a-step-by-step-guide-to-implementation
- https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwj1mOCKq7z6AhXSHrcAHa_lBwsQFnoECAkQAQ&url=https%3A%2F%2Fwww.nqa.com%2Fmedialibraries%2FNQA%2FNQA-Media-Library%2FPDFs%2FNQA-ISO-27001-Implementation-Guide.pdf&usg=AOvVaw3wl35LlQCrak_Pj5hWrpmX
- https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwj1mOCKq7z6AhXSHrcAHa_lBwsQFnoECDYQAQ&url=https%3A%2F%2Fwww.bsigroup.com%2FDocuments%2Fiso-27001%2Fresources%2Fiso-iec-27001-implementation-guide-SG-web.pdf&usg=AOvVaw1FPKz8_bmYPx9xTDhRptdn
- https://sync-resource.com/iso-27001-implementation-guide/
- https://www.isaca.org/resources/isaca-journal/past-issues/2011/2011-planning-for-and-implementing-iso-27001
- https://www.upguard.com/blog/iso-27001-implementation-checklist