Journal of Economic Growth and Entrepreneurship JEGE
Spatial and entrepreneurial development studies laboratory

Year : 2023 Vol.6 No.2 pp:48-57

ISO 27001 :2018 AS A GOOD STRATEGIC TOOL TO IT RISK MANAGEMENT

[1]Bensaad Fatna

[1]DJILALLI LIYABES, (Algeria), bensaadnabila95@gmail.com.

ARTICLE INFO

Article history:
Received:13/04/2023
Accepted:24/05/2023
Online:27/05/2023

Keywords:
IT(information technology)
Risk Management
Information Security
ISO/IEC 27001:2018
JEL Code:M1,M15, M150, L6

ABSTRACT

ABSTRACT :

Despite the multiple uses of IT and the development of its methods of management, the internal and external changes constantly increase the risks of information technology, which requires organization to adopt tools and strategies to manage information risks and eliminate or reduce risks by the proposed control measures to achieve information security and achieve competitiveness.

The ISO/IEC 27001:2018 standard is one of the most important strategic tools to achieve information security and risk management as it helps organizations to improve that threats and vulnerabilities to the system are being taken seriously.

The establishment, maintenance and continuous update of an Information security management system (ISMS) provide a strong indication that a company is using a systematic approach for the identification, assessment and management of information security risks.

KeyWords : IT(information technology), Risk Management, Information Security, ISO/IEC 27001:2018

[*] Corresponding Author: Bensaad Fatna

1. Introduction:

Manage an organization requires a flow of manyinformations as physical resources , human resources and financalresources that are increasing and changing day after day. Organisational strategy needs to take account of this and individual systems need to be sensitive to it. So any organization need to understand the process of changing information by using technology and knowledge.

Information Technology (IT) is a fundamental force in reshaping organizations by applying investment in computing and communications to promote competitive advantage , customer service and other strategic benefits.So it represent basic components of competitive research and innovation strategies.

IT is development , design and supportof computer –based information systems . and with the creation of the Internet , security and protecting information has been a new function to ensure the long-term competitiveness and survival of corporations and entire economies. That's where International Standards like the ISO/IEC 27000 family come in, helping organizations manage the security of assets such as financial information, intellectual property, employee details or information entrusted to them by third parties.

ISO/IEC 27001 is the best-known standard in the family providing requirements for an information security management system (ISMS).It's an International Standard to which an organization can be certified, although certification is optional.

In this study, we show that ISO/IEC 27001 is an important tackle IT risk management because it helps organizations keep information assets secure and know how information technology decisions should be made and monitored, and how to deal with risks.

The purpose of this research is to answer a few questions: (1) "Which are the basic concepts related to IT risk management ?" (2) "What are the applications of the ISO/IEC 27001?" (3) ""How ISO/IEC 27001 helps organization to manage IT risks?".

The organisation of this paper is as follows: section 1 covers the concepts of the IT risk management . The ISO/IEC 27001 presents in section 2 . Section 3 presents the relationship between ISO/IEC 27001 and IT risk management.and conclusion.

2- concepts of IT Risk Management :

The business risk associated with the use, ownership, operation, involvement, influence and adoption of IT within an enterprise or organization. And to identify the IT Risk Management we must first give the definitions for basic concepts of IT , Risk and Management :

2-1- what is IT ?

IT is an abreviation of information tecknology and is an umbrella termthat covers a vast array of computer disciplines thatpermit organizations to manage their information resources (Bryan, Information Technology Management , 2018, p. 23).

U.S. Information Technology Association (ITA) defined IT is "*a technology which studies, designs, develops, implements, supports or manages computer-based information systems, especially computer software and hardware programs"*. So IT deals with issues such as using electronic computers and software to turn, store, protect, process, transfer and retrieve information securely. IT is a devise among many other devices which managers can use to solve problems (Chirani & Tirgar, 2013, p. 30).

IT enables managers to quickly control and coordinate the organization's performance with the management with a quick feedback and solidarity using the quick process of information taking in consideration of their six basic functions (see exhibit 2.1below).

Exhibit (2.1) : information technology'sfunctions

Input	Collecting data using various electronic devices
communication	Access and movement of data from place to place

processing	Transferring of data from one from to another
storage	Retaining data for future reference
retrieval	Ability to recall data when needed
output	Ability to transform data into a usable format specified by the user

Source : (Bryan, information technology management, 2018)

2-2- Risk Management ‘s definition :

- ***Management*** implies someone proactively, deliberately, explicitly and systematically identifying, assessing, evaluating and dealing with risks on an ongoing basis (coping with any changes), along with related governance aspects such as direction, control, authorization and resourcing of the process, risk treatments .

- ***Risk*** is the potential occurrence of events or incidents that materially harm the organization’s interests.

- ***Risk*** is the ‘net negative impact of the exercise of a vulnerability, considering both the probability and the impact of occurrence’ (calder, 2010, p. 50).

  Risk management is a central part of any organisation’s strategic management. It is the process whereby organizations methodically address the risks attaching to their activities with the goal of achieving sustained benefit within each activity and across the portfolio of all activities.

  Also A Risk Management effectively integrates the process for managing risk into an organization’s overall governance, strategy and planning, management, reporting processes, policies, values and culture. (university of Adelaide, Australia)

2-3- Risk Management’s objectives :

Risk Management involves considering all that information in order to determine the significance of various risks, which in turn drives priorities for the next stage. The organization’s tolerance for risks is reflecting corporate strategies and policies as well as broader cultural drivers and personal attitudes of the people engaged in risk management activities.forthis the Risk Management has many objectives that are helping to identify and to treat of these risks :

-It is to add maximum sustainable value to all the activities of the organisation.

-It marshals the understanding of the potential upside and downside of all those factors which can affect the organisation.

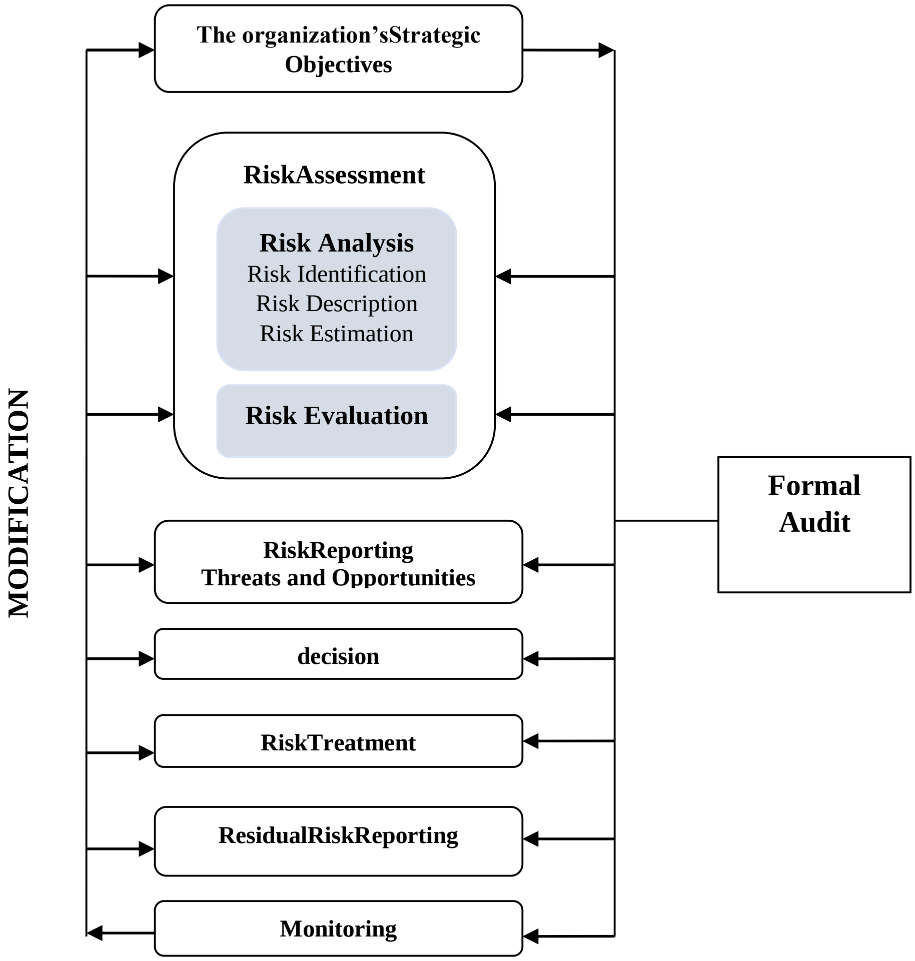
- It increases the probability of success, and reduces both the probability of failure and the uncertainty of achieving the organisation’s overall objectives.

- It supports accountability, performance measurement and reward, thus promoting operational efficiency at all levels.

2-4- The Risk Management Process :

The Risk managementProcess should be a continuous and developing which runs throughout the organisation’s strategy and the implementation of that strategy. It should address methodically all the risks surrounding the organisation’s activities past, present and in particular, future(see exhibit 2.2 below).

Exhibit (2.2) : The Risk Management Process



Source : (http://www.theirm.org/media/886056/ARMS_2002_IRM.pdf)

Risk management protects and adds value to the organisation and its stakeholders through supporting the organisation's objectives by:

• providing a framework for an organisation that enables future activity to take place in a consistent and controlled manner.

•improving decision making, planning and prioritisation by comprehensive and structured understanding of business activity, volatility and project opportunity/threat.

•contributing to more efficient use/allocation of capital and resources within the organisation..

• reducing volatility in the non essential areas of the business.

• protecting and enhancing assets and company image .

• developing and supporting people and the organisation's knowledge base .

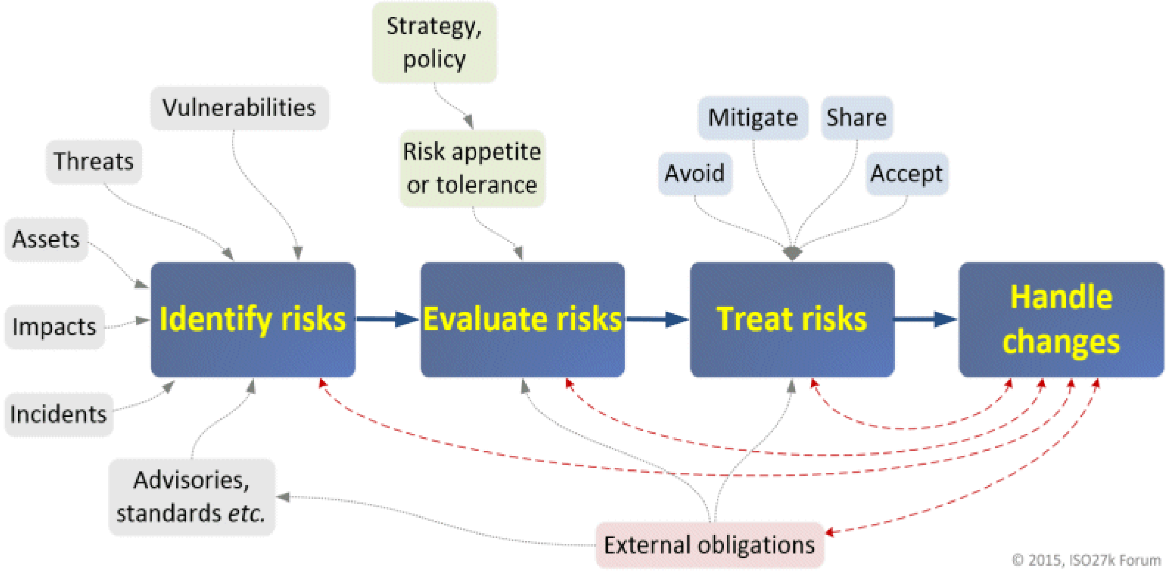
• optimising operational efficiency .

So after this illustration we can say that IT risk management can be considered a component of a wider enterprise risk management system, and we define itas :

“ *is the application of risk management methods to information technology in order to manage IT risk. ”*.

The figure(2.3) below discribes the process of how we can manage IT risk :

Figure(2.3) :Process of IT Risk Management



© 2015, ISO27k Forum

The measure of an IT risk can be determined as a product of threat, vulnerability and asset values.

The first stage of the process is to ***Identify potential information risks***. Several factors or information sources feed-in to the *Identify* step, including:

- *Vulnerabilities* are the inherent weaknesses within our facilities, technologies, processes (including information risk management itself!), people and relationships, some of which are not even recognized as such;
- *Threats* are the actors (insiders and outsiders) and natural events that might cause *incidents* if they acted on *vulnerabilities* causing *impacts*;
- *Assets* are, specifically, information assets, in particular valuable information content but also, to a lesser extent, the storage vessels, computer hardware *etc.* many of which are relatively cheap commodities these days*;*
- *Impacts* are the harmful effects or consequences of incidents and calamities affecting assets, damaging the organization and its business interests, and often third parties;
- *Incidents* range in scale from minor, trivial or inconsequential events up to calamities, disasters and outright catastrophes;
- *Advisories, standards etc.* refers to relevant warnings and advice put out by myriad organizations such as CERT, the FBI, ISO/IEC, journalists, technology vendors plus information risk and security professionals (our social network).

The Evaluate risks stage involves considering/assessing all that information in order to determine the significance of various risks, which in turn drives priorities for the next stage. The organization’s appetite or tolerance for risks is a major concern here, reflecting corporate strategies and policies as well as broader cultural drivers and personal attitudes of the people engaged in risk management activities.

Treat risks means avoiding, mitigating, sharing and/or accepting them. This stage involves both deciding what to do, and doing it (implementing the risk treatment decisions).

Handle changes might seem obvious but it is called out on the diagram due to its importance. Information risks are constantly in flux, partly as a result of the risk treatments, partly due to various other factors both within and without the organization.

And we've acknowledged that the organization often has to respond **to *External obligations*** such as compliance and market pressures or expectations. (http://www.iso27001security.com/html/risk_mgmt.html#IRM)

The identification, assessment and management of information security risks(manage IT risks) requires establishment, maintenance and continuous update of an Information Security Management System (ISMS) .

3- IT Risk Assessment :

3-1- what is ISO/ IEC 27001 :2018 ?

As global threats to information security increase in frequency and severity, and organizations of all sizes, types and sectors face increased exposure to fast-evolving cyber threats, there has never been a greater need to implement a robust information security management system (ISMS) that complies with the international standard, ISO 27001.

Where such data contains personal, financial or medical information, companies have both a moral and legal obligation to keep it safe from cybercriminals. That's where International Standards like the ISO/IEC 27000 family come in, helping organizations manage the security of assets such as financial information, intellectual property, employee details or information entrusted to them by third parties.

ISO/IEC 27001 is the best-known standard in the family providing requirements for an Information Security Management System (ISMS).It's an International Standard to which an organization can be certified, although certification is optional.

ISO/IEC 27001 :2018 is the standard that keep information assets secure , adopted by thousands of organizations across the world .It specifies the requirements for establishing , maintaining and continually improving an Information Security Management System. (Cooper, 2015, p. 25)

ISO 2700:2018 is :"The information security management system preserves the confidentiality, the integrity, and availability of information by applying a risk management process and gives confidence to interested parties that risks are adequately managed." (Kolcz, 2018, p. 15)

3-2- The Advantages of ISO 27001:2018 :

ISO/IEC 27001:2018 are generic and are intended to be applicable to all organizations, regardless of type, size or nature. And because its approach is based on regular risk assessments, ISO 27001 can helpto :

- specify the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization.

- Improve organisation'scybersecurity posture and business efficiency while ensuring meet legal and regulatory data protection obligations.

- Achieve independently audited certification to the Standard to demonstrate their information security credentials to clients, stakeholders and regulators.

- Identify appropriate controls for providing the mission-essential security capabilities.

- Includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization.

- Take a flexible, risk driven approach.

- Focuse on continual improvement and help the organization keep ahead of changes both within and outside the organization.

3-3- Family of ISO 27001 :

The family of ISO27001 provides best practice recommendation on information security management , risks and controls :

- **ISO/IEC 27000**, *Information security management systems — Overview and vocabulary*
- **ISO/IEC 27001**, *Information security management systems Requirements*
- **ISO/IEC 27002**, *Code of practice for information security management*
- **ISO/IEC 27003**, *Information security management system implementation guidance*
- **ISO/IEC 27004**, *Information security management — Measurement*
- **ISO/IEC 27005**, *Information security risk management*
- **ISO/IEC 27006**, *Requirements for bodies providing audit and certification of information security management systems*
- **ISO/IEC 27007**, *Guidelines for information security management systems auditing.*
- **ISO/IEC 27011**, *Information security management guidelines for telecommunications organizations basedon ISO/IEC 27002*

3-4- TheISO 27001 :2018 certification process :

There are three phases as follow (Riad, 2018, p. 35):

Phase 1 : Before external audit :

1- Implementation of ISMS : Complete of implementation cycle of ISMS, Including mandatory Requirements and optional Controls .

*2- Conduct Internal Audit and review result by top management :*The organization conduct periodic internal audits to ensure the ISMS incorporates adequate controls which operate effectively and review it by Top Management .

3- Selection of a Certification body : Organization select a Certification body “ BSI , DNV, SGS “ to conduct External audit activity and Certified Organization ISMS Program.

Phase II : External Audit :

4- Stage 1 : Audit Conducted off or on site to determine if your ISMS system has met the requirements of the standard and is capable of being audited.

*5- Stage 2 :*Audit Conduct on site to audit the effectiveness of the ISMS system. Stage 1 and Stage 2 must be completed to become ISMS certified.

Phase III : Following the audit :

6- Confirmation of Registration Lead Auditor recommend to Certification Manager of Certification Body that Organization are certified : The Certification Manager will review Organization file to ensure that the recommendation has been made in an impartial, fair and competent manner. Upon completion of the above Organization will be officially certified to ISO/IEC 27001:2018 .

7. Continual improvement and Surveillance audits : Conduct Internal Audit Activity by Organization and Certification body auditor will conduct surveillance audit for organization every 6 months or 12 months for next three years after organization achieve ISO/IEC 27001:2013 certification.

4- The role of ISO/IEC 27001:2018 in IT risk management:

ISO/IEC 27001:2018 made a number of improvements to the security controls listed in Annex A to ensure that the standard remains current and is able to deal with today’s IT risks, namely identity theft, risks related to mobile devices and other online vulnerabilities.ISO 27001 sets out the requirement very clearly: ‘review risk assessments at planned intervals and review the residual risks and the identified acceptable levels of risks’ taking into account changes in the business environment, to the organisation, to the risks it faces, to the incidents it experiences, to regulatory changes and in the light of the effectiveness of the controls.

So ISO27001 :2018 help the organizations to improve IT risk management and compliance activities by:

- identify risk areas and recommend improvement options.
- Utilising proven methodologies and industry knowledge to identify security measures (people, processes and technology) and process standardisation opportunities.
- Assessing current compliance monitoring capabilities against established standards and policies to identify compliance gaps and continuous improvement opportunities.

4-1- Annex A Control Objective and Controls List of ISMS :

Annex A consist the best control area of it risks as following (Riad, 2018, p. 40):

14 Control Area : Core topic areas that Covered Most Aspects of Information Security 34 Control Objective : Objectives of Control
114 Control : Applicable Controls to be Implemented on ISMS Program
A.5: Information Security Policies : Manage and Update of Organization Information Security Policies.
A.6: Organization of Information Security : Manage of Organization Information including: Identified Role and Responsibilities, Segregation of Duties, Mobile Devices and teleworking.
A.7: Human resources security : Manage of Organization Human Resource including: During, prior Employment Relationship.
A.8: Asset management :Manage of Organization Assets .
A.9: Access Control :Manage and Control Access of Organization Information.
A.10: Cryptographic : Control of Using Cryptographic inside Organization .
A.11: Physical and environmental Security :Manage and Control of Organization Physical and environmental Access .
A.12: Operations security : Manage and control all Operation security including : Operational Procedure and Responsibilities , logging and Monitoring , Technical vulnerability management and information systems audit.
A.13: Communications Security : Manage and control Organization Communication Security including : Network security management and information transfer Controls ***A.14: System acquisition, development, and maintenance :***Manage and control System Development Cycle Including: identified and enforce security requirements , Secure of development system.
A.15: Supplier Relationship : Manager suppliers relationship including : apply information security for supplier relationship and service delivery management.
A.16: Information Security Incident management :Manage information security incident.
A.17: Information Security aspects of Business Continuity : Management Manage information security Continuity and Redundancies.
A.18: Compliance : Manage organization compliance with legal and contractual requirements .

4-2- Treatement IT risk by the implementation of ISO27001 :2018 :

The standard ISO27001 :2018 can help organizations to treat IT risk and to protect themselves from the growing diversity of security attacks that business is facing today. by this operations :

1- Ensuring management support: It is very important that management supports the project. Without this support, implementing the standard (or any standard for that matter) would be doomed from the start. Management commitment should ensure that there are enough resources available to manage, develop, maintain and implement the ISMS.

2-Defining and performing Risk Assessment: This is the most crucial stage of the project. It is important to choose a risk assessment method, for example SWOT and PEST analysis, to help identify the vulnerabilities and threats that may have an effect on the specific business, and to define the acceptable level of risk. If these are not clearly defined from the outset, the resulting processes will also be incorrect. The focus is to be able to get a comprehensive picture of the dangers facing the security of the organisation’s information.

3- Processing the Risk Treatment: The purpose is to decrease the risks identified in the previous step to an, as much as possible, acceptable level.

4- Documenting the Risk Treatment Plan: The purpose of the Risk Treatment Plan is to take each of the applicable controls identified in the Statement of Applicability and define how they are to be implemented. This includes identifying the control owner and the frequency of the control, and adescription of the implementation method.

5- Implementing the controls: This is the part where the applicable controls from Annex A have to be implemented. In this step, it is important to first define how to measure the effectiveness of thecontrols. Implementing new controls, would mean implementing new technologies and behaviours in the organisation. It is often the case that resistance to change by the individuals responsible for the control is likely and this is why the next point (training and awareness) is crucial for avoiding this risk.

6- Implementing training and awareness programs: employees need to be aware of the new policies and procedures to be implemented. Training and awareness programs should be given periodically to employees so they are aware of the risks of non-compliance. There is no technology that can prevent someone falling for increasingly sophisticated social engineering attacks. Hence the necessity to have proper awareness is of utmost importance.

7- Monitoring the implementation of the ISMS: The ISO 27001 standard follows a Plan-Do-Check-Act (PDCA) cycle. In order for the ISMS implementation to be effective, it needs to be reviewed by management as part of the internal audit process in periodic, planned intervals. This should also include changes / improvements to policies, procedures, controls and staffing decisions. The results of audits and periodic reviews are documented, maintained and any recommendations actioned.

5- Conclusion :

The IT risk management assists the effective and efficient operation of the organisation by identifying those risks which require attention by management. Organizations will need to prioritise risk control actions in terms of their potential to benefit the organisation.

Once your ISMS has been certified to the Standard ISO/IEC 27001 :2018 , the organization can insist that contractors and suppliers also achieve certification, ensuring that all third parties that have legitimate access to your information and systems also maintain suitable levels of security. This is especially important for General Data Protection Regulation (GDPR) compliance, as it will be liable as a data controller if any third-party data processor suffers a breach.

Also we think that certification is merely advisable, not compulsory, and it will still benefit if we simply want to implement the best practice set out in the Standard –we just won’t have the certification to demonstrate we credentials.

References :

1. Bryan, V. (2018). *Information Technology Management .*
2. Kolcz, M. (2018). *An Information Security Management System.*
3. Bryan, V. (2018, 4 10). *information technology management*. Retrieved 1 30, 2021, from www.faculty.wiu.edu.
4. calder, A. (2010). information security risk management for ISO27001/ISO27002. *IT governance publishing* .
5. Chirani, E., & Tirgar, S. M. (2013). Information Technology’s Role In Organizations’ Performance. *Kuwait Chapter of Arabian Journal of Business and Management Review Vol. 3, No.1.* , p17.
6. Cooper, N. (2015). *The benefits of ISO 27001, Tchnical Whitepaper CAPITA.* united kingdom.
7. *http://www.iso27001security.com/html/risk_mgmt.html#IRM*. (n.d.). Retrieved 2 10, 2021
8. *http://www.theirm.org/media/886056/ARMS_2002_IRM.pdf*. (n.d.). Retrieved 1 30, 2021
9. Riad, A. (2018). *ISO/IEC 27001.*
10. university of Adelaide, Australia. (n.d.). *http://www. adelaide.edu.au/legalandrisk/risk_management_handbook.pdf*. Retrieved 1 30, 2021