Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 26 (2023), No. 3, pp. 885–898
DOI : 10.47974/JDMSC-1776

Design & analysis of novel IT security framework for overcoming data security & privacy challenges

Prashant Manuja *
Rajveer Singh Shekhawat †
Umashankar Rawat §
Manipal University Jaipur
Jaipur
Rajasthan
India

Abstract

IT security has always been a major concern for all organizations, especially after the rise in IT Integration amongst all processes, Post pandemic this has become a bigger issue than earlier. The organizations are growing also with IT Integration the negative impact of information related risk incidents are also increasing worldwide. There are several IT Risk Assessment Frameworks in use to address information security assaults, vulnerabilities, threats, and breaches, including ISO 270001/27005. COBIT, NIST SP- 800/53 etc, though following and implementation of these protocols, still organizations face challenges of IT risk, which may involve an asset or information. The biggest challenge is the data Security or privacy. Based on survey data, this study evaluates the majority of the current IT risk management frameworks and makes an effort to pinpoint any shortcomings in them. Based on the analysis done, a new IT Security framework is proposed and implemented in two organizations for its detailed analysis and validations with the existing models For the Risk Assessment of the same organization new technique for IT Risk Assessment is also proposed.

Subject Classification: *68M25, 68P27.*

Keywords: *Secure framework, Assets management, Data security, Data privacy.*

* *E-mail:* **prashant.199307601@muj.manipal.edu (Corresponding Author)**
† *E-mail:* **rajveer1957@gmail.com**
§ *E-mail:* **umashankar.rawat@jaipur.manipal.edu**

1. Introduction

Confidentiality protection, commonly referred to as information security, refers to the need to prevent any type of information from being disclosed without authorization. It is impossible to emphasize how important information security is to businesses, and these companies take the required security measures to protect their data from hacks, breaches, and other hazards that could harm customer and corporate data. It shields the organization's data from threats and weaknesses. Information security management can be put into practice through the use of an efficient information security risk management procedure, in which an organisation evaluates information security risks by identifying, analyzing, assessing, addressing, monitoring, and communicating Risk. [1] Three primary accepts of Information Security are Access control, and then asset management, and at last but not the least incident management, that businesses utilize to address them. [2]

2. Study of Various IT popular IT Security Frameworks

As per the need of industry for IT Security, many frameworks have evolved in past few years, in this section we explore the various types of IT Security frameworks normally used by various organizations:

2.1 *ISO/IEC 27001:2015*

With ISO/IEC 27001:2015, you can preserve your information assets, ensure that the security measures you implement are suitable, and establish trust with other parties.

Among the various applications for which ISO/IEC 27001:2015 is suitable in an organization are the ones listed below:

- Setting up a framework, guaranteeing management oversight, and creating security goals and specifications;
- ensure that security risks are managed economically;

2.2 *NIST SP 800-30/39/53*

To address each of these categories, NIST places a model as mentioned: [4]

- Identify: Establish methods for classifying risks and identifying controls.

- Protect: By putting controls in place to reduce or eliminate risk, you can: • Send out alerts to identify control failures.
- React: A systematic process for dealing with issues when they are found
- Recover: A defined process for restoring functioning to failed controls.

2.3 *COBIT*

Regardless of industry, COBIT is vital for developing, controlling, and maintaining risk and security for enterprises globally. [5]Three tiers of COBIT are:

1. Information requirements, such as standards for effectiveness, efficiency, confidentiality, availability, compliance, and dependability
2. IT resources, such as tools, data, staff, and information.
3. Domains are used to segment processes.

2.4 *ISO 31000*

The goal of ISO 31000 is to replace the numerous existing standards, methodologies, and paradigms that differ between industries, subjects, and locations in order to give practitioners and businesses adopting risk management processes with a widely acknowledged paradigm. [6]

3. Survey based IT Security Vulnerability Analysis

To identify challenges and issues in existing security frameworks, a systematic survey of risk management approaches followed by different industries, businesses, governments, academia, etc. is conducted. The first stage was to define the scope of the study and the inclusion and exclusion criteria. The purpose of the survey is to identify the challenges faced by organizations using risk frameworks and methodologies that provide guidance for the assessment of information security risks or the assessment and treatment of information security risks. [7, 8].

To better understand how well the technical architecture supports the current security programmes, this data is being gathered from numerous organisations. Comparing organizational controls to pertinent standards for best practices. This enables us to evaluate the security procedure in comparison to alternative, more efficient methods. Data collection offers an overall view of the technological environment, current security measures,

and overall security efficacy, which may be used to find vulnerabilities and vulnerabilities of network devices, servers, and apps.

More than 100 businesses, organizations, and academic institutions, as well as their system administrators and leaders, received the comprehensive questionnaire. Of the 94 different submissions, 72 were original contributions from business and academics that examined how these risk management frameworks may assist organizations in ensuring the security of their data and assets and identified the difficulties they encounter even while putting them into practice.

Out of the 72 different responses, 28 implemented the ISO-27001 framework; while 16 organizations each uses COBIT and SP-800-53. Only 12 organizations adhere to the framework for ISO 31001/Cyber Security Essentials.

4. Details of Analysis of Survey data

Our previous work got published with detailed analysis of responses from 72 different industries based on 3 major concerns, , namely:

- Access control
- Asset Management
- Incident management

The investigation is still expanding on the extent to which the three aforementioned problems have been addressed, i.e., how well their IT security frameworks can manage the size of their respective connected domains.

4.1 *Analysis of Various IT frameworks, with respect to Asset Management*

The management of an organization's assets, which include both information and physical items, should be its top concern. As can be seen in Figure 1, ISO 27001 has the highest average value, and according to its users, it is the most effective at managing assets, showing a greater level of asset management. The second average is SP-800-53, although COBIT users think it performs better in terms of asset management. Additionally, keep in mind that asset management presents difficulties for organizations without a structure.

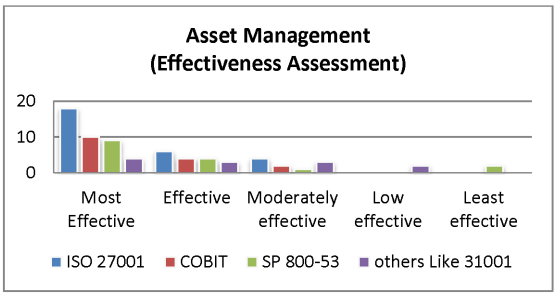

Figure 1

Effectiveness comparison of Asset Management by Various IT Frameworks

4.2 *Analysis of various frameworks, with respect to Access Control System*

Access control is one of the most important information security techniques ,that assists in determining the control of access to information based on duties and requirements. As seen in Figure 2, ISO 27001 had the highest average and was rated as the most effective access control standard by users, followed by SP-800-53, which came in second. COBIT, however, found it difficult to compete with the other standards. 2 Compared to organisations that don't employ a framework, ensuring adequate access restrictions is more difficult.

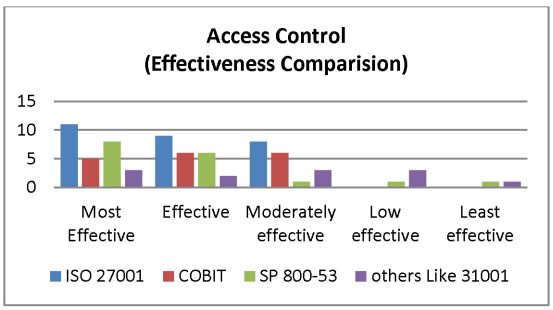

Figure 2

Effectiveness comparison of Access Control by Various Frameworks

4.3 *Analysis of various IT Security frameworks, with respect to Incident Management*

Any organisation may experience security breaches, but managing them requires an IT security architecture. Recovery of data and assets, as well as advice on how to further safeguard them, are aided by incident

management. Users of the framework deemed SP-800-53 to be the most successful for incident management, as shown in Figure 3, while COBIT and ISO 27001 had lower averages and performed less well than SP-800-53. Additionally, keep in mind that organisationswho don't use frameworks have trouble managing incidents

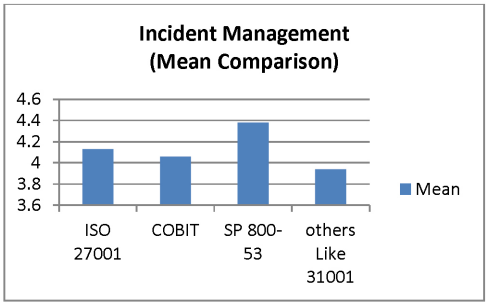

Figure 3

Mean Value comparison of Incident Management by Various Frameworks

4.4 *Security Issues faced by various Organisations after implementing IT security frameworks*

As shown in Figure 4 in spite of the numerous security precautions taken by organizations, security issues still arise, and these problems either need to be addressed by organizations or improved information security frameworks need to be used to enhance security management procedures.

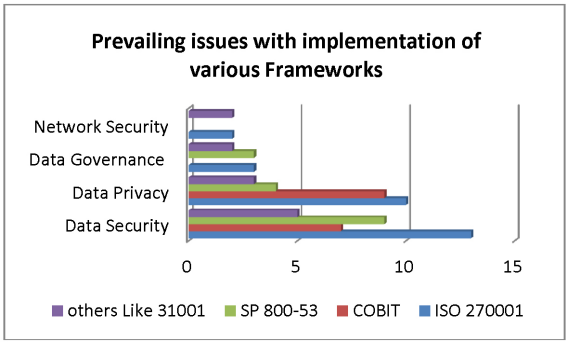

Figure 4

Prevailing issues with implementation of various Frameworks

5. Research Gap

The primary issues that the surveyed organisations face are data security and data privacy, as can be seen from the analysis above. The method used to determine risk severity by taking into account several characteristics is the main cause of this. A hybrid model that can identify assets holding sensitive and private information as well as check and compare various security standards and frameworks (such as ISO 27001, COBIT, SP800-53, ISO 31000, etc.) might be presented as a solution to this problem. The processing framework will include multiple steps, be able to identify actions that increase the standard model's absoluteness, and provide useful and effective solutions that may be applied in real-world circumstances. It is possible to chronicle the findings of analysis, evaluation, and comparison.

6. Proposed Framework

In over study with more than 72 employees of 50+ organizations using various frameworks like ISO-270001, COBIT, NIST SP-800/53, ISO 31000, and it was observed that the major issues faced by all the organizations while implementing the IT Security frameworks are, Data security, Data Privacy and Data Governance.

In order to resolve the same, in our research work we propose a improved hybrid model which is based on ISO 27001 majorly and further appended with some controls of COBIT IT framework to have better data security and governance and management.

A new approach for Criticality Analysis of the Risk during Assessment process is also proposed, where in modified Criticality Analysis technique with Privacy as a Major parameter is appended.

6.1 *Proposed IT Risk Assessment Model with Updated Controls at various Clauses*

As visible in Figure 5, in the proposed model 09 additional controls have been added in the ISO 27001 mandatory in its 14 clauses. 5 Controls are added in the clause 6, planning for planning about the risk assessment for privacy and 02 of them are adapted from COBIT, in all 07 controls are added in Clause 06.And02new controls are added in the clause 8 operation about the same. This new additional 7 clauses will be a working model for the Annex-A controls. Earlier these 07 clauses had 114 controls in our proposed framework it will have 123 controls

Figure 5

Revised Security Assessment Model at Control

The names of 05 New Controls added at Clause 6 are (As shown in Figure 6):

1. Risk Assessment must be applied within the scope of Privacy Assessment
2. Risk Assessment must ensure proper management of Information Security and Privacy
3. Information Security and Privacy objectives are established and communicated at appropriate levels.
4. Applicability of Controls must consider both risks to information security and too processing of PII
5. Risk assessment must consider both the organization and the natural person to whom personally identifiable information relates.

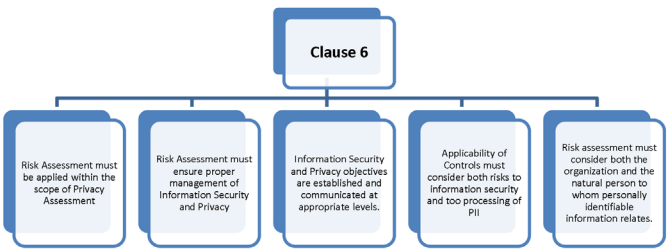

Figure 6

Names of 05 Controls added at Clause 6

The controls adopted from COBIT to append in Clause 6, for improvement of the Data Security challenges, are displayed in Figure 7:

1. Managed Program in Data Governance
2. Managed Program in Data Security

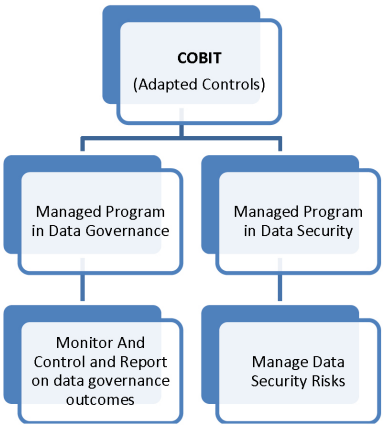

Figure 7

Names of 02 Controls added at Clause 8

The names of 02 Controls added at Clause 8 are (as shown in Figure 8):

[1] The organization must implement the Information Security & Privacy risk treatment plan.

[2] The organization shall conduct assessments for Information Security and Privacy risk assessment at regular intervals

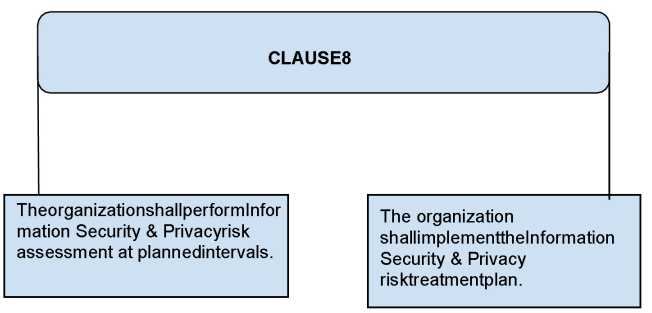

Figure 8

Names of 02 Controls added at Clause 8

After adding 9 new controls (07 at Clause 06 and 02 at Clause 8) to the redesigned framework as seen in Figure 09, there will be a total of 123 appropriate controls for the environment over the seven clauses. As per procedures, we examine and analyse everyday operations and business processes before determining which ones are appropriate for the organisation. When you see the number m/n, it signifies that there are m controls that apply to the organisation out of the n controls in one category.

Figure 9

Controls aligned with each and every mandatory clause

6.2 *Criticality Analysis during Risk Assessment Process*

After proposing the model the Risk assessment techniquewas also modified, wherein Privacy was added as one more parameter for "Criticality Analysis" of the organizations and "Privacy was given equal weightage during Risk Assessment process by the Auditor

$$\text{Current Asset criticality rating} = (C*C) + (I*I) + (A*A) \quad (1)$$

Wherein C Stands for Confidentiality, I Stands for Integrity and A Stands for Availability

$$\text{Proposed Asset criticality rating} = (C*C) + (I*I) + (A*A) + (P*P) \quad (2)$$

Wherein C Stands for Confidentiality, I Stands for Integrity,A Stands for Availability and P Stands for Privacy

Here Privacy is calculated based below given equation

$$\text{Proposed Privacy Asset criticality rating} = (L*L) + (I*I) + (R*R) \quad (3)$$

Where L= Likelihood, I= Impact and R=Risk

This modification can help the organizations to ensure the analysis of critical issues in case of Data Privacy in IT infrastructure and avoid IT Risk in all parameters.

7. Implementation of Proposed work in IT sector Organizations

The proposed model was provided to 02 startups of IT sector to ensuring implementation of controls in order to achieve Privacy over Network 38 variety assets were audited post implementations in these organizations and based the new proposed Asset Critical Rating system based on 18 parameters and 14 clauses detailed Risk assessment of each and every asset was carried out. For which IT Asset Inventory was used with the above formula (1) and (2) both and Asset Risk Profile was generated.

Risk Score of each and every asset was calculated with and without Privacy as parameter. and was given score in range,:

1. High (Critical)- 4 [This Can be disastrous for the Organization and requires immediate corrective action]
2. Major (Medium) -3 [This Can be dangerous for the Organization and requires safeguard mechanism to be implemented immediately]
3. Moderate ( )-2 [This can be Harmful for the Organization and requires some regulatory corrections]
4. Low (Minor)= [This can be Annoying for the organization and requires process fine tuning only]

8. Comparative analysis of existing model in 2 Different Organizations

For 1st IT Company as seen in Figure 10, out of 29 assets audited, 25 were found at high risk, that is almost 80% of the total asset was marked at risk

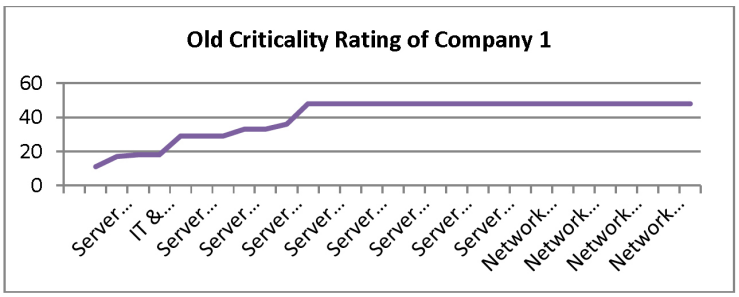

Figure 10

IT Risk assessment of an IT Company based on Criticality Analysis with old Framework

Where as seen in Figure 11 for the 1st IT with new proposed framework out of 29 assets audited, 27 were found at high risk, that is almost 90% of the total asset was marked at risk and this change was majorly where privacy was concern and corrective measures suggested have lead to improve the security of the existing system of the organization

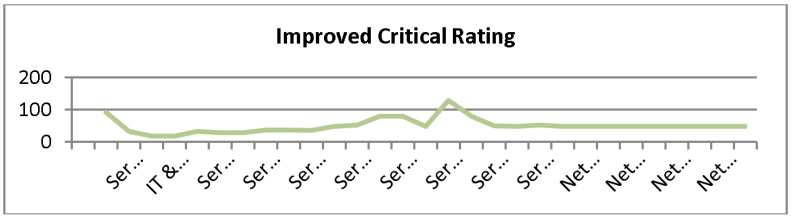

Figure 11

IT Risk assessment of an IT Company based on Criticality Analysis with New Framework and New Risk Assessment Model

For 2nd IT Company as seen in Figure 12, out of 33 assets audited, 28 were found at high risk, that is almost 80% of the total asset was marked at risk

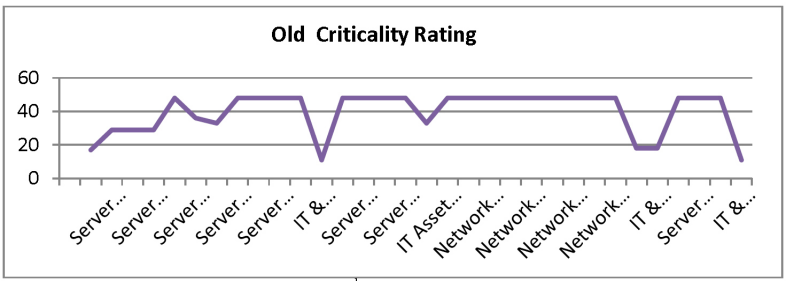

Figure 12

IT Risk assessment of 2nd IT Company based on Criticality Analysis with old Framework

Where as seen in Figure 13 for the 2nd IT with new proposed framework out of 33 assets audited, only 22 assets were found at high risk, that is only 66% of the total asset was marked at risk and this shows 2nd organization has good focus on Data Privacy

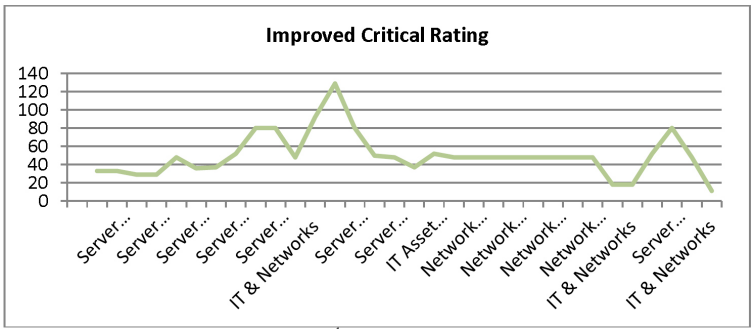

Figure 13

IT Risk assessment of 2nd IT Company based on Criticality Analysis with New Framework and New Risk Assessment Model

9. Conclusion

Data security and data privacy are major challenges faced by organizations, especially in IT infrastructure. The evolution of IT makes IT security and risk assessment important parameters. The main reason behind it is the method of calculating risk severity by considering different parameters, where in all major used IT security risk assessment frameworks (i.e. ISO 27001, COBIT, SP800-53, ISO 31000 etc. A novel approach that groups assets containing sensitive and secret information according to criticality is put forth to address the same problem. Criticality analysis can be performed during evaluation to compare and check the numerous factors specified in various security standards, including confidentiality, integrity, availability, and privacy. The adoption of our suggested methodology by two IT businesses demonstrates improved growth in security and privacy. The findings indicate that the first organization needs to strengthen its security, particularly with regard to data privacy, while the second organization is putting a lot of effort into data security but does not yet address the issue of safe asset management.

References

[1] Allen, Julia H. : Governing for Enterprise Security. Carnegie Mellon University. Report (2018). https://doi.org/10.1184/R1/6573995.v1

[2] Patrick MachariaNjorogeet. Al. A framework for effective information security risk management in kenyan public universities, *IJSSIT*, Volume IV, ISSUE X (2019).

[3] https://www.educause.edu/focus-areas-and-initiatives/policy-and-security/cybersecurity-program/resources/information-security-guide/toolkits/information-security-governance.

[4] https://www.diligent.com/en-gb/blog/information-security-governance-best-practices/.

[5] https://www.iso.org/standard/42103.html#:~:text=ISO%2FIEC%2027001%3A2005% 20specifies,the%20organization's%20overall%20business%20risks.

[6] https://www.foundpg.com/iso-31000.

[7] NIST US, Information Security, Managing Information Security Risk Organization, Mission, and Information System View, Special Publication 800-39 (2017).

[8] Kidd Chrissy, BMC Blogs (2019). (https://www.bmc.com/blogs/cobit/).

[9] Prashant Manuja & Rajveer Singh Shekhawat. Developing information security metrics and measures for risk assessment of an organization, *Journal of Discrete Mathematical Sciences and Cryptography,* 25:4, 1195-1202 (2022), DOI: 10.1080/09720529.2022.2075092.

[10] YashpalSoni, GeetaChhabra Gandhi & Dinesh Goyal. Improved and secure framework for existing e-Bazaar model in Rajasthan, *Journal of Information and Optimization Sciences*, 43:8, 1975-1985 (2022), DOI: 10.1080/02522667.2022.2111042.

[11] YashpalSoni, GeetaChhabra Gandhi & Dinesh Goyal. A secure e-health framework for rural Rajasthan, *Journal of Statistics and Management Systems*, 25:8, 2113-2122 (2022), DOI: 10.1080/09720510.2022.2119000.