Social Lens

Innovative

Article

Cybersecurity Compliance Frameworks- a pragmatic view with an IT outsourcing company case study

Rachel John Robinson

Faculty of IT, IU University of Applied Sciences, Berlin 10247, Germany
* Correspondence: info@rachel-johnrobinson.com

Abstract: This paper practically deals with the theoretical base drawn from the standards and rules posed by various international bodies in terms of information security. To start with, this paper defines what security framework is applied practically to an IT outsourcing company based in UK named Cyberfox. Hence the relevant laws of the land are analyzed like NIS (The Network and Information Systems Regulations 2018) and GDPR (General Data Protection Regulations). By doing so, a framework in cyber security is tried to be fit in for this company called Cyberfox. By careful analysis and critical evaluation ofthe pros and cons of such companies' framework and whether it is a workable model is discussed in the first half of the paper. The second half of the paper basically details the NIST (National Institute of Standards & Technology) cyber security framework and the Internal Organization of Standardization protocols in respect to 4 specific standards like Information Security Management systems (ISMS) measurement (ISO 27004), Information security risk management (ISO 27005), Requirements of bodies providing audit services (ISO 27006) and Governance of Information Security (ISO 27014). All these four are studied for their merits and demerits for practical purposes.

Keywords: NIST Cyber security framework; NIS; GDPR; Cyberfox; critical evaluation; ISO 27004; ISO 27005; ISO 27006; ISO 27014

1. Introduction

Cyber security is an impending and a very vogue concept of the internet world today. Every business house which deals with information and security have no option of overlooking cyber security in the organization. Understanding the importance of the presence of cyber security in the organizations today, National Institute of Standards & Technology (NIST)of the US Department of Commerce has developed a voluntary framework of guidelines, best practices and rules for the companies of today's world to adopt. This paper is going to critically analyze that framework in a company situation called Cyberfox (a UK based IT outsourcing company) and what implementation techniques of cyber security it follows and what are its combined pros and cons. No only this, but also the second important aspect of this paper being the security standardization standards, commonly known as ISO's (International Organization for Standardization). In this paper its standards on Information Security Management systems (ISMS) measurement (ISO 27004), Information security risk management (ISO 27005), Requirements of bodies providing audit services (ISO 27006) and governance of Information security (ISO 27014) are dealt in detail analysis.

Current study was designed to identify the security landscape of the Cyberfox company, changes in the security frameworks and study the benefits and challenges and the strategic security management techniques for maintaining economic and long-term viability as sustainability in businesses.

2. Method Overview - Cyberfox Cyber Security

Current research will describe a practical situation of a company based in UK who is desirous of implementing cyber security framework in its organization. No framework in the real world can provide one-size-fits all approach to any company. The impending framework is always adopted in customization to the market and stakeholders' need of the company and gets implemented. Such understanding and implementation start with the basic understanding of the underlying base framework of NIST.

The NIST Cloud computing definition is adopted from the source as "cloud computing is a model for enabling convenient, on- demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly

Citation: Rachel John Robinson. 2024. Cybersecurity Compliance Frameworks- a pragmatic view with an IT outsourcing company case study. *Social Lens* 1, 15-25. https://doi.org/10.69971/sl.1.1.2024.6

provisioned and released with minimal management effort or service provider interaction." (Niekerk and Jacob 2015). With this definition, it is imperative to understand the cloud computing working mechanism and its major players. There are four major players in the cloud computing world like the service/ cloud provider, the consumer, the intermediary/ broker and the cloud auditor. In terms of business, only the first three make the major contribution but to ensure consistent continuity of the service the role of the last player is important. Each of the players in the cloud architecture model plays a role in the service management, resource provision, and controls abstraction in the layer of service provider. While the service intermediary/ broker has the service arbitrage and aggregation services to be provided, the consumer who gets all this plays the role of the taker of services and maintains the business relationship. The cloud auditor who performs different kind of security, performance and privacy impact audits to ensure the integrity of the services provided (Shackelford 2015).

3. Cyberfox- The Company & Its Implementation Plan

This Cyberfox is an IT outsourcing company based in London-UK, which started working in 2018. IT outsourcing falls under the digital service providers (DSP) category under The Network and Information Systems Regulations 2018 ("Regulations") of UK, has an imperative that the company had to follow the law of the land first. As per the security requirements of the law of the land, "both OESs (operators of essential services) and DSPs (digital service providers) must take appropriate and proportionate technical and organizational measures to manage risks posed to the security of the network and information systems. These measures taken must, having regard to the state of the art, ensure a level of security of network and information systems appropriate to the risk posed (again, language which will be familiar to those acquainted with the GDPR)." (DDA, 2017).

It is construed that the company Cyberfox is EU based operational company, where not just it is governed by the NIST 2018 UK laws but also has to comply with the General Data Protection Regulation (GDPR). This is because UK has to follow GDPR rules with effect from 2018. As the company operates off shore, it is important that the data protection and data privacy laws of the land of its operations are complied with to have a strong cyber security base. Being a new multi boarder company, its Information Technology Manager had to do a cumbersome task of implementing a proper cyber security framework for the company, so that Cyberfox in its cyber security maturity will move from the partial tier to the adaptive tier (Mani 2022). Cyberfox being a relatively a year-old company, the implementation of cyber security framework in this company is quite a task, as the process/ function identification, and categorization and sub-categorization of activities of the functions have to be done to achieve the outcomes proposed by the stakeholders of the company (Mani 2022).

As in NIST framework the cyber security work starts with first defining the functions and categories. For this, three levels of characters are involved in the organization as shown in Figure 1.

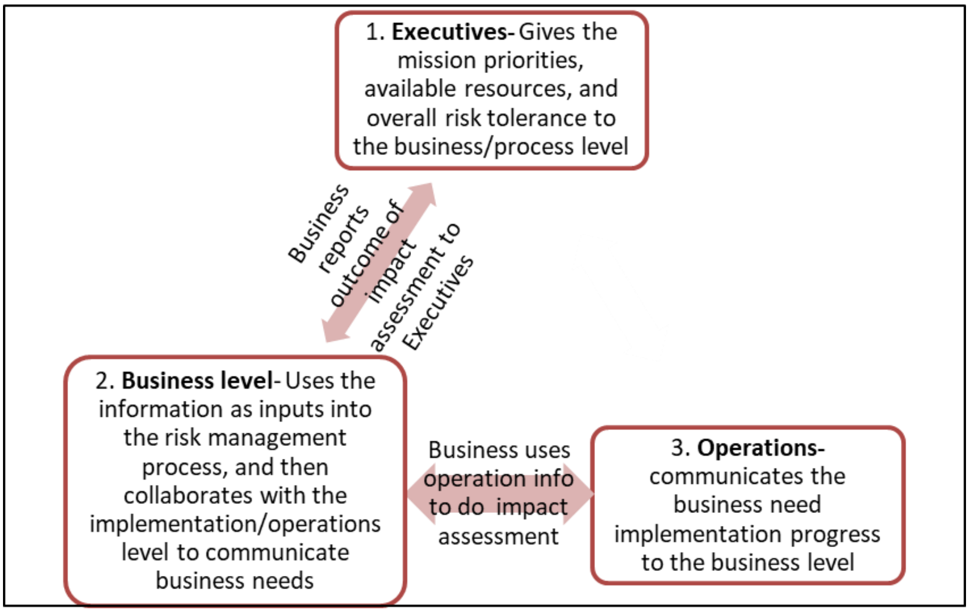

1. **Executives**- Gives the mission priorities, available resources, and overall risk tolerance to the business/process level
Business reports outcome of impact assessment to Executives
2. **Business level**- Uses the information as inputs into the risk management process, and then collaborates with the implementation/operations level to communicate business needs
Business uses operation info to do impact assessment
3. **Operations**- communicates the business need implementation progress to the business level

Figure 1. Implementation roles.

IT Manager of the organization had to recommend the company to properly segregate roles like executives, business level or process level people and the ultimate operations team. Each of their roles and responsibilities should be properly laid down and defined with segregation of duty. This has to be ensured and monitored on a timely basis, because as the structure stays in place so will the processes and operations of the organization. Once this topology is achieved, the employees are supposed to align the five main functions of the framework (Clark and Ward 2018). Based on the implementation plan by the IT manager (Figure 2), after considering the very fact that the organization is a relatively new, the processes had to be started out from first with a clear delineation of work and processes.

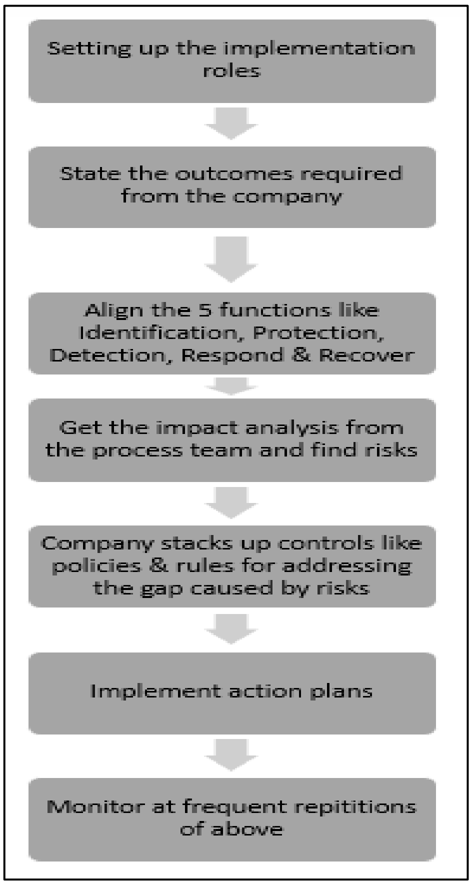

Setting up the implementation roles
State the outcomes required from the company
Align the 5 functions like Identification, Protection, Detection, Respond & Recover
Get the impact analysis from the process team and find risks
Company stacks up controls like policies & rules for addressing the gap caused by risks
Implement action plans
Monitor at frequent repititions of above

Figure 2. Implementation Plan.

4. Assessment of the Cyberfox Implementation Plan

Critical analysis of the plan implemented for Cyberfox, suggests lapses in the implementation plan. Though the plan had been brought out well in alignment with the NIST cyber security framework, missing (Amy 2018) elements like non-communication of results to the stakeholders, absence of orientation or staff training component in the structure, not mentioning the frequency timeline of monitoring the functions and gaps, role-based implementation steps not construed from the presented flow chart, and no pointers on access control stated are worth mentioning.

Implementing such a framework in a relatively new organization which has cross boarder operations are (Amy 2018) has various advantages. Setting of proper topologies within the organization as a starting point shows the broad eye view to have a lasting significant impact on the organization's capabilities. Immediately defining the needs of the organization, in line with the stakeholder's expectation portrays the business commitment of the company. Aligning the key five functions of the NIST framework into Cyberfox operations gets the into various model approaches of the business and never wanted to leave even one stone unturned in the process. Impact analysis of these functions and identifying the gaps and risks, makes the organization risk mature in the process as they strive for excellence. The manager had rightly incorporated the same into the structure.

It can be summarized that the model proposed is realistic and in time vogue recommendations to the organisation in line with the laws of the land and boarders. It would be even more realistic and wholesome in nature if the IT Manager of Cyberfox can consider the disadvantages pointed out and incorporate them as action plans into the company framework, it may work and definitely meet up to the expectation of the stakeholders of the company (Dutch Accreditation Council. 2015).

5. Framework evaluations

The type of frameworks in the security and cloud computing parlance with its critical analysis to understand on how the cyber frameworks dwell in today's application realm and practice in the industry is outlined below.

5.1 NIST Cyber Security Framework

Framework for cyber security by NIST started in 2014 when the US introduced The Cybersecurity Enhancement Act of 2014. Continuing this Act, the role of NIST was updated to frame Framework Version 1.0 (2014). This framework was revisited in 2018 to provide the Framework Version 1.1 (2018). From the information gathered (ISO/IEC 27006:2015), "The Framework provides a common taxonomy and mechanism for organizations to describe their current cyber security posture; describes their target state for cyber security; identifies and prioritizes opportunities for improvement within the context of a continuous and repeatable process; assesses progress toward the target state; and communicates among internal and external stakeholders about cyber security risk."

The framework suggests a set of activities to be done to achieve a group of outcomes. These outcomes are the requirements defined by the organisation's stakeholders and customers. The activities carried out are called as core which comprises of paramount functions, categories, sub categories and informative references. The core functions listed out in the NIST 2018 Framework version 1.1 is in Figure 3.

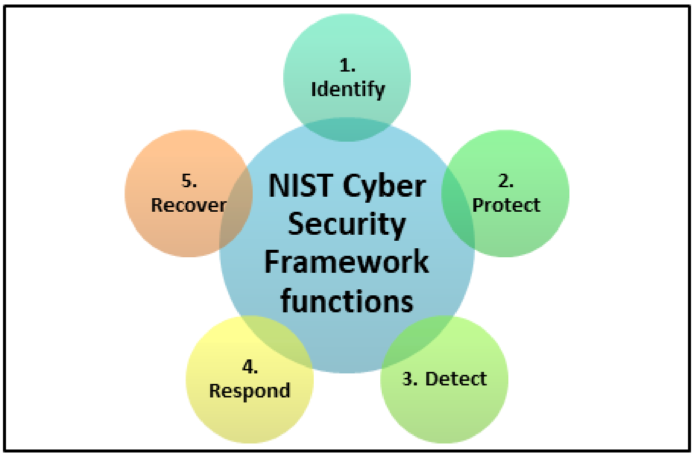
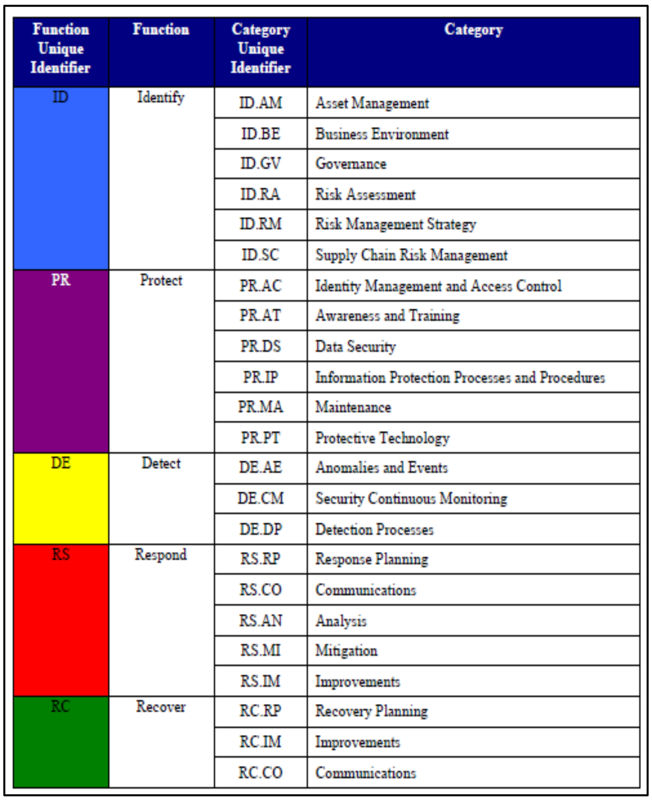


Figure 3. NIST cyber security functions.

It is mainly the responsibility of the management to undertake this. Categories are those which are closely tied with the function, e.g., asset management under protect. Sub categories are even more specific in nature which enable the outcome achievement, e.g., different assets being catalogued. Informative references are the set of rules and guidelines which are illustrative for outcome achievement. (ISO/IEC 27006:2015). It's well depicted in the appendix column of the framework in Figure 4. Figure 4 shows the main functions of the framework and how it is categorised and sub categorised (if necessary) as per the organisation needs. These act as pointers to the framework core to complement existing business and cyber security operations.

Based on how well the organisation aligns with the procedures and implementation, the framework had come up with something called implementation tiers. Tiers are a tool between cyber security risk management and operational risk management (ISO/IEC 27004:2016). Higher the NIST tier level of the organisation higher is the sophistication and maturity of the organisation in cyber security (Figure 5).



Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Identity Management and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Figure 4. Cyber security Framework (Version 1.1) Identifiers (ISO/IEC 27004:2016).

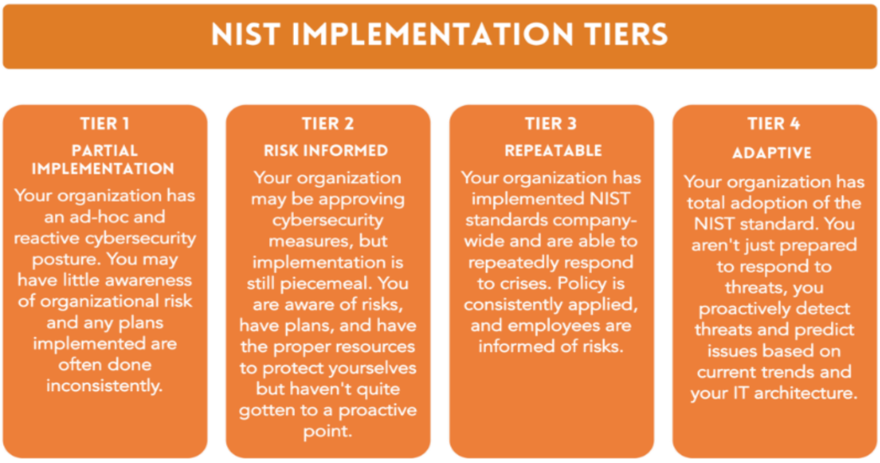

NIST IMPLEMENTATION TIERS
TIER 1
PARTIAL IMPLEMENTATION
Your organization has an ad-hoc and reactive cybersecurity posture. You may have little awareness of organizational risk and any plans implemented are often done inconsistently.
TIER 2
RISK INFORMED
Your organization may be approving cybersecurity measures, but implementation is still piecemeal. You are aware of risks, have plans, and have the proper resources to protect yourselves but haven't quite gotten to a proactive point.
TIER 3
REPEATABLE
Your organization has implemented NIST standards company-wide and are able to repeatedly respond to crises. Policy is consistently applied, and employees are informed of risks.
TIER 4
ADAPTIVE
Your organization has total adoption of the NIST standard. You aren't just prepared to respond to threats, you proactively detect threats and predict issues based on current trends and your IT architecture.

Figure 5. Risk Framework Implementation Tiers (Faris et al. 2014).

5.2 ISO 27004 Analysis

Being the branch head of ISO 27001, it mainly focusses on the ISMS (Information Security Management System) requirements and its implementation in the organization. It does not impose any new restrictions over and above the set ISO 27001 series. It only facilitates its implementation in terms of monitoring and measurement of ISMS, which in turn will help in corporate governance, management, operational effectiveness and continuous improvement. To understand the standard in a lucid manner, a parallel is drawn between the parent standard and the sub-standard (ISO 27004) as given in the Figure 6.

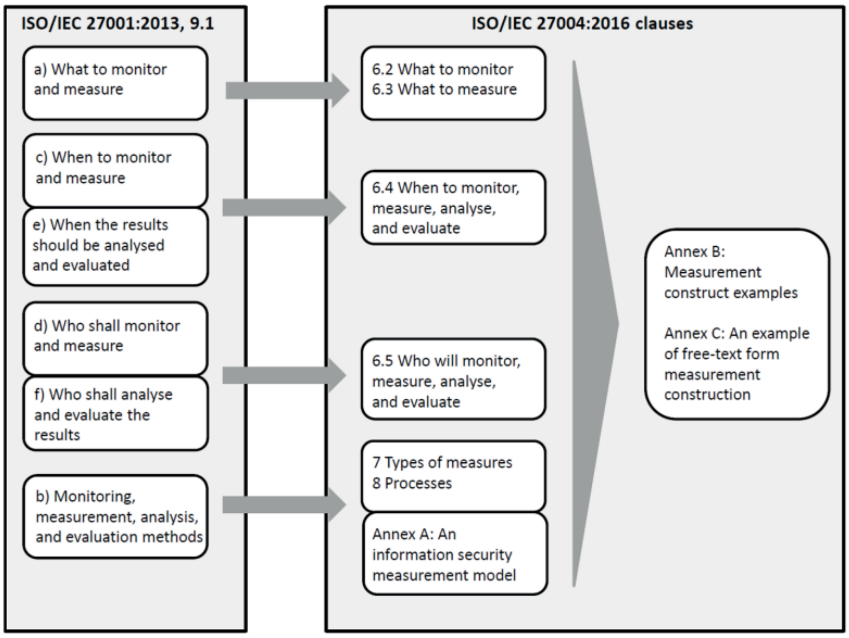

ISO/IEC 27001:2013, 9.1
a) What to monitor and measure
c) When to monitor and measure
e) When the results should be analysed and evaluated
d) Who shall monitor and measure
f) Who shall analyse and evaluate the results
b) Monitoring, measurement, analysis, and evaluation methods
ISO/IEC 27004:2016 clauses
6.2 What to monitor
6.3 What to measure
6.4 When to monitor, measure, analyse, and evaluate
6.5 Who will monitor, measure, analyse, and evaluate
7 Types of measures
8 Processes
Annex A: An information security measurement model
Annex B: Measurement construct examples
Annex C: An example of free-text form measurement construction

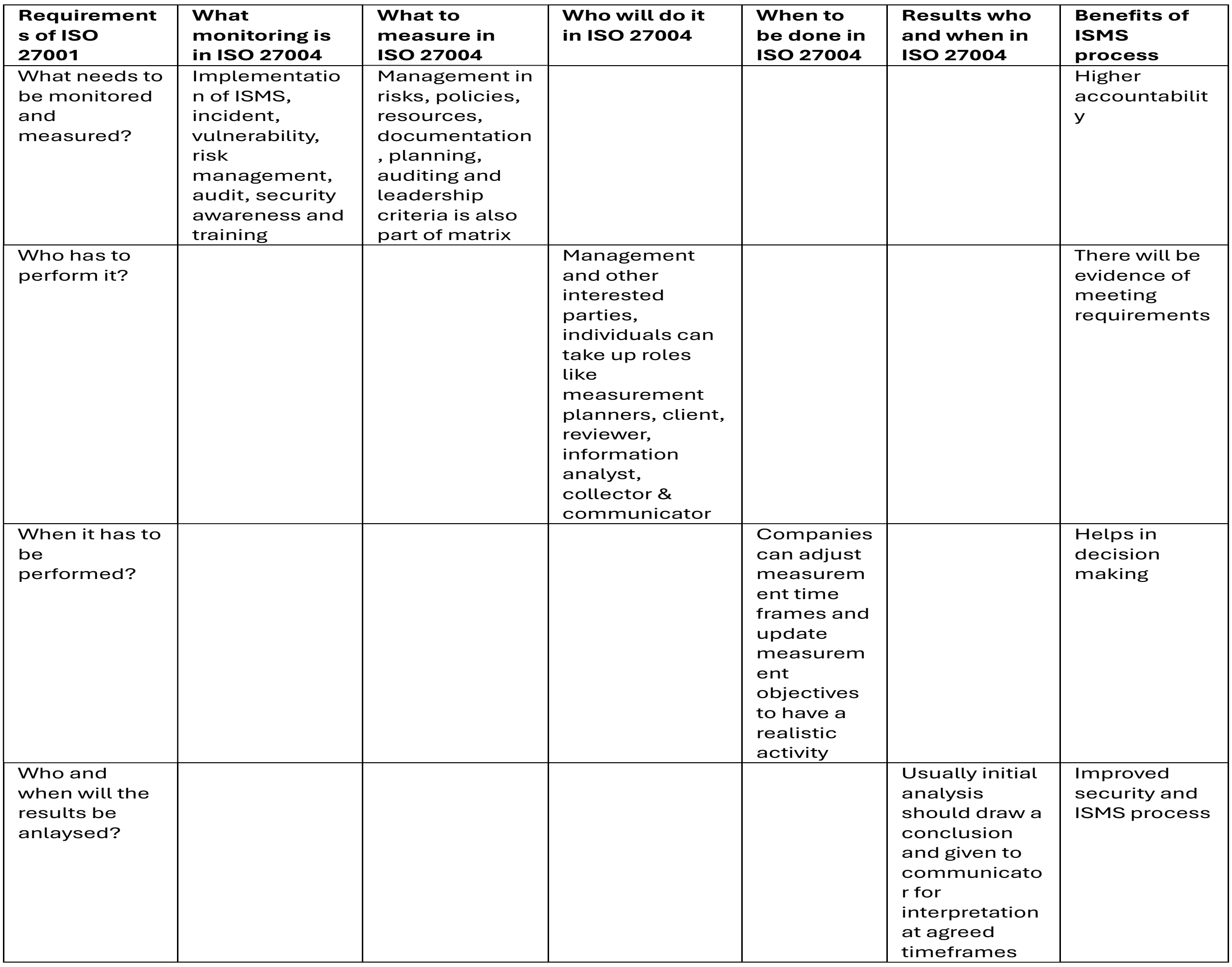
Figure 6. Mapping of ISO 27004 to ISO 27001.

It can be inferred that the needs of ISO 27001 being imposed in ISO 27004 in a more structured way are clear enough to provide results for decision making to the management (Cloud Security Alliance 2019). Comparison between ISO 27001 & 27004 requirements (Figure 7), indicates that previous standards criteria are met by ISO 27004. However, a key problem is that measurement timeline is not specific to the situations and are not definable. Hence may alter the intended results within the timeframe as expected in the standards (Shiroya and Rosinson 2023).

5.3 ISO 27005 Analysis

To support the concept of ISMS of ISO 27001, the concept of risk management was introduced back in 2008 as a first edition of ISO 27005. This standard deals with risk management principles and indicates how satisfactorily ISMS can be deployed in the organisation using such approach. “ISO/IEC 27005 is based on the generic ISO/IEC 31000 risk management-principles and guidelines but tailored to, and aimed at, information security risk management. The ISO/IEC 27005 standard also closely correlates with the US National Institute of Standards and Technology (NIST) SP 800-39 Managing Information Security Risk, which was developed for the USA. ISO/IEC 27005:2011 does not cover organizational risk, whereas NIST SP 800-39 does (NIST 2018).”

Based on the correlation drawn above between the standards the suggested model of risk management process is given below in Figure 8.



Requirements of ISO 27001	What monitoring is in ISO 27004	What to measure in ISO 27004	Who will do it in ISO 27004	When to be done in ISO 27004	Results who and when in ISO 27004	Benefits of ISMS process
What needs to be monitored and measured?	Implementation of ISMS, incident, vulnerability, risk management, audit, security awareness and training	Management in risks, policies, resources, documentation , planning, auditing and leadership criteria is also part of matrix				Higher accountability
Who has to perform it?			Management and other interested parties, individuals can take up roles like measurement planners, client, reviewer, information analyst, collector & communicator			There will be evidence of meeting requirements
When it has to be performed?				Companies can adjust measurement time frames and update measurement objectives to have a realistic activity		Helps in decision making
Who and when will the results be anlaysed?					Usually initial analysis should draw a conclusion and given to communicator for interpretation at agreed timeframes	Improved security and ISMS process

Figure 7. ISO 27004 to ISO 27001 Evaluation.

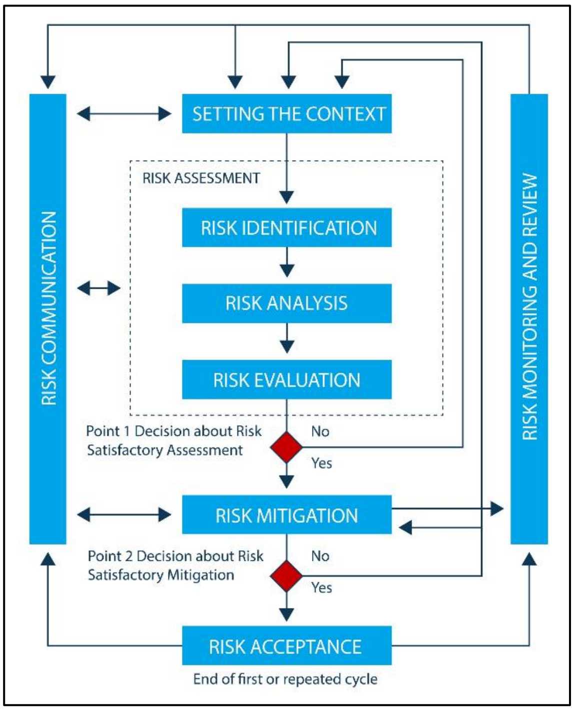
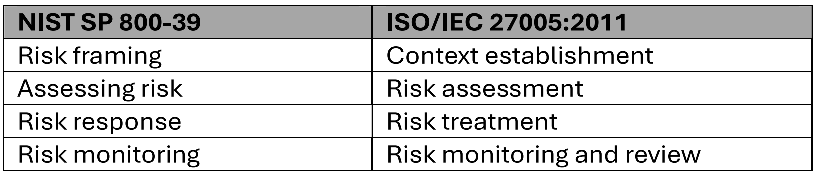

SETTING THE CONTEXT
RISK ASSESSMENT
RISK IDENTIFICATION
RISK ANALYSIS
RISK EVALUATION
Point 1 Decision about Risk Satisfactory Assessment
No
Yes
RISK MITIGATION
Point 2 Decision about Risk Satisfactory Mitigation
No
Yes
RISK ACCEPTANCE
End of first or repeated cycle
RISK COMMUNICATION
RISK MONITORING AND REVIEW

Figure 8. ISO/IEC 27005:2011 Risk management process.

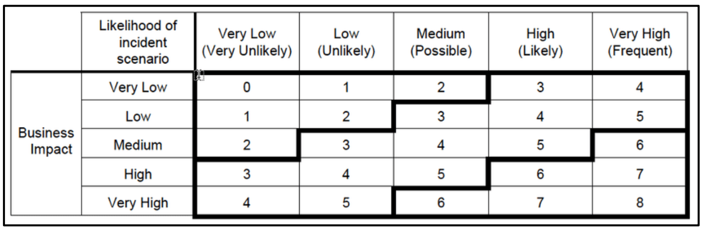
The process starts with the identification of risks in the organisation, their analysis, and evaluation followed by treatment. Based on the organisation structure and the risk acceptance or absorption criteria, the organisations risks can be mitigated by accepting, mitigating, transferring, avoiding or by ignoring the minimal risks. But to enable this constant communication and monitoring of results is paramount. [14] A parallel is drawn between the previous similar standard of ISO 27005: 2011 like NIST SP (National Institute of Standards and Technology Special Publication) 800-39 to comprehend it. (ISO/IEC 27005:2011) [15] The main objectives of both the standard are compared to see the crux of the intended framework stays in place (Figure 9).



NIST SP 800-39	ISO/IEC 27005:2011
Risk framing	Context establishment
Assessing risk	Risk assessment
Risk response	Risk treatment
Risk monitoring	Risk monitoring and review

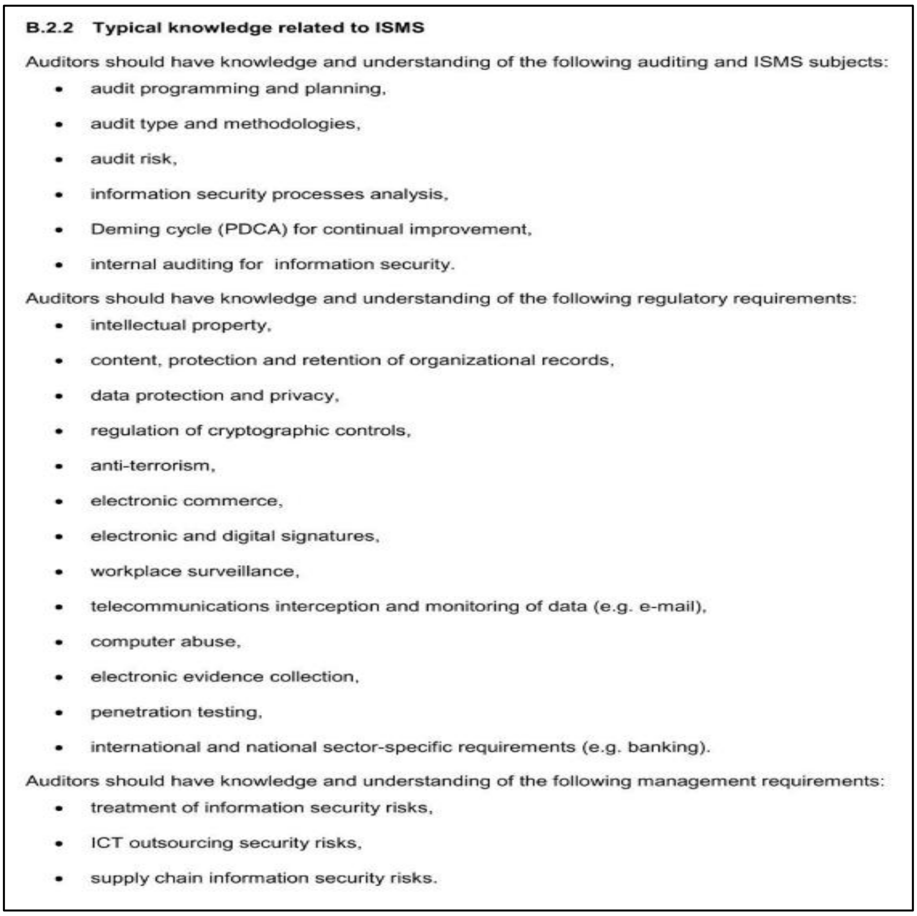
Figure 9. Correlation between NIST SP 800-39 and ISO/IEC 27005:2011 (ISACA 2015).

It is seen that risk management is a cyclical process of first context establishment, risk assessment, risk treatment, risk acceptance, risk communication & consultation and finally risk monitoring/review (Robinson 2020). This level of security management in terms of risks can protect the organization from sensitive information threats and attacks. This standard ISO 27005 mostly deals from an administrative perspective. Merits (SSH Academy 2018):



	Likelihood of incident scenario	Very Low (Very Unlikely)	Low (Unlikely)	Medium (Possible)	High (Likely)	Very High (Frequent)
Business Impact	Very Low	0	1	2	3	4
	Low	1	2	3	4	5
	Medium	2	3	4	5	6
	High	3	4	5	6	7
	Very High	4	5	6	7	8

Figure 10. Risk Matrix (ISO/IEC 27005: 2011).



B.2.2 Typical knowledge related to ISMS

Auditors should have knowledge and understanding of the following auditing and ISMS subjects:

- audit programming and planning,
- audit type and methodologies,
- audit risk,
- information security processes analysis,
- Deming cycle (PDCA) for continual improvement,
- internal auditing for information security.

Auditors should have knowledge and understanding of the following regulatory requirements:

- intellectual property,
- content, protection and retention of organizational records,
- data protection and privacy,
- regulation of cryptographic controls,
- anti-terrorism,
- electronic commerce,
- electronic and digital signatures,
- workplace surveillance,
- telecommunications interception and monitoring of data (e.g. e-mail),
- computer abuse,
- electronic evidence collection,
- penetration testing,
- international and national sector-specific requirements (e.g. banking).

Auditors should have knowledge and understanding of the following management requirements:

- treatment of information security risks,
- ICT outsourcing security risks,
- supply chain information security risks.

Figure 11. Audit Service provider requirements (ISO/IEC 27006).

This administrative standard has various merits as it's a very flexible approach adaptable to any business model, it emphasizes on continuous risk management, human factor plays a very important role in all the processes mentioned, and priority order for risk treatment/ actions are emphasized more. Demerits of SISO/IEC 27005:2011): [17] are that effectiveness of risk treatment relies on the results of risk assessment and if the latter is not done properly end results are useless. It's a limited model as controls for scope and boundaries of this standard are laid down by ISO 27001 ISMS for risks. Business impact and risk ranking is done by a pre-determined scale or risk matrix approach like high, medium, low as shown below (Figure 10) which may not be applicable to all business models alike. No specific laid methodology for risk management is emphasized.

5.4 ISO 27006 Analysis

This standard propagates the requirements of the certifying bodies and lays down control points of audits in the ISMS environment of the organisation. The ISO/IEC 27006:2015 standard "Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems" has been published on 1 October 2015. This standard replaces the ISO/IEC 27006:2011 standard with the same title. This standard been administered by International Organisational of Standardization is a document in demand, hence free access in the internet for the standard was not possible but however the various checkpoints available as posted for the standard is now picked and dealt upon to evaluate on the same. (Robinson, 2023) [18] To start with the audit providing bodies requirements, the ISMS had to be administered by them only if the conditions laid down in the Figure 11 are met by the parties involved in such action.

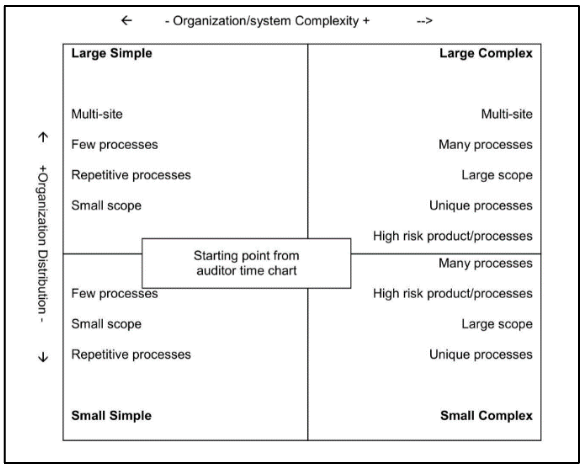


Figure 12. Factors for finding Audit Time span (ISO/IEC 27006).

In the Figure 12 above, the prospect of audit time span in each organization and what are the factors to be considered in determining the span of audit is based on the decision matrix above laid down in the guideline. The time span is segregated from simple to complex operations and from small to large organization (Robinson, 2023). In terms of certification organizations, the requirements as per standard are laid down in ISO 27006 under 5 major requirement heads are stated below in Figure 13.

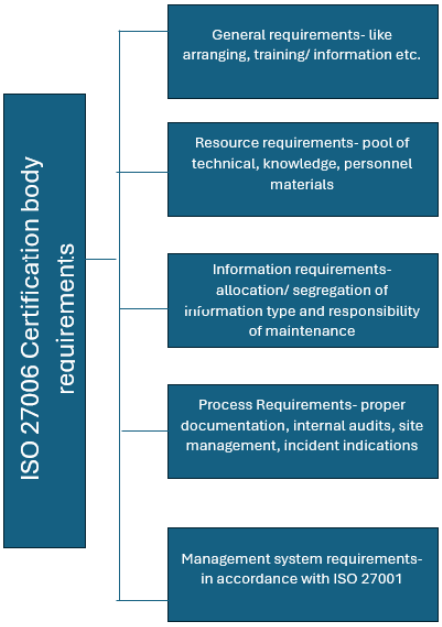

ISO 27006 Certification body requirements
General requirements- like arranging, training/ information etc.
Resource requirements- pool of technical, knowledge, personnel materials
Information requirements- allocation/ segregation of information type and responsibility of maintenance
Process Requirements- proper documentation, internal audits, site management, incident indications
Management system requirements- in accordance with ISO 27001

Figure 13. Certification body requirements.

This particular standard is a hierarchical one, which states the step wise checkpoints to be followed in implementing services of certification and audits of ISMS in an organization. Its very precise, easy to understand and follows the checklist if all the processes in the organization are as per the laid down guidelines of ISO 27001. It provides a detailed aspect of various areas to be regarded and fulfilled by the service providers in the course of providing such certification service. Some disadvantages are availability of too many pointers, hence the segregation of the important and the most important are not easily decipherable. Not all organizations can practice every check point at all times, though it can be flexible according to organization requirements, such flexibility may be at the cost validating efficiency as per the standard at times.

5.5 ISO 27014 Analysis

The main purpose of ISO 27014 Governance of Information Security standard was to align the objectives and strategies of information security with that of the business objectives of the organization. The governing body is ultimately accountable for the organizations decisions and key roles. Hence they had to be accessed, analyzed and evaluated via risk management approach supported with a strong internal control system. Hence the standard was introduced to implement the same in 2013. There was another synonymous standard in line with the ISO 27014 called ISO 38500, but they are way different in concepts and principles and same in some aspects (Robinson 2023), the same are brought out in Figures 14 & 15 respectively.

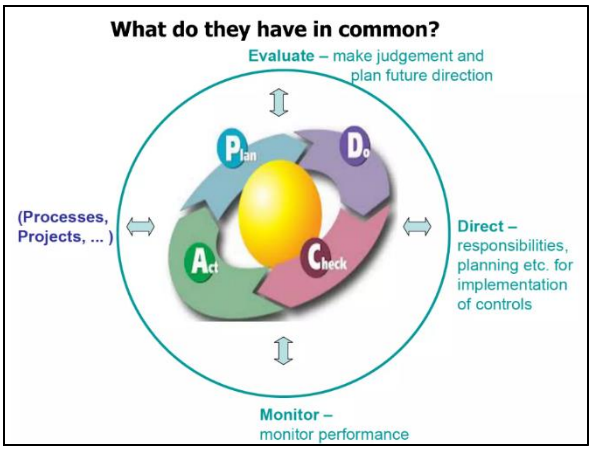
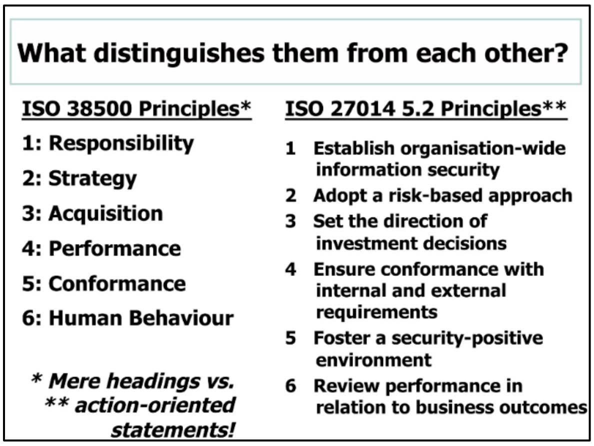

What do they have in common?
Evaluate – make judgement and plan future direction
Plan
Do
(Processes, Projects, ...)
Direct – responsibilities, planning etc. for implementation of controls
Act
Check
Monitor – monitor performance

Figure 14. Similarities between ISO 27014 & 38500.


What distinguishes them from each other?

ISO 38500 Principles*	ISO 27014 5.2 Principles**
1: Responsibility	1 Establish organisation-wide information security
2: Strategy	2 Adopt a risk-based approach
3: Acquisition	3 Set the direction of investment decisions
4: Performance	4 Ensure conformance with internal and external requirements
5: Conformance	5 Foster a security-positive environment
6: Human Behaviour	6 Review performance in relation to business outcomes

** Mere headings vs. ** action-oriented statements!*

Figure 15. Differences between ISO 27014 & 38500, Source for Fig 14 & 15: (ISO 27014:2013).

Critical Evaluation & Benefits

This standard been administered by International Organization of Standardization is a document in demand, hence free access in the internet for the standard was not possible but however the various net sources available were studied to bring out the pros and cons of the standard in a nutshell as detailed below.

The disadvantages include states that the major failure drivers are: (Robinson 2023)

- Boundaries set for the information security
- Lack of executive interest
- Poorly defined risk appetite
- Silo mentality among the organization personnel
- Ineffective policies on security within the organization
- Bringing up of new revolutions like BYOD (bring your own device) with the organization

- Speed of innovation larger than the space of monitoring and evaluation
- Inability to put value of information

Some of the advantages of the standard are: [20]

- Following risk-based approach to enable effectiveness
- Enterprise-wide information security is been propagated to ensure smooth working.
- Responsibility gets defined at the governance level and the commitment to the shareholders or stakeholders ensured
- Ensures robust control system and in line operations within all departments, as the business and IT strategies and goals are now aligned together
- Maximum business satisfaction can be derived

6. Conclusions

The company's reactions propose that serious protections for digital information are required and are being executed. However, with the right strategic methodology, Management details can help with limiting the digital possible dangers and difficulties and boosting the digital and cloud benefits. Solid frameworks and security efforts are set up to guarantee that authorized or approved staff approach the information, accounts are not signed in public domains, and files, passwords, and other security details are appropriately shared without leaving any trace. Furthermore, when seen from various frameworks and company objective viewpoints, the findings make plainly, larger part of security experts at organizations see online protection systems claims as a main concern and have measures set up to moderate them. In current parlance, the reason for Objective to keep up with financial and long haul suitability for the supportability of organizations. The notable patterns that these organizations follow are highlighted. The fast reception of cloud administrated services is because of its benefits, like expense reserve funds, versatility, and openness. The NIST circulated registering designing gives a broad construction that helps relationship with grasping the various parts that make up a distributed computing framework, from the client layer to the cloud provider layer. In assessment, the ISO plan in the Data security frameworks environment, takes advantage of the flexibility, versatility, and cost-practicality of registering through microservices, compartments, and course of action gadgets. These give long stretch support to associations. While cyber safety in processing offers many benefits, it furthermore gives basic troubles respects to insurance and trust through uplifted and regulated security, which are getting watched out for through the strong, solid and moving measures perceived as a component of the investigation plans. For businesses in general, cyber security issues is a problem from an abstractive perspective and capture the security requirements of various stakeholders at various levels to assist them in securing their network / cloud systems in a time-based rather than a long-term manner. In order to find a solution to this issue, additional research into network, application and cloud architecture security patterns and its governing frameworks, security enforcement, and feedback on these organizations' current security status is needed from stakeholders at various levels, including internal and external (which is not the focus of this study) but could be extended further for future in depth study.

References

Cid, Ramiro. 2016. IT Governance & ISO 38500. 2016. Available online: https://www.slideshare.net/slideshow/it-governance-iso-38500/64575586 (accessed on 13 July 2024).

Clark, James, Ward Johanne. 2018. UK: The network and information systems regulations 2018. Available online: https://www.dlapiperdataprotection.com/index.html?t=law&c=GB (accessed on 13 July 2024).

Cloud Security Alliance (CSA). 2019. Definition. Deutschland: tech target. Available online: https://www.techtarget.com/searchsecurity/definition/Cloud-Security-Alliance-CSA (accessed on 13 July 2024).

Dakks Deutsche Akkreditierungsstelle DDA. 2015. Documents: Report / Checklist ISO/IEC 27006: Available online: https://www.dakks.de/files/Dokumentensuche/Dateien/M%20Datenschutz.pdf, 2017 (accessed on 13 July 2024).

Dutch Accreditation Council. 2015. Explanation concerning the implementation of ISO/IEC 27006:2015. Available online: https://www.rva.nl/wp-content/uploads/2021/07/T033-UK-200218.pdf (accessed on 13 July 2024).

Faris, Sophia, Soukaina Elhasnaoui, Hicham Medromi, Hajar Iguer and Adil Sayout. 2014. IJACSA toward an effective information security risk management of universities' information systems using multi agent systems, Itil, Iso 27002, ISO 27005. *International Journal of Advanced Computer Science and Applications* 5:114-118. https://dx.doi.org/10.14569/IJACSA.2014.050617

ISO/IE C 27004:2016. Information security management- monitoring, measurement, analysis and evaluation. International Standard Second Edition 15-12-2016. Ref# ISO/ IEC 27004:2016€, 2016.

ISO/IEC 27005:2011. Information security risk management. International Standard First Edition. Available online: https://www.iso.org/standard/56742.html (accessed on 13 July 2024).

ISO/IEC 27006:2015. Requirements of bodies providing audit and certification of ISMS. International Standard First Edition. Available online: https://www.iso.org/standard/62313.html (accessed on 13 July 2024).

Mahn, Amy. 2018. Identify, protect, detect, respond and recover: The NIST cybersecurity framework. Available online: https://www.nist.gov/blogs/taking-measure/identify-protect-detect-respond-and-recover-nist-cybersecurity-framework (accessed on 13 July 2024).

Mani, Vimal.2022. Strengthening cybersecurity with red team engagements. *ISACA Journal* 1:1-6. https://www.isaca.org/resources/isaca-journal/issues/2022/volume-1/strengthening-cybersecurity-with-red-team-engagements

Niekerk, van Brett, Pierre Jacobs.2015. Toward a secure data center model. *ISACA Journal* 3: 1-10. https://www.isaca.org/resources/isaca-journal/issues/2015/volume-3/toward-a-secure-data-center-model

NIST. 2018. Cloud Computing. Available online: https://csrc.nist.gov/Projects/cloud-computing (accessed on 13 July 2024).

NIST. 2018. Cybersecurity framework. Version 1.1. Available online: https://www.nist.gov/cyberframework/csf-11-archive (accessed on 13 July 2024).

Robinson, Rachel John. 2020. Structuring IS framework for controlled corporate through statistical survey analytics. *Journal of Data, Information and Management* 2: 167-184. https://link.springer.com/article/10.1007/s42488-020-00021-3

Robinson, Rachel John. 2023. Cloud systems with its security, privacy and trust claims to a sustainable solution. 3rd International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME). https://doi.org/10.1109/ICECCME57830.2023.10252796.

Robinson, Rachel John. 2023. Insights on cloud security management. *Cloud Computing and Data Science* 2:212-222. https://doi.org/10.37256/ccds.4220233292

Shackelford, Scott J., Proia Andrew, Proia Andrew, Martell Brenton and Craig Amanda. 2015. Toward a global cybersecurity standard of care? Exploring the implications of the 2014 NIST cybersecurity framework on shaping reasonable national and international cybersecurity practices. *Texas International Law Journal* 50:305-355. https://ssrn.com/abstract=2446631

Shiroya, Aarti Himmatbhai, Rachel John Robinson. 2023. Strategic risk management case analysis of restaurant industry. *Global Journal of Tourism, Leisure and Hospitality Management* 1: 1-14. 10.19080/GJTLH.2023.01.555552

SSH Academy. 2018. NIST cybersecurity framework - summary & guidance. Available online: https://www.ssh.com/academy/compliance/cybersecurity-framework (accessed on 13 July 2024).