

Information Technology Service Audit of Company X Using ITIL v4 Framework

Maria Christina Hartono^{a1}, Dwi Putra Githa^{a2}, Muhammad Alam Pasirulloh^{a3}

^a Department of Information Technology, Faculty of Engineering, Udayana University,
Bali, Indonesia

e-mail: ¹mariachristinahartono@gmail.com, ²dwiputragitha@gmail.com,

³muhammad.alam@unud.ac.id

Abstrak

Perusahaan X bertanggung jawab menyediakan air bersih bagi masyarakat, memiliki sistem informasi layanan konsumen untuk kemudahan akses informasi, pendaftaran sambungan air baru, dan pengaduan. Sistem ini masih menggunakan keamanan yang standar, beberapa kali terjadi masalah server down dan pelayanan TI yang perlu ditingkatkan performanya. Fokus penelitian menggunakan framework ITIL v4 subdomain Service Desk, Incident Management dan Information Security Management. Hasil pengukuran maturity level sistem informasi layanan konsumen sebelum pengumpulan bukti subdomain Service Desk berada di level 1, Incident Management dan Information Security Management berada pada level 0, sedangkan maturity level setelah pengumpulan bukti seluruh subdomain berada pada level 5. Hasil yang berbeda jauh menunjukkan kurangnya pemahaman pegawai terkait standarisasi layanan TI yang sudah dibuat sehingga diberikan rekomendasi berupa sosialisasi mengacu pada pedoman ITIL v4.

Kata kunci: Teknologi Informasi, Audit, ITIL v4, Maturity Level

Abstract

Company X is responsible for providing clean water to the community, has a customer service information system for easy access to information, registration for new water connections, and complaints. This system still uses standard security, several times there are server down problems and IT services that need to be improved. The focus of the research uses the ITIL v4 framework subdomains Service Desk, Incident Management and Information Security Management. The results of measuring the maturity level of the customer service information system before collecting evidence of the Service Desk subdomain are at level 1, Incident Management and Information Security Management are at level 0, while the maturity level after collecting evidence of all subdomains is at level 5. The significantly different results indicate a lack of understanding of employees concerning the standardization of IT services that have been made so that recommendations are given in the form of socialization referring to the ITIL v4 guidelines.

Keywords : Information Technology, Audit, ITIL v4, Maturity Level

1. Introduction

Information Technology (IT) services are an important element that provides various solutions and support to users in carrying out business activities [1]. IT services can be internal services aimed at units within the organization or external services offered to customers outside the organization. Speeding up and simplifying the service process and strengthening security can be done using information technology. The quality of IT services depends heavily on good management and a deep understanding of user needs, so that service providers can effectively meet customer expectations [2].

IT service audit is a systematic evaluation process of IT services to ensure that services operate in accordance with established procedures and policies. The audit process aims to measure the effectiveness of information technology management from several aspects such as

time, accuracy, availability, compliance, data integrity and data security [3]. IT service audits help companies to identify parts that need improvement and ensure that IT services provide added value to the business [4]. Audits also help reduce risks associated with information security and ensure that service quality is maintained [5].

Company X is a company responsible in the distribution of clean water through the service and distribution of clean water for the public in Bali. In line with its vision to realize excellent service towards an international standard company and in line with government targets, Company X needs to pay attention to information access services to the community to ensure sufficient and reliable water availability. Ensuring service availability and maintaining customer satisfaction certainly has a big effect on supporting government administration.

The customer service information system is a system built by Company X to provide easy access to information to the community as a water provider. The website-based customer service information system is used as a bridge between Company X and customers so that customers can register for new water connections, and make complaints. The customer service information system still uses standard security, several times there are server down problems and IT service services that need to be improved. Based on these problems, it is important to conduct an information technology service audit to support IT service operations and incident management.

Information technology service audit research using the ITIL v4 framework is not only limited to analyzing IT service problems, but also provides recommendations for gradually increasing maturity levels for company growth based on the ITIL v4 framework. The selection of the ITIL v4 framework is also very appropriate considering that the IT service being analyzed is the customer service information system with a long-term goal of integrating corporate practices in a sustainable manner and optimizing information technology service operations in more efficient water management.

2. Research Method

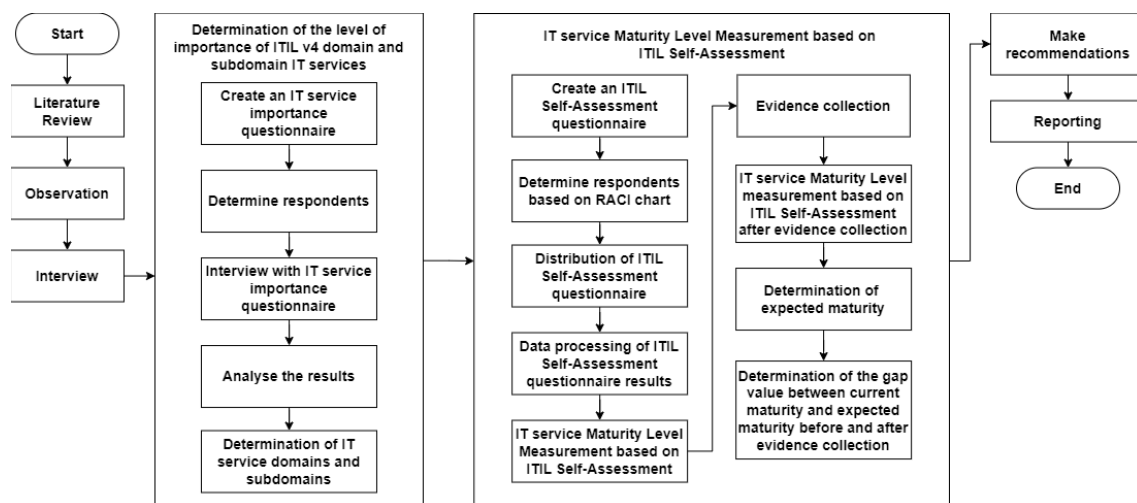


Figure 1. Research Flow

Data collection using observation, interviews and questionnaires. Determination of the level of importance of IT services is carried out to determine the scope of ITIL v4 domains and subdomains starting with making questionnaires, determining respondents, conducting interviews to fill out questionnaires, analyzing the results and determining the final ITIL v4 domains and subdomains. Measuring the maturity level of IT services based on ITIL Self-Assessment starts with making an ITIL Self-Assessment questionnaire based on ITIL v3 which has been adapted to ITIL v4 guidelines, determining respondents with a RACI Chart. Distribution of questionnaires is given to respondents according to the RACI Chart. Data processing of ITIL Self-Assessment questionnaire results is useful for recapitulating the results of questionnaires that have been filled out by respondents. The results of the questionnaire will be analyzed for the current maturity level

at a level between 1 and 5. Evidence collection is carried out as a validation of whether the output of the current maturity level of the ITIL Self-Assessment questionnaire are in accordance with existing evidence, evidence can be in the form of regulations, Standard Operating Procedures (SOP), reports or other evidence. Measurement of maturity level is done again after collecting evidence.

The results of the analysis are continued by discussing with the company regarding the higher target level that the company will achieve (expected maturity) between levels 1 to 5, where level 5 is the highest. The determination of the gap value is derived from the difference between expected maturity and current maturity [6]. Recommendations for improving service quality are given to help companies develop at the next level. These recommendations will later be reported to the company in the form of an information technology service audit report.

3. Literature Study

The literature review in this study is a theory sourced from books and journals related to information technology service audits using the ITIL v4 framework.

3.1 Information Technology Service Audit

An information technology service audit is a systematic evaluation process of IT services to ensure that services operate in accordance with established procedures and policies. The audit process aims to assess the effectiveness of information technology management from several aspects such as time, accuracy, availability, compliance, data integrity and data security [3]. IT service audits help companies to identify parts that need improvement and ensure that IT services provide added value to the business [4]. Audits also help in reducing risks associated with information security and ensuring that service quality is maintained [5].

3.2 ITIL v4

ITIL (Information Technology Infrastructure Library) is a framework that is used as a globally recognized standard in IT service management [2]. ITIL provides a framework that organizations can adopt to align IT services with business needs and improve overall service quality. ITIL covers various processes and functions related to service strategy, design, transition, operation, and continuous improvement.

ITIL v4 is the latest framework of ITIL containing practices regarding IT service management adapted to the utilization of modern technology. The previous version of ITIL, ITIL v3 focused on 26 processes covering various aspects of service management, ITIL v4 comes with the introduction of 34 practices that have integrated modern practices such as Agile, DevOps, and Lean. ITIL v4 is designed to ensure a flexible, coordinated, and integrated system for effective IT governance and service management [7]. ITIL v4 has 3 domains, namely General Management Practices, Service Management Practices, and Technical Management Practices [8].

3.3 Maturity Level

Maturity level in the context of information technology auditing refers to evaluating the extent to which an organization has reached a level of maturity in the management and implementation of IT-related practices. Evaluation of this maturity level is very relevant in understanding the extent to which the organization has optimized the use of information technology in its operations [6]. Details about the maturity level are available in Table 1.

Table 1. Maturity Level

Level	Index	Description
Level 0: Non-Existent	0,00-0,50	The company doesn't pay attention to the importance of the use of information technology by management.
Level 1: Initial	0,51-1,50	The company reactively implements information technology according to urgent needs, but there is no standardization.
Level 2: Repeatable	1,51-2,50	The company already has procedures in place for managing activities related to information technology governance, but

Level	Index	Description
		there has been no training or communication so its existence is not well-defined and remains formally inconsistent.
Level 3: Defined	2,51-3,50	The company already has formal and written standard procedures that are communicated to all stakeholders that must be adhered to and carried out in daily activities.
Level 4: Managed	3,51-4,50	The company already has a number of indicators that become targets in the application of information technology applications.
Level 5: Optimized	4,51-5,00	The company has implemented information technology management governance that refers to "best practice" or best practices through a process of continuous improvement and is able to adapt to company needs.

4. Results and Discussion

The outcome of the IT service audit research consist of analysis of determining the level of importance of IT services, determination of RACI chart, analysis results, gap analysis, and recommendation.

4.1. Analysis of Determining the Level of Importance of IT Services

The results of determining the level of importance of IT services are an important stage that determines the domains and subdomains that will be audited using ITIL v4. The respondents selected are the parties concerned about the customer service information system. Respondents are heads of fields who are authorized to make decisions related to IT services. Table 2 is the composition of respondent data on the IT service importance questionnaire.

Table 2. Respondents of the IT Service Importance Determination Questionnaire

Respondent	Position
I	Head of Information System Technology Unit
II	Head of Customer Department
III	Head of Distribution Department

Analysis of the results was carried out to analyze the recapitulation of the results of the questionnaire determining the level of importance of IT services using Mean of Importance (MOI). The questionnaire that has been filled in by the respondent is then summed and divided by the number of respondents, the subdomain with the highest value indicates that the subdomain has a higher priority for an IT service audit.

Table 3. Calculation Result of IT Service Importance Level Questionnaire

ITIL v4 Domain	ITIL v4 Subdomain	Respondent			Total Score
		I	II	III	
General Management Practices	Architecture Management	1	2	5	2.6
	Continual Improvement	1	1	5	2.3
	Information Security Management	4	4	4	4
	Knowledge Management	1	2	4	2.3
	Measurement and Reporting	1	1	3	1.2
	Organizational Change Management	1	1	4	2
	Portfolio Management	1	2	4	2.3
	Project Management	2	2	4	2.6
	Relationship Management	1	2	4	2.3
	Risk Management	2	1	4	2.3
	Service Financial Management	1	1	3	1.2
	Strategy Management	1	1	2	1.3

ITIL v4 Domain	ITIL v4 Subdomain	Respondent			Total Score
		I	II	III	
Service Management Practices	Supplier Management	3	2	4	3
	Workforce and Talent Management	1	2	4	2.3
	Availability Management	1	1	3	1.2
	Business Analysis	1	3	4	2.6
	Capacity and Performance Management	3	2	3	2.6
	Change Control	1	2	4	2.3
	Incident Management	3	2	4	3
	IT Asset Management	1	2	4	2.3
	Monitoring and Event Management	1	3	4	2.6
	Problem Management	3	2	4	3
	Release Management	3	1	4	2.6
	Service Catalogue Management	1	1	4	2
	Service Configuration Management	1	2	4	2.3
	Service Continuity Management	3	1	4	2.6
	Service Design	1	1	4	2
	Service Desk	3	2	4	3
	Service Level Management	1	1	4	2
	Service Request Management	3	1	3	2.3
	Service Validation and Testing	3	2	4	3
Technical Management Practices	Deployment Management	3	1	4	2.6
	Infrastructure and Platform Management	3	2	4	3
	Software Development and Management	3	2	4	3

The results of the calculation of the IT service importance questionnaire in Table 3 were then submitted to the company, the subdomains were sorted from the highest value to facilitate analysis. Subdomains that have the same value, further discussions are held with respondents to determine the prioritized part.

Table 4. Domain and Subdomain Determination Results

Domain ITIL v4	Subdomain ITIL v4	Total Score	Reason for Selection
General Management Practices	Information Security Management	4	Still using standard computer security
Service Management Practices	Incident Management	3	Several times there were server down problems that hampered performance
	Service Desk	3	Need to improve performance

4.2 Determination of RACI Chart

The determination of the RACI Chart is done to help avoid any overlap in roles and responsibilities, which can result in errors or double work. The preparation of the RACI Chart is done by evaluating the main duties and responsibilities of each party contained in company documents.

Table 5. RACI Chart

RACI	Respondent							
R = Responsible (The party performing the activity)	Head of Information Systems Technology Unit	Software Coordinator	Head of Customer Department	Head of Customer & Public Relations Section	Head of Distribution Department	Head of North Badung Distribution & Maintenance Section	Head of South Badung Distribution & Maintenance Section	Head of Meter Management Section
A = Accountable (The party that ultimately has the authority to ensure that a task or activity is successful)								
C = Consult (The party that needs feedback or suggestions and contributes to the activity)								
I = Inform (The party that needs to know the result of a decision or action)								
Information Security Management	A	R	C	I	C	I	I	I
Service Desk	C	I	A	R	C	I	I	I
Incident Management	A	R	A	R	A	R	R	R

4.3 Analysis Results

The results of the ITIL Self-Assessment questionnaire analysis aim to measure the maturity level of each audited subdomain. Table 6 is the result of the ITIL Self-Assessment questionnaire that has been distributed to 8 respondents.

Table 6. ITIL Self-Assessment Questionnaire Result	
Subdomain ITIL v4	Current Maturity (CM)
Service Desk	1
Incident Management	0
Information Security Management	0

The next stage is to collect evidence. Collecting evidence of IT service implementation is a validation stage to ascertain whether existing IT service regulations have been planned and implemented. Validation is done by analyzing whether it is appropriate between the output of the maturity level of the ITIL Self-Assessment questionnaire and the existing evidence. Evidence can be in the form of regulations, Standard Operating Procedures (SOPs), reports or other evidence. The maturity level measurement is carried out again after collecting evidence, then compared with the maturity level results before collecting evidence. Details about the maturity level after collecting evidence are available in Table 7.

Table 7. Maturity Level After Evidence Collection

ITIL v4 subdomain	Current Maturity (CM)
Service Desk	5
Incident Management	5
Information Security Management	5

4.4 Gap Analysis

Gap analysis is the gap between the current maturity level and the expected maturity level. The determination of the expected maturity level value is obtained based on the output of interviews conducted by Company X. Gap analysis before evidence collection using current maturity (CM) results of the ITIL Self-Assessment questionnaire. The gap analysis is visualized in the form of tables and spider charts.

Table 8. Gap Analysis Before Evidence Collection

ITIL v4 subdomain	Current Maturity (CM)	Expected Maturity (EM)	Gap (EM-CM)
Service Desk	1	5	4
Incident Management	0	5	5
Information Security Management	0	5	5

Based on the spider chart, it can be seen that the gap value for all subdomains is significantly different, namely 4 for the Service Desk subdomain and 5 for the Incident Management and Information Security Management subdomains. The gap analysis spider chart before evidence collection is illustrated in Figure 2.

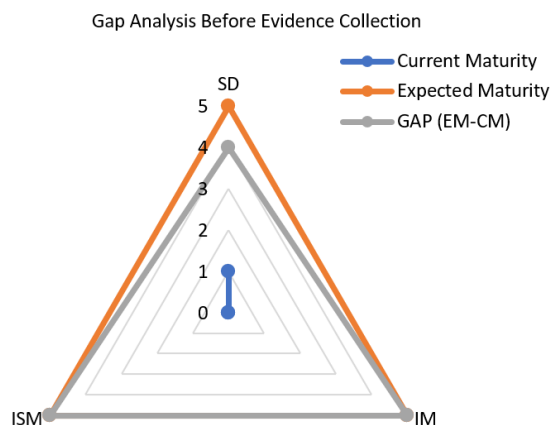


Figure 2. Gap Analysis Spider Chart Before Evidence Collection

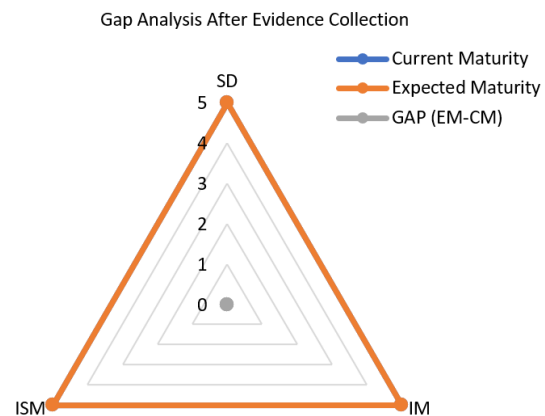


Figure 3. Gap Analysis Spider Chart After Evidence Collection

The gap analysis after evidence collection is the maturity level of the evidence collected as validation of the answers to each question of the ITIL Self-Assessment questionnaire. Details about the gap analysis after evidence collection are available in Table 9.

Table 9. Gap Analysis After Evidence Collection

Subdomain ITIL v4	Current Maturity (CM)	Expected Maturity (EM)	Gap (EM-CM)
Service Desk	5	5	0
Incident Management	5	5	0
Information Security Management	5	5	0

Current maturity of the customer service information system after collecting evidence of the Service Desk, Incident Management and Information Security Management subdomains is at

level 5. Expected maturity is at level 5, so the gap after collecting evidence of all subdomains is 0, which means it has reached expected maturity. The gap analysis spider chart after evidence collection is illustrated in Figure 3.

4.5 Recommendation

Based on the results of the gap analysis, the level of gap before and after evidence collection has very different results so that recommendations need to be given, namely conducting socialization to employees related to Service Desk, Incident Management and Information Security Management in order to improve employee understanding regarding the use of customer service information system services can be effective and optimal. Providing this recommendation is based on best practice in the ITIL v4 guidelines [8]. The following are recommendations that can be given to each subdomain.

Table 10. Service Desk Recommendation

No	Recommendation	
	Socialization Topic	Evidence of Socialization
	Service Desk Concept Description	Evidence of having conducted socialization related to the implementation of Service Desk: <ul style="list-style-type: none"> • Name of document: Minutes of Service Desk Socialization at Company X. • The contents of the report consist of: Date of implementation, time and place, purpose of implementation, list of participants, event agenda, materials, minutes during implementation, list of feedback questions from participants, attendance list of participants, and documentation during implementation consisting of photos or videos of implementation in addition to the signature of the Company X leader to prove the officiality of the report.
1	Service desk's main role as the main point of contact for managing all customer complaints or inquiries	
	Purpose and Benefits of Service Desk	
2	The purpose and benefits of a service desk to handle all complaints and service requests.	
	Management Commitment to Service Desk	
3	Commitment or support from management regarding budget, and adequate resources for effective Service Desk operations.	
	Service Desk Structure and Responsibilities	
4	Provide employees with an understanding of the workload and contribution of the service desk.	
	Service Desk Procedures and Policies	
5	Outline the various procedures and policies that apply such as procedures for obtaining necessary information from customers, procedures for managing service requests, assessment or classification of requests received, new service requests, and changes to services.	
	Training and Tool Functions for Service Desk	
6	Provide training and use tools for service desk operations	
	Compliance with Standards and SLAs	
7	Provide socialization related to standards and requirements that must be adhered to by the service desk team as well as an understanding of service level agreements (SLAs).	
	Collaboration between Teams and Departments	
8	The importance of collaboration between teams and other departments	

No	Recommendation	
	Socialization Topic	Evidence of Socialization
	Service Desk Management Weekly Reports and Meetings	
9	Delivery of making reports and holding weekly Service Desk management meetings to discuss service availability, customer satisfaction, and service issues	
	Monitoring Feedback from Users	
10	The importance of listening to feedback from users by conducting user satisfaction surveys	

Table 11. Incident Management Recommendation

No	Recommendation	
	Socialization Topic	Evidence of Socialization
	Incident Management Concept Description	<p>Evidence of having conducted socialization related to the implementation of Incident Management:</p> <ul style="list-style-type: none"> • Name of document: Minutes of Incident Management Socialization at Company X. • The contents of the report consist of: Date of implementation, time and place, purpose of implementation, list of participants, event agenda, materials, minutes during implementation, list of feedback questions from participants, attendance list of participants, and documentation during implementation consisting of photos or videos of implementation in addition to the signature of the Company X leader to prove the officiality of the report.
1	The main role of Incident Management to manage incidents, records, provide resolution and incident progress	
	Purpose of Incident Management	
2	The goal of Incident Management is to handle all incidents and service requests.	
	Management Commitment to Incident Management	
3	Commitment or support from management regarding reducing the impact of incidents with timely resolution, budget, and adequate resources for effective Incident Management operations.	
	Incident Management Structure and Responsibilities	
4	Provide employees with an understanding of Incident Management's workload and contributions.	
	Incident Management Procedures and Policies	
5	Outlines the various procedures and policies in place such as procedures for managing incidents, incident progress updates, violations and incident closure.	
	Incident Management Training and Tool Functionality	
6	Provide training and use tools for Incident Management operations.	
	Compliance with Standards and SLAs	
7	Socialization related to standards and requirements that must be adhered to by the Incident Management team as well as understanding related to service level agreements (SLAs).	
8	Collaboration between Teams and Departments	

No	Recommendation	
	Socialization Topic	Evidence of Socialization
	The importance of collaboration between teams and other departments	
	Incident Management Weekly Report and Meeting	
9	Submission of report generation and holding weekly Incident Management meetings to discuss service availability, customer satisfaction, and incidents.	
	Monitoring User Feedback	
10	The importance of listening to feedback from users by conducting user satisfaction surveys	

Table 12. Information Security Management Recommendation

No	Recommendation	
	Socialization Topic	Evidence of Socialization
	Information Security Management Concept Description	Evidence of having conducted socialization related to the implementation of Information Security Management: <ul style="list-style-type: none"> Minutes of Information Security Management Socialization at Company X. The contents of the report consist of: Date of implementation, time and place, purpose of implementation, list of participants, event agenda, materials, minutes during implementation, list of feedback questions from participants, attendance list of participants, and documentation during implementation consisting of photos or videos of implementation in addition to the signature of the Company X leader to prove the officiality of the report.
1	The main role of Information Security Management is to handle and mitigate information security.	
	Purpose and Benefits of Information Security Management	
2	The purpose and benefits of Information Security Management are to ensure the protection of company information by ensuring the confidentiality, integrity, and availability of information, so that organizational information is protected from unauthorized access and misuse.	
	Management Commitment to Information Security Management	
3	Commitment or support from management regarding budget, and adequate resources for effective Information Security Management operations.	
	Information Security Management Testing	
4	The importance of conducting tests such as software configuration, penetration testing on a regular basis to identify vulnerabilities in the system.	
	Information Security Management Structure and Responsibilities	
5	Provide understanding to employees for the workload and contribution of Information Security Management.	
	Information Security Management Procedures and Policies	
6	Outlines various procedures and policies in place such as security configuration procedures, data backup and recovery, risk	

No	Socialization Topic	Evidence of Socialization
	analysis procedures, protection of information assets, managing records of information security incidents and incidents, security controls.	
	Training and Tool Functions for Information Security Management	
7	Provide training and use tools for Information Security Management operations such as antivirus, firewall, encryption, or multifactor authentication.	
	Compliance with Standards and SLAs	
8	Socialization related to standards and requirements that must be complied with by the Information Security Management team and understanding related to service level agreements (SLAs)	
	Collaboration Between Teams and Departments	
9	The importance of collaboration between teams and other departments	
	Information Security Management Weekly Reports and Meetings	
10	Submission of reports and holding weekly Information Security Management meetings to discuss service availability, customer satisfaction, and incidents.	
	Monitoring User Feedback	
11	The importance of listening to feedback from users by conducting user satisfaction surveys	

An activity plan for the implementation of recommendations is made so that companies can more easily determine the priority scale of recommendations that need to be carried out or postponed for now. There are 3 socializations that can be carried out in 1 year, the distribution of this schedule is balanced because it can be adjusted to the schedule of Company X with a distance of 4 months between socializations. The implementation plan table is illustrated in Table 13.

Table 13. Recommendation Implementation Schedule

Recommendation	Month											
	1	2	3	4	5	6	7	8	9	10	11	12
Implementation of Service Desk recommendations	█											
Implementation of Incident Management recommendations					█							
Implementation of Information Security Management recommendations									█			

5. Conclusion

Based on the research outcomes, the conclusion is that the results of the questionnaire determining the level of importance of IT services to determine the scope of ITIL v4 domains and subdomains resulted in the selected domain being General Management Practices with the Information Security Management subdomain and the Service Management Practices domain with the Incident Management and Service Desk subdomains. Based on the results of the ITIL Self-Assessment questionnaire completed by 8 respondents, the maturity level of the customer service information system subdomain Service Desk is at level 1, meaning initial, Incident Management and Information Security Management are at level 0, meaning non-existent. Expected maturity is at level 5, then the gap value of the Service Desk subdomain is 4, Incident Management and Information Security Management is 5. Measurement of maturity level is carried out again after collecting evidence, the results of the customer service information system maturity level after collecting evidence of the Service Desk subdomain, Incident Management and Information Security Management are at level 5, then the gap value after collecting evidence of all subdomains is 0 which means it has reached the expected maturity. The recommendation given is to conduct socialization related to Service Desk, Incident Management and Information Security Management so that Company X employees better understand the operations being carried out.

References

- [1] D. Febrian, F. N. Salisah, Megawati, M. Afdal, and A. Marsal, "Evaluation of Maturity Level and Design of Incident Management SOP in Academic Information System Using ITIL v4," *Jurnal Teknik Informatika (JUTIF)*, vol. 5, no. 4, pp. 337–344, 2024, doi: 10.52436/1.jutif.2024.5.4.2286.
- [2] I. B. Suban, A. Wahju, and R. Emanuel, "Peran Framework ITIL V3 Mengukur Kualitas Layanan TI (Studi Kasus: Perpustakaan UAJY)," *Jurnal Informatika: Jurnal pengembangan IT (JPIT)*, vol. 5, no. 2, pp. 59–63, 2020.
- [3] M. K. Anam, A. R. Putra, S. Fadli, M. B. Firdaus, F. Suandi, and Lathifah, "Audit Teknologi Informasi Pada Sistem Perkreditan Online Terpadu Bank XYZ Cabang Perawang Menggunakan ITIL v3," *MISI (Jurnal Manajemen informatika & Sistem Informasi)*, vol. 3, no. 2, pp. 90–99, 2020.
- [4] I. A. H. Pradana, D. P. Githa, and I. P. A. Bayupati, "Service Audit in Filling Annual tax Return Using The Cobit 5 Framework at Tabanan Primary Tax service Office," *International Journal of Computer Applications Technology and Research*, vol. 8, no. 12, pp. 441–445, 2019.
- [5] A. A. N. A. Adityawinata, I. M. Sukarsa, N. Kadek, and N. K. D. Rusjyanthi, "Audit Layanan SKA (Surat Keterangan Asal) Untuk Barang Ekspor Menggunakan Framework COBIT 5," *Jurnal Ilmiah Merpati*, vol. 7, no. 2, pp. 103–112, 2019.
- [6] Z. S. Maharrani, L. P. Sumirat, and Y. Kristyawan, "Pengukuran Kinerja Sistem E-Learning UNITOMO Menggunakan Framework ITIL V4," *Progresif: Jurnal Ilmiah Komputer*, vol. 20, no. 1, pp. 529–539, 2024.
- [7] B. Putra, M. Jazman, M. Megawati, and F. N. Salisah, "IT Governance Audit at The Kampar Regency Library and Archives Department Using COBIT 2019 and ITIL 4," *Jurnal Teknik Informatika (Jutif)*, vol. 3, no. 6, pp. 1591–1600, 2022.
- [8] Axelos, *ITIL 4 Edition*. ITIL Foundation, 2019.