Library Progress International
Vol.44 No. 3, Jul-Dec 2024: P. 18351-18360

Print version ISSN 0970 1052
Online version ISSN 2320 317X

Original Article

Available online at www.bpasjournals.com

Identification of Sustainability Issues in Current Legal System Using Quality Function Deployment (QFD)

Manuj Darbari, Naseem Ahmed

Faculty of Law, Integral University, Lucknow.,manujuma@gmail.com.

How to cite this article: Manuj Darbari, Naseem Ahmed (2024) Identification of Sustainability Issues in Current Legal System Using Quality Function Deployment (QFD). *Library Progress International,* 44(3), 18351-18360.

ABSTRACT

This study aims to adopt Quality Function Deployment (QFD) effectively for deriving guidelines for sustainable infrastructure, pinpointing on the essentials required for the same, specifically in the domain of cyberlaw. This article will in detail discuss three major areas: the privacy of personal data of the victims, penalties regarding computer-related offenses, and finally, a clear definition and follow-up with the penalties for content-related offenses. The choice of QFD as the methodological backbone has been predicated on its proven systematic prowess in translating precise user requirements into concrete design qualities. Such a transformation becomes essential in the wake of manhandling complexity and dynamism, which is on increased hues getting witnessed in cybercrime scenarios. This research, therefore, focuses on fostering a strong legal framework in these key areas, not only to address the existing deficiencies but also to cater for the challenges expected in future management of cyber-crime.

This research, through the QFD tool, endeavors to provide actionable insights and recommendations that could significantly improve the efficacy of strategies adopted by India in preventing cyber-crime and hence contribute towards an even more secure and resilient digital infrastructure. This really drives home not just the urgent necessity of more updated and comprehensive cyber-law statutes in India which should provide the benchmark for international best practice.

Keywords: Quality Function Deployment (QFD), Cyberlaw, Victim Management, Penalties for computer-related offenses, Sustainable Cyber-crime management systems, Crime prevention, IT Act-2000, EU- General Data Protection Regulation.

Introduction

Quality Function Deployment, a tool developed in Japan in the late 1960s, is primarily used in product design and development to translate customer requirements into specific company offerings. Its unique approach involves a systematic process that captures customer desires and finally it is translated into company capabilities, product features, or service designs. By applying this method to the legal system, this Chapter innovatively adapts QFD to a non-traditional domain. The aim is to systematically identify the "customer requirements" of society in terms of justice, fairness, and legal clarity, and to map these against the existing legal system's "product features."

The current legal system, while robust in many aspects, is not fool proof there exists some lacuna in some areas of our IT ACT-2000, issues such as lengthy court procedures, lack of accessibility, systemic biases, and the inability to keep pace with technological advancements plague legal systems. These challenges often result in disconnection between the legal framework and societal need. The chapter posits that applying QFD can uncover these discrepancies, providing a structured method to identify and address gaps in the legal system.

This study begins by detailing the methodology of QFD (Aigul R. Bizhanova et al., 2022; L. Chan, 2005; L.-K. Chan & Wu, 2002) and its potential adaptation for legal system analysis, it then delves into an examination of the current shortcomings within the legal framework, drawing on examples from various jurisdictions to illustrate global challenges. The integration of these two fields presents a novel approach to legal reform, offering a structured, customer-focused perspective that could lead to more effective and responsive legal systems.

This unique application of QFD (Belhe & Kusiak, 1996; Delgado-Hernandez & Aspinwall, 2008; Neeru et al., 2023; *QFD Institute Home - The Official Source for ISO 16355 Modern QFD*, n.d.; Tayntor, 2007) in cybercrime victim protection provides new dimension in defining and penalizing cybercrimes, along with stringent data confidentiality.

A Brief Overview of Sustainable Cyber Infrastructure

QFD (English, 1993; Olewnik & Lewis, 2008; Ramaswamy & Ulrich, 1993), traditionally is a tool for quality management in manufacturing and service industries, has seen limited but impactful applications in legal frameworks. Erdil and Arani (2019) highlight its potential beyond design, suggesting its utility in systematizing legal processes by transforming user demands into operational requirements. However, (L.-K. Chan & Wu, 2002) note a scarcity of research in applying QFD within legal systems, particularly in the context of cybercrime, indicating a significant gap in the literature.

The evolution of cybercrime laws has been a subject of much debate. (Jaishankar, 2011) and Gordon and (Gordon & Ford, 2006) discuss the complexities of defining and penalizing cybercrimes in the ever-evolving digital landscape. The need for adaptive legal frameworks that can respond to the dynamic nature of cybercrime is echoed in the work of (Ali et al., 2023), who emphasize the challenges faced by existing laws in keeping pace with technological advancements.

The GDPR in Europe has set a benchmark in data privacy and protection, offering a contrast to other legal systems such as India's IT Act 2000 (Ardiani et al., 2023; L.-K. Chan & Wu, 2002; Erdil & Arani, 2019), discusses the gaps in various national frameworks concerning data privacy, underscoring the importance of aligning with international standards like GDPR. This comparison is crucial in understanding the deficiencies in current legal systems regarding cybercrime and data protection.

There is a growing recognition of importance of a victim-centric approach in cyberlaw which is observed by the work of (Aigul R. Bizhanova et al., 2022; Shandil, 2023) pointing to the need for legal frameworks prioritizing the rights and protections of cybercrime victims, an aspect often overlooked in traditional lawmaking processes.

Despite the extensive research on cybercrime laws and data protection, there is a noticeable gap in the literature regarding the application of QFD (Batyrbek K. Yermekbayev et al., 2023; Masaki, 2016; Murat K. Shynybekov et al., 2023; Shandil, 2023) in these areas. While QFD has been successfully applied in various industries for quality and process improvement (Chandra et al., 2023; Yanita Mila Ardiani et al., 2022), its potential in legal system reform, especially in the context of cybercrime, remains largely unexplored. This gap presents an opportunity for this research to pioneer the application of QFD in enhancing cybercrime management and victim protection (Gordon & Ford, 2006; Jaishankar, 2011).

The study by (Kassa et al., 2024) provides a comprehensive review of the methods used to recognize cybercrime intentions. The authors systematically analyze various approaches and methodologies applied in the detection and prediction of cybercrime behaviors. Their work emphasizes the importance of advanced computational techniques, such as machine learning and artificial intelligence, in enhancing the accuracy and efficiency of cybercrime detection systems. The review identifies key gaps in existing literature, including the need for more sophisticated models that can adapt to the evolving tactics of cybercriminals, thereby laying the groundwork for future research in this area.

Understanding the human element in cybercrime is crucial, as highlighted by (Akdemir & Lawless, 2020). Their research explores the role of lifestyle and routine activities in increasing the risk of becoming a victim of cyber-enabled and cyber-dependent crimes. The authors adopt a lifestyle routine activities approach to examine how individual behaviors and choices make them susceptible to cybercrime. This study is significant as it shifts the focus from purely technological solutions to incorporating human factors in the prevention strategies against cybercrime. By acknowledging the behavioral patterns that contribute to victimization, this research offers valuable insights for developing more comprehensive and effective cybercrime prevention frameworks.

The effectiveness of local law enforcement in addressing cybercrime is another critical area of focus. (Davis, 2012) investigates the perceptions of local law enforcement officials regarding their role and effectiveness in combating crimes with a cyber component. The study reveals several challenges faced by law enforcement agencies, including limited resources, lack of specialized training, and the fast-evolving nature of cyber threats. Davis suggests that enhancing the capacity of local law enforcement through targeted training and resources is essential for improving their ability to handle cybercrime cases effectively. This research underscores the need for a multi-faceted approach that includes technological, human, and institutional perspectives in the fight against cybercrime.

(Furnell & Dowling, 2019) provide a detailed portrait of the current cybercrime landscape, discussing the various types of cybercrimes and the strategies employed to counter them. Their study highlights the importance of a dynamic and responsive approach to cybersecurity, considering the rapidly changing tactics employed by cybercriminals. The authors argue for the integration of continuous monitoring, advanced analytics, and international cooperation to effectively mitigate cyber threats. This comprehensive overview of the cybercrime landscape serves as a foundational reference for policymakers and practitioners in the cybersecurity domain.

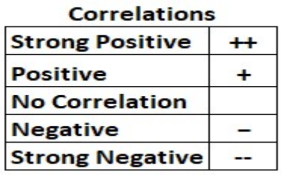
Integration of Quality Function Deployment in Knowledge Management

The integration of knowledge management systems into organizational frameworks can significantly enhance the response to cyber threats. (Reis et al., 2022) explore the application of Quality Function Deployment (QFD) as an integrative method for implementing knowledge management. Their study demonstrates how QFD can be used to align organizational knowledge with cybersecurity objectives, thereby improving the effectiveness of cyber risk management strategies. Similarly (Tan et al., 1998) emphasize the importance of QFD in designing information technology systems, including those related to cybersecurity. Their research provides a framework for incorporating customer and stakeholder requirements into the design process, ensuring that IT systems are robust, resilient, and capable of withstanding cyber threats.

The literature reviewed in this study provides a holistic view of the current state of research on cybercrime and the various strategies employed to mitigate its impact. From recognizing cybercrime intentions to understanding the human factors involved, the studies highlight the need for a comprehensive approach that integrates technological, human, and institutional perspectives. Additionally, the role of knowledge management in enhancing organizational resilience against cyber threats is emphasized, showcasing the value of adopting integrative methods like QFD. Future research should focus on developing more adaptive and predictive models that incorporate these multifaceted aspects, ensuring a robust and sustainable defense against the ever-evolving threat of cybercrime.

Development House of quality

The development of House of Quality involves identification of requirements which are sustainable for both User's prospective as well as law Enforcement Agencies. The steps involve use of competitive assessment by benchmarking the existing Indian cyber law against European GDPR (General Data Protection Regulation). We will be searching for the solutions for WHATs of the Cyber Users / Internet users and implement using Information Technology Act-2000 and European GDPR. If the European GDPR scores better in meeting the WHATs of the user, then Information Technology Act-2000 needs to be amended.



Correlations

Strong Positive	++
Positive	+
No Correlation	
Negative	−
Strong Negative	--

Figure 1: Relationship between Technical Descriptors and Customer's Requirements

Step 1: The first step involves listening to customers' requirements in the form of (WHATs) to analyze what the customer wants. In our case it is the cyber users or Internet users and What they want from enforcement Agencies like Legal system and Police, it is categorized into three most important requirements of the users which is stated as:

- Confidentiality of personal data
- Computer related offense with penalties
- Content related offence definitions with penalties

Step 2: Second step involves list of Technical Descriptors (HOWs). After finalizing the needs of the customers, we must check its feasibility that can be done by WHAT's the counterpart characteristics that can be possible for the probable requirement in technical language it is defined as achieving the system level specification to part level specification (A. Sharma et al., 2023; J. Sharma et al., 2023).

Step 3: Third step deals with developing the relationship matrix between WHATs and HOWs. The general principle followed in finding out the relationships between customer requirement add technical descriptors is to use L shaped Matrix. This L-shaped link shows the interaction of distinct items. They are related to each other by the symbol carrying weight score as shown in figure 3.

Step 4: Develop and Inter-relationship matrix of HOWs: in this step we double up the Roof of HOQ (House of Quality) which represents the relationship between technical descriptors, in our case it is the functional requirement represented as in figure 2.

Step 5: Competitive Assessment: It represents block of columns related to every customer's requirement in the House of quality on the extreme right-hand side of the relationship.

Relationships		
Strong	●	9
Moderate	○	3
Weak	▽	1

Figure 2: Inter-Relationship of House of Quality

The numbers 1 through 5 are listed where rating of 1 represents the worst and 5 represents the best. This column is where the QFD team decides whether they want to keep their product unchanged, improve the product, or make the product better than the competitor. In this research, it is the existing Indian legal framework compared with the European Union.

Technical Competitive assessment incorporates the probability of achieving the objective value with a higher probability of success, in this case the set of rows corresponding to each technical descriptors are represented by the values ranging from 1 to 5, with 5 being the highest rating.

Step 6: The practice customer requirement makes up a block of columns corresponding to each customer's requirements in the House of quality on the right-hand side, it is rated from 1 to 10, where 1 represents least important and 10 represents the most important.

Besides this there are other important dimensions which provides significant value addition in calculating the outcome of QFD which are stated as:

Target Value: It evaluates each customer's requirements and thereby sets a new assessment value in the improved version of existing product as we can see from the QFD diagram the User's privacy of **IPDB** is "3" and Data Privacy as EGDP has already set the target as "4" now in order to compete with EGDP we have to assign the Target value as "4", which means we must improve Data Privacy part in order to cope up with EGPD.

Scale-Up factor: It is the ratio of the product-rating given by customer competitive assessment. The higher its value the more the effort required to achieve it. For example, take the case of "User Privacy", here how much development is expected. Here the scale-up factor represents the division of "Target Value" by the "User's Privacy" given under the column of customers with Indian Personnel Data Protection (IPDP), the customer rating "3" and the target value is "4", then the scale-up factor is "1.3".

Sales-Point: The sales-point gives an idea about how much the customer (Cyber Users) requirements [24,25,26] will be helpful in curbing the menace of Cyber Crime it strengthen the Best Customer Requirements.

Absolute Weight: Absolute Weight can be calculated by multiplying the importance to Customer, Scale-up factor, and Sales Point.

AbsoluteWeight= (Imporance to Customer). (Scale-Up Factor). (SalesPoint)

It is the overall customer weightage of each of the factors selected. For example, the absolute weight for "Users Privacy" is calculated as

$$\text{AbsoluteWeight\_UserPrivacy} = 8\times1.3\times1.5 = 15.$$

Step 7: Develop Prioritized Technical Descriptors: It refers to the Technical Descriptors defined through the Functional Requirement at the TOP left corner like: User Data Encryption Techniques, obtaining explicit consent for Data collection and Use, Adhere to Data Minimization etc. It enables to identify the Technical Descriptors that should be given highest priority to fulfil the cyber-User's requirements and improvement needed. It is represented by various sub domains like:

Degree of Difficulty: The Degree of Technical difficulties in achieving such infrastructural requirement to safeguard the Cyber User is expressed within the range of *1(least difficult) to 10(Very Difficult).*

Target Value: It tells how much more effort and improvement is required to improve the security of the User such that it meets the expectation of the User. It ranges from "0" to "5".

Absolute Weight: The Absolute Weight:

$$[\ a\_j = \sum\_(i = 1)\hat{}n ▒ R\_ij \ \ C\_j\ ]$$

where:

a_j= Row Vector of absolute weights for the Technical Descriptors.

R_ij = Column in Relationship matrix

C_i = Column of Importance to Customers.

For example, let us take the case of "Obtain Explicit consent for collection and use". We take the Dot Product of the Column in the relationship Matrix band the column in the relationship matrix for "Importance to Customers." which is calculated as:

$$= 9 \times 8 + 9 \times 5 + 9 \times 5 + 0 \times 1 = 162$$

The greater the value of Absolute weight indicates that User are very concerned about the Privacy of any organization dealing with User's information, they are bound to disclose the Usage of personal information to the Users.

Relative Weight: Relative Weight is calculated by replacing the Degree of importance for the customers (Users)

requirements with the Absolute Weight for the Customer's requirements.
It is calculated using the formula:

[b_j = ∑_(i = 1)^n▒R_ijd_i]

where:

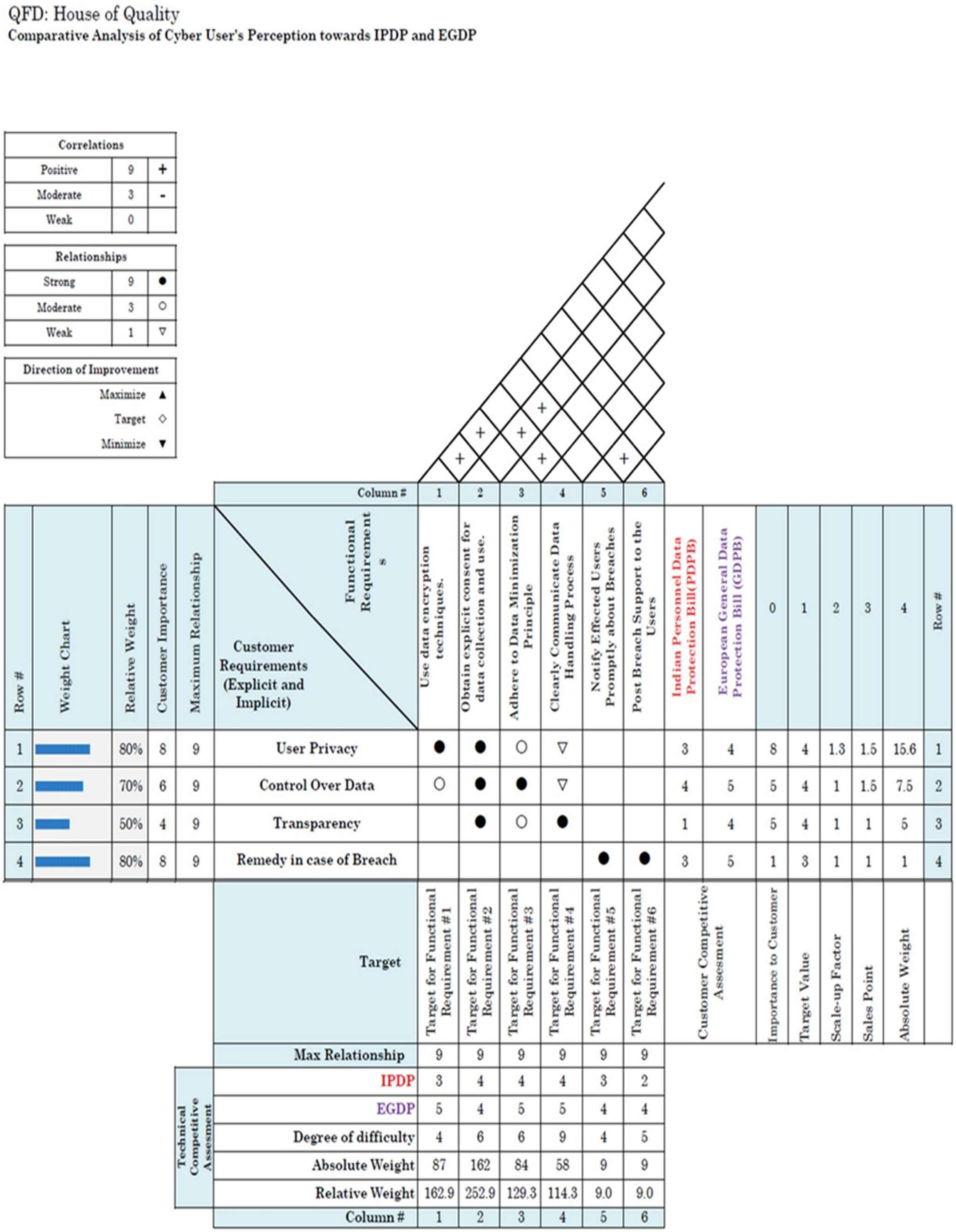
bj=Row Vector of Relative weights for Technical Descriptors

di= Column Vector of Absolute Weights for Customer's requirements

The higher the value of Absolute and Relative ratings the higher is the Effort required at the infrastructure level as well as Law enforcement Agencies.

The use of these Charts is independent of the type of product or services it is used for, it provides the best comparative Analysis of two or more parties on the same parameters.

By consistently applying QFD, organizations and law enforcement agencies can make well-informed decisions to strengthen the legal framework and effectively curb cybercrime. The methodology's versatility allows it to be applied across various products and services, providing a comparative analysis on the same parameters.



QFD: House of Quality

Comparative Analysis of Cyber User's Perception towards IPDP and EGDP

Correlations		
Positive	9	+
Moderate	3	-
Weak	0	

Relationships		
Strong	9	●
Moderate	3	○
Weak	1	▽

Direction of Improvement	
Maximize	▲
Target	◇
Minimize	▼

					Column #	1	2	3	4	5	6								
Row #	Weight Chart	Relative Weight	Customer Importance	Maximum Relationship	Functional Requirements Customer Requirements (Explicit and Implicit)	Use data encryption techniques.	Obtain explicit consent for data collection and use.	Adhere to Data Minimization Principle	Clearly Communicate Data Handling Process	Notify Effected Users Promptly about Breaches	Post Breach Support to the Users	Indian Personnel Data Protection Bill(PDPB)	European General Data Protection Bill (GDPB)	0	1	2	3	4	Row #
1	▬▬▬▬	80%	8	9	User Privacy	●	●	○	▽			3	4	8	4	1.3	1.5	15.6	1
2	▬▬▬	70%	6	9	Control Over Data	○	●	●	▽			4	5	5	4	1	1.5	7.5	2
3	▬▬	50%	4	9	Transparency		●	○	●			1	4	5	4	1	1	5	3
4	▬▬▬▬	80%	8	9	Remedy in case of Breach					●	●	3	5	1	3	1	1	1	4
					Target	Target for Functional Requirement #1	Target for Functional Requirement #2	Target for Functional Requirement #3	Target for Functional Requirement #4	Target for Functional Requirement #5	Target for Functional Requirement #6	Customer Competitive Assesment		Importance to Customer	Target Value	Scale-up Factor	Sales Point	Absolute Weight	
					Max Relationship	9	9	9	9	9	9								
				Technical Competitive Assesment	IPDP	3	4	4	4	3	2								
					EGDP	5	4	5	5	4	4								
					Degree of difficulty	4	6	6	9	4	5								
					Absolute Weight	87	162	84	58	9	9								
					Relative Weight	162.9	252.9	129.3	114.3	9.0	9.0								
					Column #	1	2	3	4	5	6								

Figure 3: QFD showing the relationship between WHAT Cyber Users wants and what Legal and Infra Facilities available.

Conclusion:

QFD serves as a powerful tool to bridge the gap between customer expectations and technical implementation (Dwiki, 2018). It empowers businesses and authorities to proactively address the needs of cyber users and prioritize efforts to enhance data security and user privacy. The continuous application of QFD can lead to a more efficient and user-centric legal framework, fostering a safer and more trustworthy digital environment for all.

QFD matrix provides an exhaustive overview where we stand in terms of Information Technology Act-2000 on Indian Personnel Data Protection (IPDP) in comparison to EGDP. Overall various parameters are compared in relation to the Societal expectations and the areas which needs enforcement. The planning matrix contains the target values of “HOWs”, which might be determined based on expert opinion.

From the Output of the QFD we can Analyze the Outcome as:

Table 1. QFD Analysis.

	Protection of personal data	**Stringent penalties for cybercrime**	**Clear Definitions of cybercrimes**
Information Technology Act, 2000 (ITA 2000) exists	Strong	Moderate	Strong
Some penalties under ITA 2000	Not Related	Strong	Moderate
Some definitions under ITA 2000	Moderate	Moderate	Strong

Finally, this study provides a groundbreaking perspective on employing Quality Function Deployment in legal system reform, particularly in the realm of cybercrime. It opens new avenues for research and practice, encouraging a proactive, systematic, and victim-focused approach to legal challenges in the digital age. As cyber threats continue to evolve, so must our methods of managing them, and this research contributes a vital piece to that ever-changing puzzle.

This research embarked on an innovative journey to explore the application of Quality Function Deployment (QFD) in the legal domain, particularly in managing cybercrime. Our study revealed critical gaps in the current legal system, especially in safeguarding cybercrime victims' rights and data privacy. The use of QFD translates complex user requirements into actionable legal frameworks, focusing on three pivotal areas: Confidentiality of victims' personal data, Penalties for computer-related offenses, and Defining content-related offenses.

Implications of the Research

The application of QFD in cybercrime law has several significant implications related to sustainable Cyber Infrastructure:

1. Enhanced Victim Protection: Our research underscores the importance of a victim-centric approach in cybercrime legislation. By systematically incorporating victim needs into legal definitions and penalties, we propose a more empathetic and effective legal framework (Singh & Singh, 2023).
2. Dynamic Legal Frameworks: The dynamic nature of cybercrime necessitates adaptable legal systems. The use of QFD facilitates continual updates and refinements to laws, keeping pace with technological advancements and evolving cyber threats.
3. International Benchmarking: Comparing the Indian IT Act 2000 with the GDPR demonstrated the benefits of international benchmarking. This approach is vital for countries to align their cyber laws with global standards, ensuring comprehensive data protection and privacy.
4. Empowering Law Enforcement and Policy Makers: The findings provide valuable insights for law enforcement and policymakers. By prioritizing user (victim) requirements and adopting a structured approach to legal reform, we can enhance the efficacy of cybercrime management.

While this study marks a significant step forward, it is not without limitations. The primary constraint lies in the application of QFD, a method traditionally used in manufacturing, to the legal field. Further research is needed to refine these methodologies and test their effectiveness in diverse legal environments.

Furthermore, the calculation of absolute weights and relative weights provides a quantitative measure of the importance of each technical descriptor in meeting customer requirements. These metrics give valuable insights into the level of concern and the effort required to ensure robust cybersecurity and privacy measures.

References

Aigul R. Bizhanova, Aliya S. Koshkinbayeva, Gulmira A. Zhunisova, Gulaina Zh. Osmanova, Belkhozhayeva, D., & Dana S. Baisymakova. (2022). Regulatory Issues of Depollution in Kazakhstan. *Evergreen*, *9*(4), 903–908. https://doi.org/10.5109/6622877

Akdemir, N., & Lawless, C. J. (2020). Exploring the human factor in cyber-enabled and cyber-dependent crime victimisation: A lifestyle routine activities approach. *Internet Research*, *30*(6), 1665–1687. https://doi.org/10.1108/INTR-10-2019-0400

Ali, O., Krsteska, K., Said, D., & Momin, M. (2023). Advanced technologies enabled human resources functions: Benefits, challenges, and functionalities: A systematic review. *Cogent Business & Management*, *10*(2), 2216430. https://doi.org/10.1080/23311975.2023.2216430

Ardiani, Y. M., Kurniawan, K. R., & Lukito, Y. N. (2023). Anti-colonialism During Suharto's New Order Era and its Impact on Conservation of Architecture in Indonesia. *International Society for the Study of Vernacular Settlements*, *10*(8), 62–71. https://doi.org/10.61275/ISVSej-2023-10-08-05

Batyrbek K. Yermekbayev, Nazymkul V. Dzhangarasheva, & Gaukhar M. Rakhimzhanova. (2023). Overview of Grazing as a Land Use System in Kazakhstan. *Evergreen*, *10*(2), 658–666. https://doi.org/10.5109/6792812

Belhe, U., & Kusiak, A. (1996). The house of quality in a design process. *International Journal of Production Research*, *34*(8), 2119–2131. https://doi.org/10.1080/00207549608905017

Chan, L. (2005). A systematic approach to quality function deployment with a full illustrative example. *Omega*, *33*(2), 119–139. https://doi.org/10.1016/j.omega.2004.03.010

Chan, L.-K., & Wu, M.-L. (2002). Quality function deployment: A literature review. *European Journal of Operational Research*, *143*(3), 463–497. https://doi.org/10.1016/S0377-2217(02)00178-9

Chandra, A., Yadav, A., Singh, S., & Pawan Kumar Arora. (2023). Optimisation of Machining Parameters for CNC Milling of Fibre Reinforced Polymers. *Evergreen*, *10*(2), 765–773. https://doi.org/10.5109/6792826

Davis, J. T. (2012). Examining perceptions of local law enforcement in the fight against crimes with a cyber component. *Policing: An International Journal of Police Strategies & Management*, *35*(2), 272–284. https://doi.org/10.1108/13639511211230039

Delgado-Hernandez, D. J., & Aspinwall, E. (2008). Quality management case studies in the UK construction industry. *Total Quality Management & Business Excellence*, *19*(9), 919–938. https://doi.org/10.1080/14783360802224545

Dwiki, S. (2018). Development of Environmental Policy in Indonesia regarding Mining Industry in Comparison with the United States and Australia: The Lesson That Can Be Learned. *Evergreen*, *5*(2), 50–57. https://doi.org/10.5109/1936217

English, J. R. (1993). Quality Function Deployment: Integrating Customer Requirements into Product Design. *Journal of Quality Technology*, *25*(1), 63–64. https://doi.org/10.1080/00224065.1993.11979419

Erdil, N. O., & Arani, O. M. (2019). Quality function deployment: More than a design tool. *International Journal of Quality and Service Sciences*, *11*(2), 142–166. https://doi.org/10.1108/IJQSS-02-2018-0008

Furnell, S., & Dowling, S. (2019). Cyber crime: A portrait of the landscape. *Journal of Criminological Research, Policy and Practice*, *5*(1), 13–26. https://doi.org/10.1108/JCRPP-07-2018-0021

Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. *Journal in Computer Virology*, *2*(1), 13–20. https://doi.org/10.1007/s11416-006-0015-z

Jaishankar, K. (Ed.). (2011). *Cyber Criminology: Exploring Internet Crimes and Criminal Behavior* (0 ed.). Routledge. https://doi.org/10.1201/b10718

Kassa, Y. W., James, J. I., & Belay, E. G. (2024). Cybercrime Intention Recognition: A Systematic Literature Review. *Information*, *15*(5), 263. https://doi.org/10.3390/info15050263

Masaki, Y. (2016). Characteristics of Industrial Wastewater discharged from Industrialized Provinces and Specific Industrial Sectors in China based on the Official Statistical Reports. *Evergreen*, *3*(2), 59–67. https://doi.org/10.5109/1800873

Murat K. Shynybekov, Kurmankul T. Abayeva, Zhandos K. Rakymbekov, Andiya T. Serikbayea, & Faruza A. Toktasinova. (2023). Study of Natural Regeneration of Sogdian Ash (Fraxinus Sogdiana Bunge) and Silvicultural Measures to Promote it in the Sharyn River Floodplain of Almaty Region. *Evergreen*, *10*(2), 820–829. https://doi.org/10.5109/6792834

Neeru, Nitesh Singh Rajput, & Patil, A. (2023). Reducing Oil Leakage in Heavy Duty Transformers Made in Small-Scale Manufacturing Industry Through Six Sigma DMAIC: A Case Study for Jaipur. *Evergreen*, *10*(1), 196–211. https://doi.org/10.5109/6781070

Olewnik, A., & Lewis, K. (2008). Limitations of the House of Quality to provide quantitative design information. *International Journal of Quality & Reliability Management*, *25*(2), 125–146. https://doi.org/10.1108/02656710810846916

QFD Institute home – The official source for ISO 16355 modern QFD. (n.d.). QFD Institute - The Official Source for QFD. Retrieved August 30, 2023, from https://www.qfdi.org

Ramaswamy, R., & Ulrich, K. (1993). Augmenting the house of quality with engineering models. *Research in Engineering Design*, *5*(2), 70–79. https://doi.org/10.1007/BF02032576

Reis, L. P., Fernandes, J. M., Silva, S. E., & Pereira, A. D. S. (2022). Application of Quality Function Deployment as an Integrative Method to Knowledge Management Implementation. *Journal of Information & Knowledge Management*, *21*(02), 2250022. https://doi.org/10.1142/S0219649222500228

Shandil, P. (2023). A Survey of Different VANET Routing Protocols. *Evergreen*, *10*(2), 976–997. https://doi.org/10.5109/6793653

Sharma, A., Sharma, S., & Gupta, D. (2023). Ant Colony Optimization Based Routing Strategies for Internet of Things. *Evergreen*, *10*(2), 998–1009. https://doi.org/10.5109/6793654

Sharma, J., Tyagi, M., Bhardwaj, A., & Ravinderjit Singh Walia. (2023). Factors Assessment for Encumbering the Implementation of Sustainability Based Lean Six Sigma Practices in Food Supply Chain. *Evergreen*, *10*(1), 379–388. https://doi.org/10.5109/6781097

Singh, D., & Singh, A. (2023). Role of Building Automation Technology in Creating a Smart and Sustainable Built Environment. *Evergreen*, *10*(1), 412–420. https://doi.org/10.5109/6781101

Tan, K. C., Xie, M., & Chia, E. (1998). Quality function deployment and its use in designing information technology systems. *International Journal of Quality & Reliability Management*, *15*(6), 634–645. https://doi.org/10.1108/02656719810196234

Tayntor, C. (2007). *Six Sigma Software Development, Second Edition*. Auerbach Publications. https://doi.org/10.1201/9781420044287

Yanita Mila Ardiani, Kemas .R Kurniawan, & Yulia Nurliani Lukito. (2022). The Gap on Architecture Conservation Regulations from Colonial until Postcolonial Era in Indonesia. *Evergreen*, *9*(2), 594–600. https://doi.org/10.5109/4794207

KEY TERMS AND DEFINITIONS:

Quality Function Deployment (QFD) is a customer-focused process that systematically translates customer needs into specific technical requirements for product or service design. It aims to ensure that the final deliverable aligns closely with customer expectations and quality standards.

IT Act-2000 is a comprehensive law in India that provides a legal framework for electronic governance, cybersecurity, and the handling of electronic records and digital signatures. It also defines cybercrimes and prescribes penalties, aiming to promote secure electronic transactions and protect against cyber threats.

EU- General Data Protection Regulation is a comprehensive data privacy law that governs how personal data of EU residents must be collected, processed, and protected by organizations globally. It aims to enhance data privacy rights, ensure transparency, and impose strict penalties for non-compliance.

Sustainable Cyber Infrastructure refers to digital systems designed to minimize environmental impact while maintaining robust security, efficiency, and resilience. It integrates eco-friendly practices, such as energy-efficient data centers and sustainable resource management, to support long-term digital ecosystem stability.

Knowledge Management is about gathering, organizing, and sharing what an organization knows so that everyone can use it to work smarter and make better decisions. It's a way to ensure that important information and expertise are available when needed to help the organization grow and improve.

Behavioural Patterns of Cyber User describes the typical ways people act when they're online, like how they manage passwords, respond to security warnings, or use social media. These patterns help companies understand how users might accidentally or intentionally create risks in digital spaces.

Data Confidentiality is all about keeping sensitive information private and safe from people who shouldn't have access to it. Whether it's personal details, business secrets, or any other important data, confidentiality ensures that only the right people can see or use it, protecting individuals and organizations from harm.