



**Apply the principles and practices of Data Security, Governance,
and Compliance**

**By
Jay Chaturbhai Kakadiya**

Submitted to the University of Wales Trinity Saint David

Module: Data Security, Governance and Compliance

Word Count: 2771

Table of Contents

1.	Introduction	4
2.	Various security frameworks or models	5
2.1	ITIL (Information Technology Infrastructure Library)	7
3	Research for the company	8
3.1	Need of Nature Garden information system security, governance, and compliance ..	8
3.2	Security Policies:.....	9
3.3	Importance of security plan:.....	9
3.4	Requirement of updating standards concerning time.....	11
4	Conclusion	13
5	Reference	14

List of figures

Figure 1: Internet Security Diagram.....	6
Figure 2: ITIL model	7
Figure 3: Security Policy Diagram	9

1. Introduction

In today's era of socialization and digitalization, business organization is putting a strong emphasis on security information and internet risk security. There are numerous regulation that needs to be imposed by the different sector to protect such information. The company needs to comply with such regulations and needs to work on regulatory technology to save it from data breaches and cyber-attacks. So the below report covers the model or the international security standards which are important and need to be complied with by the company in protecting their data. The need of the Nature Garden (NG) how protects customer data and increase its international customer base, and the last will report why this standard must be upgraded from time to time. The company information is based on the wireless base. So client data are the major concern of the company. The company wants to analyse how such information can be secured and saved. The security policy, internet governance, the ISO, and the ISO 2700 are being complied with and studied for a better understanding of the research.

2. Various security frameworks or models

The International Organisation for Standardisation (ISO) will define the management of risk with coordinated activities that will be able to control and direct the organization that will be related to the risk. As per the standards explained by the European Network and Information Security Agency (ENISA), the process of identifying risks and marking qualifications to them so such risks can be managed and the loss of the organization can be reduced will be termed risk management. In the field of organization, security is the major source that will cause lots of hindrances in the company's business and will lead to higher losses. Many standards will be in the favour of the stakeholders and this will be managing and maintaining security risk which will exist in the matter of security.

The International Standard Organisation is an independent and non-governmental organization that works on the international level. This will bring all the experts from the global level together and work in the same direction to make a process that will help reduce the risk and increase the security against cybercrime (Tawalbeh et al., 2014). There are many standards which had been given by the ISO. Some of them are as follows:

- **ISO 9000:** These are the standards that are applicable to give quality management to the organization. This will give the way for an organization to improve their quality and needs to be consistent in the execution to the customers.
- **ISO 45001** is the standard that is being given focus on health and safety standards. The company needs to apply such standards as this will get them security so that each employee will reach home safely.
- **ISO 14001** is the standard that will help in the environmental management of the company. As the company needs to be focused and aimed to the better averment this can be done by the reduction of carbon emission and to decrease the pollution.
- **ISO/IEC 27001** - The ISMS will be abbreviated as the information security management systems, so the company needs to make the security that will meet the requirements of ISO and IEC. This ISO/IEC 27001 will apply to all business sectors and activities. The guidance for establishing and implementing maintaining and continual information will help in improving the function of the security management system. The importance of the cheer will be decreasing the risk of new threats which will be constantly emerging and give a difficult time with cybercrime. The holistic approach of the information security systems will encourage the company to be aware

of the security risks and will make them applicable to standards that will reduce the risk. The ISO provides the tool for measuring risk management and for giving solicited to cybercrime.

Cyber-attacks are costlier in terms of financial and non-financial. The financial loss that can be justified with cybercrime is that all the monetary losses are included but above that there are informative losses that are classified under the quantitative terms of the cyber-attack (Molstad et al., 2016). All the information re confidential and records which the company needs for the growth. The hackers are using this information and selling this to the competitors. As per the report of the World Economic Forum, the report generated on the Global Cybersecurity Outlook report indicated that this cyber attack had increased by 125% from the year 2021. There is evidence that this growth rate will increase and will change the landscape which will give leaders to strategic approach to decrease cyber risk.

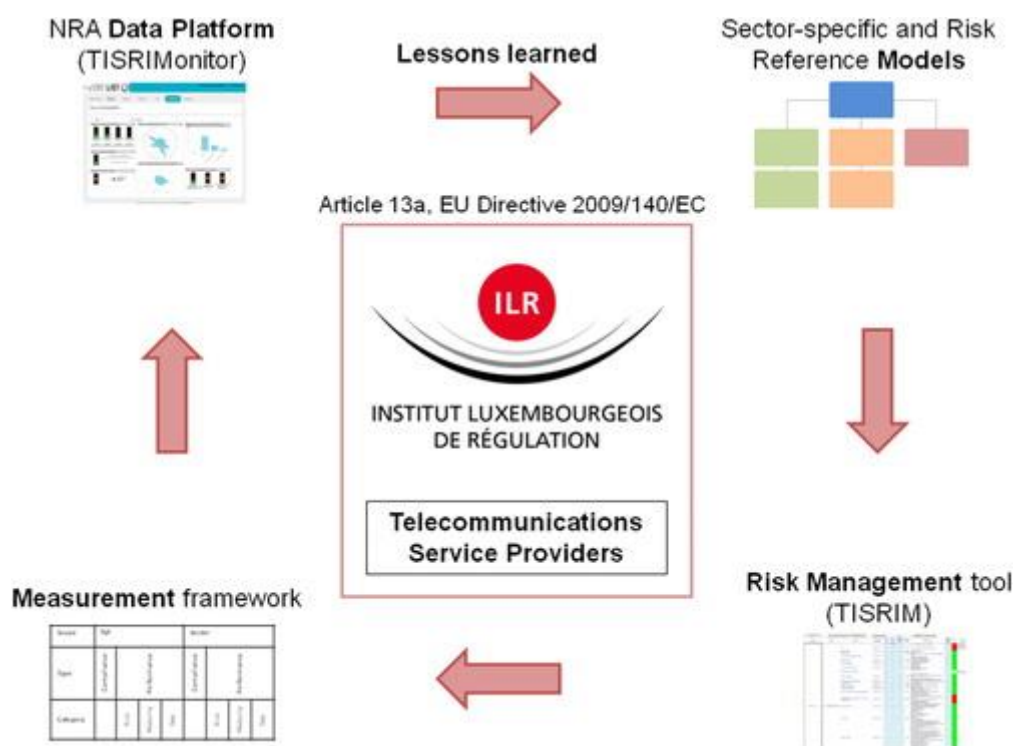


Figure 1: Internet Security Diagram

(Source: Nicolas et al., 2021)

Below is the list of advantages which will help the organization with the ISO/IEC 27001:

- All the information which are confidential or at a higher risk is secured with the help of this standard. It gives the ability organization to save the data in a digitalized manner or to store them in the cloud-based networking

- This standard will help the company to increase the protection against cyber-attacks, as all the vulnerable threats of cyber-attacks are already known so the organization is being prepared for the risk.
- All the frameworks which are needed for the security purpose are centrally managed, this will help in decision-making and also helps the organisation to take the steps for the improvement.

2.1 ITIL (Information Technology Infrastructure Library)

Information Technology Infrastructure Library, the wide protection of the security is given to the organisation which will include all the technologies which will reduce the threats and cyber risks. The company rates to respond the cybercrime will be increased as the security threats are well addressed by the company and they are being awarded in advance. The cost that is spent on mitigating risk or being applied to the new technology will be reduced with the standard applicability. The standards give the proper and systematic manner for the company to fight such cybercrime. The company integration, confidentiality and data availability will have more value.



Figure 2: ITIL model

3 Research for the company

3.1 Need of Nature Garden information system security, governance, and compliance

Information security is complicated and ever-changing which needs to be efforted for the corporation. This means there is a high need for the governance of the higher level of organisation. Information security governance has a condition which needs to be difficult at the practical level. There is a high difference between the governance of security risk and the management of the risk. Management is the day-to-day decision-making as the governance is the board of principles which are the value or guide which needs to be set up and followed by every principle (Ihsan, 2021). Information security governance is a vital role which is a requirement of today's era. This will improve the business organisation's data security. The customer base will be increased and there will be a higher response from the incident regarding the response. There are 5 core components of corporate governance which are as follows:

- Organisation structure: there should be a proper organisational structure which needs to be priced for security governance because it will help in identifying risk management and will help in identifying poor practices and will help in avoiding them. There are the proper plans which need to be maintained for making security incidents and which will help in managing security risk information.
- Business continuity: Nature Garden should ensure business continuity for the event like breach security and failure of investment or the business reputation
- The company should define security measures and needs to ensure the business needs have the highest priority and how the employee will follow such steps.
- The company should make sure that there should be stays in business **compliance** which will increase the requirements and regulatory standards. All the standards need to be followed as per the National Institute for Security and Technology (NIST) publication 800-53.
- The communication reference needs to be done for the information which has both internal staff and external to the potential partners. All the governance processes from the boards have directors (Verhulst et al., 2014).

3.2 Security Policies:

A document which will be outlining the rules and method that needs to be followed by the organisation to protect the data are termed the security policies. This will generally include the goals which are related to the security of data and cover specific issues such as who can access the data remotely access, the acceptable use of data and other methods of data collection. The other documents which need to be attached to such security policies are the procured of operation, backup plans and recovery plans (Cath, 2019).



Figure 3: Security Policy Diagram

3.3 Importance of security plan:

Security policies are crucial aspects regarding the information of security programs. This will include the technical support and team which will control the security department of the organisation. This will give them a starting point and the security teams will be specially designed to check all the society-related takes, this team have the aim to translate the false intentionally and to save the organisation from the hard loss.

The policies of security will ensure that the individuals who are applying for the same standard. This will give the outline which is appropriate and will enhance the behaviour of risk and devices which is being used by the company software.

There are generally three types of standards which are being ensured by the NIST the first one is to design the policies which are related to the program which are of high level and have confidential information this program is very costlier and needs to be secured from hackers as this will give information to the competitors. The second one is issue-specific policies, as per these policies the company needs to give security to the issues which are important for the organisation's operation. In this, some of them are the company tender information or the information related to the acquisition. The last and third one is system-spaced policies (Van et al., 2018). All the systems and computers which are being used by the Nature Garden need to be secured with high technology, the access should be limited and very strict. Remote access has very high loopholes which will allow any hackers or threats to enter and attack the vulnerable information.

The core components of effective security policies should contain the following:

- The goals and the objectives underlying the security policies should be clear and precise, and all the organisation's staff and stakeholders should be aware of such policies.
- The policies' scope and applicability must be denied if there is any geographical or political restriction then this must be known in advance.
- There must be always an endorsement of such policies from the senior management to gain support and for successful information and clear communication.
- The enforcement of procedures should have a mechanism that will give compliance and prevent the security policies. This will aim to achieve perfection by applying a realistic approach and to rescue the burden of the adoption of any policies (Asgarkhani et al., 2017).
- The level of risk accepted in such security policies must be determined according to the given structure and proper cyber-attack.

Nature Garden (NG) estimated that 95% of the wireless network. Personal staff security is the data collection and client staff is the major concern. The covering of the needs of the security. For the Nature Garden (NG) the security governance program includes the senior management and the staff will work together. There is a need the document risks for the third parties. The board has direct management which needs to be aligned. The collection of feedback needs to be done on time and the security program needs to be updated from time to time. Information security needs to be part of the business strategy.

As per company details, Company needs to secure its data which is related to security **governance** and will help secure the policy related to cybercrime. This will also help in securing company awareness and help in making a better structure.

3.4 Requirement of updating standards concerning time

Standards help in making a structure for better governance. It will give the responsibilities and will make the organisation comply with all the guidelines that need to be followed by the company. But the standards are never be same on each side which means that they are not guaranteed that they must be able to fight with the competitors or the outside environment. As the standards are made internally and internally circulated. The external guidelines are taken for a better preview. There the emerging needs of the relevant laws so this must be upgraded from time to time.

Governance always needs to be as per the legalization and guidance together in the same format. There is a requirement to keep them on the legislation and technical support. The company's objective should be to create a policy that will be safe and budget-friendly (Van, 2013).

- **Service Level Agreement:** This is the agreement that needs to be made between the supplier and the company regarding internet security. The whole process of saving the information keeping it confidential and making conditions is on the internal management. So, if they think there is a merger that needs to upgrade the standards then the company should upgrade it. As for the example, there is an attack on the firewall and there is a high risk of a data breach, so in such case, if the company needs to increase the security password of the data access, then the company needs to do that.
- **Protection mechanisms:** Security protection is the major concern of the Nature Garden. Required by law: the first need to upgrade or amend the standards is needed by the law. If the law is needed, then the company needs to comply with the law regulation and should give retrospective effect for such. As for the example, there is the need for maintenance of internet security as per the ISO2007, so the company needs to upgrade its standard accordingly. The protection needs to be as per the amended standards. As for the case of cloud computing, if the company needs that the information needs to be saved in the cloud computing, then the company needs to ensure that the data needs to be secured accordingly, the whole agenda of saving data is to secure them and keep them confidential.

- **Contingencies planning:** Contingencies are situations where there is an un-notified change in the company from the external factor. There are many stages when the company should comply with the technology, so if such technology had been upgraded and there the attached ancillary needs that the internet security also needs to be upgraded accordingly, then in such case this needs to be done from time to time as per the required manner (Yusif, 2023). If the company is upgrading their business and trying for expansion and up-gradation, then the company should go for upgradation, because the standards need to be matched with the acquired company or should be made as per geographical needs or political needs.

4 Conclusion

It has been concluded that there is an essential component of security policy which needs to be done for better business operation. There is a need for threat protection which will help eliminate the vulnerabilities and will increase the security audits. As digitalization increases the demand of the society policy and the standards needs to be increased. As the business grows the staff and internal management needs to be increased. There should be clear and precise communication between the company and the internet security team regarding the company's security. So secure internet access is a must.

Security standard needs to be amended from time to time because of the technology change, change in political parties or change in geographical restriction. But before upgrading it must be taken permission from the senior management and the board of directors. In case the company indulged in some cybercrime, then there must be a proper protocol which had been ensured and understood by the employees what they need to be done. So without wasting a moment, the company needs to report it and work on high-security procedures and the recovery plan. The implant things that need to be worked by the company to procedure data are lock-free access or limited freedom of access for the data or the accessed data needs to be password protected either by the biological lock or other high-security protection. Also, the equipment needs to be protected with a firewall so the data can be highly secured.

5 Reference

- Asgarkhani, M., Correia, E. and Sarkar, A., 2017, February. An overview of information security governance. In *2017 International Conference on Algorithms, Methodology, Models and Applications in Emerging Technologies (ICAMMAET)* (pp. 1-4). IEEE.
- Cath, C., 2019. Internet governance and human rights: A literature review. *The 2018 Yearbook of the Digital Ethics Lab*, pp.105-132.
- Ihsan, F. and Bintarsari, N.K., 2021. Internet governance forum analysis on artificial intelligence in cyber security. *Insignia: Journal of International Relations*, pp.32-47.
- Molstad, L., Dörsch, P. and Bakken, L., 2016. Improved robotized incubation system for gas kinetics in batch cultures. *Researchgate. DOI, 10*.
- Mayer, N. and Aubert, J., 2021. A risk management framework for security and integrity of networks and services. *Journal of Risk Research*, 24(8), pp.987-998. DOI: [10.1080/13669877.2020.1779786](https://doi.org/10.1080/13669877.2020.1779786)
- Tawalbeh, Y., Ajo, R., Al-Udatt, M., Gammoh, S. and Maghaydah, S., 2014. Investigation of the antimicrobial preservatives in the dairy product (labneh).
- Van Eeten, M.J. and Mueller, M., 2013. Where is the governance in Internet governance?. *New media & society*, 15(5), pp.720-736.
- Van Horenbeeck, M., 2018. The future of Internet governance and cyber-security. *Computer Fraud & Security*, 2018(5), pp.6-8.
- Verhulst, S., Noveck, B.S., Raines, J. and Declerq, A., 2014. Innovations in global governance: toward a distributed internet governance ecosystem. *Global Commission on Internet Governance Working Paper*, (5).
- Yusif, S., Hafeez-Baig, A. and Anachanser, C., 2023. Internet governance and cyber-security: a systematic literature review. *Information Security Journal: A Global Perspective*, pp.1-14