Jurnal Sistem Informasi Bisnis 04(2025)
Copyright ©2025, JSINBIS, p-ISSN: 2502-2377, e-ISSN: 2088-3587
On-line: http://ejournal.undip.ac.id/index.php/jsinbis/article/view/72634

Security Risk Management Assessment in Information Technology Services using Information Technology Infrastructure Library (ITIL) V4

Andys Sandra Kurniawan [a,*], Aris Puji Widodo[b], Adi Wibowo[c]

[a,b,c] Master of Information Systems, School of Postgraduate, Diponegoro University, Semarang, Indonesia

Submitted: April 23th, 2025; Revised: June 10th, 2025; Accepted: June 16th, 2025; Available Online: June 18th, 2025

DOI: 10.21456/vol15iss4pp469-480

Abstract

Information Technology (IT) is currently implemented in various fields of life, including in higher education. Information technology security is very crucial in higher education because cyber disruptions or attacks, such as malware, ransomware, and theft of personal data, can greatly affect teaching and learning activities and administration. Therefore, universities must be proactive in identifying risks, protecting sensitive data, and implementing effective security risk management to ensure the continuity of IT-based services. This study aims to measure capability and assess maturity levels of IT services, especially in risk management practices and information security management and analyze the level of gap between actual conditions that occur and expected standards. This study uses survey-based assessment using the ITIL V4 framework as a methodology. The results of the study indicate that the assessment of the level of maturity of higher education in managing IT service security risks, especially in both management practices, is at level 3 (Defined) with a maturity score of 3,48. These findings suggest that institutions have started to recognize the critical role of IT security risk management, with clearly defined practices and well-documented processes and activities already in place. Understanding the current capability and maturity levels offers valuable insight into areas that require enhancement, particularly in aligning with ITIL V4 standards. As a recommendation, institutions should focus on developing formal risk management policies, clarifying roles and responsibilities, enhancing technological infrastructure, conducting routine audits, and fostering strong organizational support with continuous evaluations to ensure effective and sustainable IT security risk management practices.

Keywords: ITIL V4 Maturity Model; Risk Management; Information Security Management; Capability level; IT Service Management

1. Introduction

Technological advancements are crucial for enhancing an organization's business operations. With the aid of Information Technology (IT), business processes can be conducted in a more efficient and effective manner Rais et al., 2024). Various sectors within organizations have started to incorporate information technology into their operational processes, including the education sector. Educational institutions, such as universities, need to manage their infrastructure effectively. According to Sukums et al (2023), universities, being institutions of higher education, are anticipated to leverage information technology to boost productivity in both academic and administrative areas, particularly regarding customer service management. Higher education requires good IT infrastructure management in order to provide maximum service to all users consisting of students, teaching staff or lecturers, education staff and all employees in the educational institution environment. One of the important services is academic services. In the current era of information technology, academic services are transforming into services based on information technology. Some IT-based academic services include electronic learning (E-Learning) using the Learning Management System (LMS), digital libraries (E-Library), online registration systems, academic assessment systems, administration systems, and so on (Setyaningsih et al., 2023). Along with the existence of information technology-based services, several problems have arisen. Several technical problems such as server down, slow systems, poor integration and system errors are common problems. Security, data and user issues are also important things that must be a concern for University managers (Rani et al, 2024).

Based on preliminary research data, it shows that Diponegoro University is highly dependent on IT to support academic activities, such as academic information systems, digital libraries, student and lecturer data management, and technology-based learning. However, disruptions or security attacks on IT infrastructure can have a major impact on the smooth operation of the university. In addition, cyber attacks such as malware, ransomware, or theft of personal data are increasing, so universities need to identify risks and ensure adequate mitigation.

*) Corresponding author: andysk@students.undip.ac.id

Copyright ©2025, JSINBIS, p-ISSN: 2502-2377, e-ISSN: 2088-3587
On-line: http://ejournal.undip.ac.id/index.php/jsinbis/article/view/72634

Higher education institutions in Indonesia are required to comply with various regulations related to data security and information technology, such as the Electronic Information and Transactions Law (UU ITE). Risk management assessments with frameworks such as ITIL V4 help ensure compliance with these standards. The use of IT is increasingly maximized to support the educational process, therefore providing optimal services is important (Yurisca Bernanda & Pangrestu, 2021). IT Service Management (ITSM) is a strategic method for planning, delivering, overseeing, and enhancing the use of information technology within an organization. (Sukums et al., 2023). ITIL is one of the most popular ITSM frameworks, including evaluation (Al Faruq, 2020). ITIL ranked first (47% of 261 IT leaders) among the five most widely used ITSM frameworks (N. K. Gunawan et al., 2020). The ITIL framework provides a set of concepts and policies for managing IT infrastructure, development and operations to align business needs with ICT services to improve the implementation of core functions (teaching, learning, research, administration and public services) in higher education institutions (Selvi Sabrina, Ilhamsyah, 2019). Universities as educational service providers need to know to what extent the services provided meet user needs. Therefore, a maturity level assessment is needed, especially for academic services for security risk management. Previous research used the ITIL V4 framework to evaluate IT service management in government agencies (Setyaningsih et al., 2023). The maturity level assessment is also used to evaluate IT service management incidents using ITIL V4 (Rani, et al, 2024). ITIL is used to assess the maturity of incident management in IT services and to conduct a gap analysis of current incident handling with incident handling in accordance with ITIL V4.

Most of the research on ITIL V4-based IT security risk management focuses on the industrial and business sectors (Lopes, 2021), (Hidayah et al., 2019) (H. Gunawan et al., 2024). However, the education sector, especially in universities, faces challenges such as the need for continuity of academic services, protection of sensitive data, and adaptation to new technologies. Implementation of ITIL V4 requires significant investment in infrastructure, training, and process adaptation (Al-Ashmoery et al., 2021). Several studies on educational institutions include research by Pratama & Umaroh (2024) measuring the maturity level of asset management at the General Finance Bureau (BKU) with Cobit 2019 and designing its management using ITIL V4. Another study used ITIL V4 to measure the maturity level and design operational procedures for incident management in the Academic Information System at an educational institution (Febrian, et al., 2024). Several studies related to the discussion of risk management, especially in educational institutions, have not been widely conducted. Based on this background, this study aims to: (1) measure the capability level of IT security risk management at Diponegoro University; (2) assess the maturity level according to ITIL V4 standards; and (3) analyze gaps between current and desired practices. By knowing the level of maturity of a management practice, the organization can measure the actual condition of the organization and can analyze the gap between the actual condition and the expected condition according to the ITIL V4 standard. This paper is written in a structured manner consisting of an introduction, Theoretical Framework, Methods, Results and Discussion, and Conclusion.

2. Theoretical Framework

Several theories are used to support research on security risk management assessment in information technology services using the ITIL V4 framework..

2.1. Information Technology Governance

IT governance is a subset of corporate governance that encompasses a series of reporting, planning, and performance reporting and review processes that involve decision-making. IT governance includes establishing performance metrics, controlling IT investments, providing and authorizing new or modified IT services, and ensuring compliance with regulations, organizational policies, and laws (H. Gunawan et al., 2024). Governance refers to a framework of policies, procedures, and practices that guide management, planning, and performance evaluation. It includes clearly defined decision-making rights, which establish control, authority, and performance indicators over investments, strategic plans, budgeting, service delivery, major organizational changes, as well as areas such as security, privacy, business continuity, and compliance with legal and internal regulations. (Selig, 2008).

2.2 Information Technology Service Management (ITSM).

Information technology service management (ITSM) is now an integral part of the organization. Efficient delivery of IT services is essential to ensure smooth operations, especially in the era of digitalization (Herlinudinkhaji & Kurnia Ramadhani, 2023). A service is a method of delivering value to both internal and external customers by enabling them to attain desired outcomes, while minimizing associated risks and costs. (Lopes, 2021). So ITSM is an approach to managing information technology that seeks to align business objectives with IT operations, ensuring the delivery of efficient, effective services while upholding established quality standards. (H. Gunawan et al., 2024).

2.3. ITIL V4 Framework

Information Technology Infrastructure Library (ITIL) is a general guide that presents best practices in

Copyright ©2025, JSINBIS, p-ISSN: 2502-2377, e-ISSN: 2088-3587
On-line: http://ejournal.undip.ac.id/index.php/jsinbis/article/view/72634

IT service management. There is a framework that emphasizes continuous evaluation and improvement of IT service quality, which is used to manage and organize IT services efficiently and effectively in ITIL (Rais et al., 2024). In its current development, ITIL is at version 4. In the previous version, namely V3, the implementation focused on the process, while in V4 it focuses more on the elements needed to create value for customers and all stakeholders that can provide business value benefits for the organization (Herlinudinkhaji & Kurnia Ramadhani, 2023). ITIL 4 offers essential guidance for organizations to address emerging challenges in service management and to leverage contemporary technologies. It is structured to support a flexible, cohesive, and integrated approach to governing and managing IT services effectively. (Axelos, 2019). There are several things that are the main discussion in ITIL 4 including the dimension model, Service Value System (SVS), and Service Value Chain (SVC).

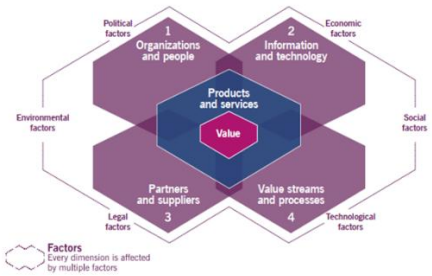


Figure 1. Dimensions In ITIL V4 Services

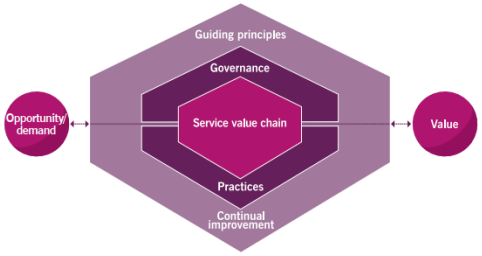


Figure 2. Service Value System (SVS) in ITIL V4

2.3.1. Dimension Model of Service Management

ITIL 4 presents a holistic approach, divided into four dimensions that have the main objective of providing value to ICT services to customers and stakeholders (Lopes, 2021), as can be seen in Figure 1 (Axelos, 2019).

The first dimension of service management focuses on organizations and people. An organization's success cannot rely solely on its formal structure or authority systems; leadership must also actively promote and embody core values. The second dimension involves information and technology, with in-depth insights available in other ITIL resources. The third dimension emphasizes partners and suppliers, recognizing that both organizations and their services depend on external contributions. Lastly, the fourth dimension, value streams and processes, encompasses the necessary activities, workflows, controls, and procedures needed to accomplish established objectives.

2.3.2. Service Value System (SVS)

ITIL 4 relies on the Service Value System (SVS) approach and the 4-Dimensional Model as key elements of the ITIL 4 framework. The Service Value System (SVS) focuses on how to collaborate activities to deliver IT services, while the 4-dimensional model discusses how to think about IT services and the aspects that need to be considered in delivering those services (Axelos, 2019). In the latest version of ITIL, namely ITIL 4 and its new conceptual model in general, there are several key elements, namely the service value system (SVS) shown in Figure 2.

The ITIL Service Value System (SVS) outlines how an organization's elements and activities collaborate to deliver value through IT-enabled services. Its flexible structure demands effective coordination to maintain organizational consistency.

ITIL SVS supports this by offering integrated guidance and a unified, value-driven direction. The ITIL SVS which is shown in figure 2, consists of five core components: 1) the service value chain, 2) practices, 3) guiding principles, 4) governance, and 5) continual improvement. The service value chain offers a flexible operational model for creating and enhancing services through six key activities. ITIL practices complement this by supporting various value chain activities, enabling adaptable service management. Guiding principles promote consistent decision-making, while governance ensures alignment with strategic goals. Continual improvement underpins all components, helping organizations stay resilient and responsive to change.

2.3.3. Service Value Chain (SVC)

In ITIL 4, every practice plays a role in supporting the service value chain. This value chain serves as an operational model that outlines the essential activities needed to address demand and support the development and management of products and services. Within the Service Value System (SVS), the service value chain functions as a flexible framework for delivering, creating, and continually enhancing services.(Lopes, 2021). There are six activities in the service value chain that lead to the creation of products and services, namely plan, improve, engage, design and transition, obtain/build, and deliver and support (Ilyasa & Bisma, 2022) (Axelos, 2019). The service value chain is shown in figure 3.

The activities in the service value chain as shown in Figure 3 reflect the stages an organization takes to create value, with each activity transforming inputs into outputs. Inputs can come from external demand or from other activities, and all activities are interconnected and trigger subsequent actions.

Copyright ©2025, JSINBIS, p-ISSN: 2502-2377, e-ISSN: 2088-3587
On-line: http://ejournal.undip.ac.id/index.php/jsinbis/article/view/72634

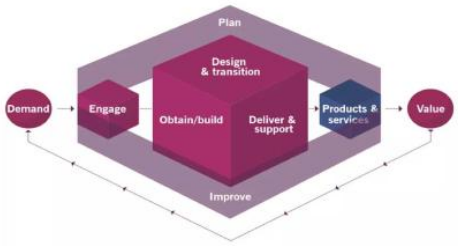


Figure 3. Service Value Chain in ITIL V4

2.3.4.ITIL Maturity Model

The ITIL maturity model is one of the most important models in IT, focusing on service management to evaluate the maturity level of an IT service organization. (Ahmad & Shamsudin, 2013). The ITIL maturity model helps organizations assess the capabilities and maturity of their Service Value System (SVS) in a clear and objective way. The main goal of this assessment is to guide improvement planning by identifying areas that need enhancement. (Axelos, 2021).

The assessment of an organization's service management capability (Practice Capability Level) is based on evidence of meeting criteria for the 34 ITIL management practices. The assessment of an organization's maturity (SVS Maturity Level) relies on evidence of meeting criteria for the five key components of the Service Value System (SVS).

a. Practice Capability Level

Assessment capability level is one of the maturity assessment models in the ITIL framework to measure the capability of a service management practice implemented in an organization. In ITIL v4 there are 34 practices that can be assessed (Axelos, 2021). In each management practice there is a scale that applies to measure the level of capability or ability as shown in Table 1.

For each practice, specific capability criteria are defined for each capability level. These criteria are designed to thoroughly assess the practice's ability to meet its objectives, and are based on Practice Success Factors (PSFs). Each PSF includes several criteria, and fulfilling these ensures the practice's objectives are achieved.

b. Maturity level assessment

The ITIL maturity model has five levels as shown in Table 2 (Pratama and Umaroh, 2024). Before reaching the next maturity level, activities and processes from the lower level must be completed by creating conditions to move to the higher level. A Likert scale can be used to measure the level of achievement of individual indicators which are then evaluated by applying statistical methods. The maturity levels in ITIL V4 are shown in Table 2.

c. Measurement value range

The assessment of the maturity level of practice shown in Table 2

Table 1. ITIL management practice capability levels

Level	Description
1	Practice is still intuitive and unstructured, so that goal achievement is often not fully optimal.
2	This practice achieves its goals systematically through basic activities supported by dedicated resources.
3	The practice is clearly structured, supported by dedicated resources, and integrated with other practices in the service management system.
4	Practices are run in a highly organized manner and evaluated on an ongoing basis within a service management system.
5	This practice continuously improves the organization's capabilities in line with its goals.

Table 2. Maturity Levels in ITIL V4

Maturity level	Description
Initial	The work has been completed, but the full purpose and intent of the focus area has not been achieved.
Managed	Performance planning and measurement already exist, although not in a standardized way.
Defined	Organizational standards provide guidance across the organization.
Quantitative	Organizations are data-driven, with quantitative performance improvements.
Optimizing	Organization focused on continuous improvement

is determined based on the average score of the capability level of all assessed practices (Pratama and Umaroh, 2024). The range of values for determining the maturity level is shown in Table 3.

3. Methods

3.1. Research Materials and Tools

This research was conducted at the Directorate of Data and Information Systems at Diponegoro University. This unit is tasked with creating policies related to Information and Communication Technology (ICT) at Diponegoro University. These policies include the Organizational Structure and Governance for ICT, Infrastructure and Network Development Policy, Application and Information System Development Policy and Human Resources Policy for ICT.

The material for this study is in the form of data on Information Technology (IT) infrastructure management and IT infrastructure usage management at Diponegoro University. The tools used are in the form of a list of questions for interviews with senior management, users and stakeholders related to the management of information technology for academic services at Diponegoro University.

The questionnaire was completed by 125 respondents who were informed of the study's objectives and provided consent prior to participation. The instrument consisted of 25 statements aligned

Copyright ©2025, JSINBIS, p-ISSN: 2502-2377, e-ISSN: 2088-3587
On-line: http://ejournal.undip.ac.id/index.php/jsinbis/article/view/72634

with the ITIL V4 practice dimensions and assessed using a 5-point Likert scale, where 1 indicated strong disagreement and 5 indicated strong agreement.

To ensure the quality of the instrument, both validity and reliability tests were conducted. Conceptually, content validity was established through a review of the questionnaire items by experts in IT service management and ITIL V4 to ensure that each statement accurately reflected the intended dimensions and practices. This process ensured alignment between the measurement indicators and the constructs being assessed, thereby supporting the instrument's relevance and representativeness.

Reliability was tested using Cronbach's Alpha, with results indicating acceptable internal consistency of the questionnaire. This combination of conceptual and statistical validation strengthens the credibility of the data collected for assessing the maturity of IT risk management and information security practices.

3.2. Research Procedure

The research method used in this study is quantitative descriptive with an inductive approach. The qualitative descriptive method is a type of quantitative data analysis that helps summarize, describe, or present data in a clear way. It focuses on statistical descriptions to better understand data by identifying patterns and summarizing details from specific samples (Aziza, 2023). While the approach used is an inductive approach, namely an approach that describes problems in case studies by referring to facts in the field, then analyzed to find solutions in the form of recommendations and conclude the results (Ilyasa&Bisma, 2022). There are steps taken in conducting research as shown in the following figure 4.

In this literature study, the researcher conducted a literature study from several journals and articles that discuss information technology service management. In addition, the researcher also conducted a literature study on the utilization of the ITIL version 4 framework, especially in incident management and security in information technology service infrastructure. Data collection was conducted through observation, interviews and questionnaires. Observations were conducted on several objects including: a) IT service operational processes; b) Physical and logical infrastructure (servers, networks, software); c) Security practices implemented (firewall). The instrument in this observation uses ITIL V4, focusing on the domains of risk management, information security management and continual improvement. Determining the sample using the Lemeshow formula with a total of 125 respondents.

$$n = \frac{Z^2 1-\alpha/2 P(1-P)}{d^2} \quad (1)$$

Description:
n = number of samples
Z = z score at 95% confidence = 1.96
P = maximum estimate = 0.5

Table 3. Range of maturity score

Score range	Maturity score	Level maturity
0 – 0,50	0	Incomplete
0,51 – 1,50	1	Initial
1,51 – 2,50	2	Managed
2,51 – 3,50	3	Defined
3,51 – 4,50	4	Quantitative
4,51 – 5,00	5	Optimizing

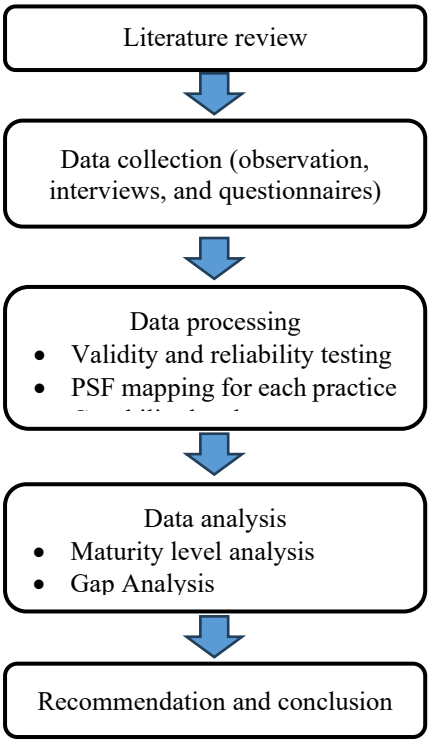


Figure 4. Research steps for assessing maturity levels using ITIL V4

in the equation calculated with the n value is 96.04 = 100 people so that in this study took data from a sample of at least 100 respondents. In this study will use a sample of 125 respondents or 20% to avoid respondents who do not complete the data entry in this study (drop out).

At the data processing stage, validity and reliability tests are carried out on the results of the questionnaires that have been filled out by respondents. The test is carried out to determine whether the questions given can be met or not. After that, a Practice Success Factor (PSF) mapping is carried out on each assessed practice. This mapping aims to determine the criteria contained in each assessed practice. Each criterion in each PSF is then calculated for its capability level to then be assessed for maturity. The maturity score range is set as in Table 3. The equation for the validity test using the Pearson Product Moment formula is as follows:

Copyright ©2025, JSINBIS, p-ISSN: 2502-2377, e-ISSN: 2088-3587
On-line: http://ejournal.undip.ac.id/index.php/jsinbis/article/view/72634

$$r_{xy} = \frac{n(\sum XY) - (\sum X)(\sum Y)}{\sqrt{\{n\sum X^2 - (\sum X)^2\}\{n\sum Y^2 - (\sum Y)^2\}}} \quad (2)$$

Description:
r = Correlation coefficient (r-count)
n = Number of respondents
X = Score of each question item
Y = Total score of all items for each respondent

Meanwhile, Reliability is tested using Cronbach's Alpha to see internal consistency with the following equation.

$$\alpha = \frac{k}{k-1}\left(1 - \frac{\sum \sigma^2_{item}}{\sigma^2_{item}}\right) \quad (3)$$

Description:
α = Cronbach's Alpha
k = Number of items in the questionnaire
σ²_item = Variance of each item's score
σ²_total = Total variance of overall score
Criteria:
α ≥ 0.7 = Reliable (consistent instrument)
α < 0.7 = Not reliable (needs improvement)

After analyzing the capability level for each practice, then the maturity level analysis and ITIL V4 gap analysis were carried out. The maturity level analysis is carried out by calculating the weight of each attribute value of the question, then adding it up and dividing it by the result of the number of questions, multiplied by the number of respondents, resulting in an average maturity level score with Equation 4 (Putri & Nuryana, 2024).

$$Assessment = \frac{\text{sum of the total values in the criteria x respondents who chose}}{\text{number of questions x number of respondents}} \quad (4)$$

The gap analysis stage has the objective of evaluating the gap that occurs between current incident handling and incident handling based on the ITIL V4 framework. The calculation of the gap analysis is formulated with the following equation:
Gap analysis = Expectation level - Maturity level (5)

In the final stage, the researcher concludes the findings from the interviews and recommendations based on the results of processing and analyzing data from the previous process. These findings and recommendations are compiled following the best practices in ITIL V4 Service Management Practices.

4. Result and Discussion

4.1. Result

4.1.1 Maturity Level of Security Risk Management in Academic Services in Higher Education using ITIL V4

The data processing process obtained from questionnaires that have been distributed to respondents and processed using the help of SPSS software version 25.

a. Validity test

The next step is to conduct a validity test that aims to measure whether the questionnaire is appropriate and valid in measuring the variable in question. The validity test was carried out using the Pearson Product Moment correlation formula with a pilot-test as an initial test of the research instrument in a small number of respondents before the main study was conducted, in this study using 30 respondents. The results of the test validity are as follows Table 4.

An indicator is said to be valid in a validity test if the r-count value is greater than the r-table value. Table 4.1 The r-table value is 0.512, each indicator has a r-calculation value greater than 0.512, so all indicators are declared valid. based on Table 4 shows that for each indicator makes a significant contribution to the assessment of aspects of academic services using the ITIL V4 framework.

Table 4. Validity test results

Indicator	r-count	r-table	Description
I1	0,664	0,512	Valid
I2	0,565	0,512	Valid
Indicator	r-count	r-table	Description
I3	0,700	0,512	Valid
I4	0,965	0,512	Valid
I5	0,850	0,512	Valid
M1	0,580	0,512	Valid
M2	0,563	0,512	Valid
M3	0,665	0,512	Valid
M4	0,750	0,512	Valid
M5	0,760	0,512	Valid
D1	0,800	0,512	Valid
D2	0,675	0,512	Valid
D3	0,770	0,512	Valid
D4	0,900	0,512	Valid
D5	0,519	0,512	Valid
Q1	0,590	0,512	Valid
Q2	0,581	0,512	Valid
Q3	0,760	0,512	Valid
Q4	0,751	0,512	Valid
Q5	0,627	0,512	Valid
O1	0,620	0,512	Valid
O2	0,610	0,512	Valid
O3	0,752	0,512	Valid
O4	0,670	0,512	Valid
O5	0,810	0,512	Valid

This validity shows that the instrument used has good quality to measure each dimension (initial, managed, defined, quantitative, optimizing).

b. Reliability test

After the validity test was conducted, the next step was the reliability test. This test also used the help of SPSS software version 25. The results showed that all indicators contained in this questionnaire had a

Copyright ©2025, JSINBIS, p-ISSN: 2502-2377, e-ISSN: 2088-3587
On-line: http://ejournal.undip.ac.id/index.php/jsinbis/article/view/72634

Cronbach Alpha value of more than 0.60 so that all question items were declared reliable as shown in Table 5.

The instruments used are very reliable, so that the data obtained can be trusted to analyze aspects of academic services using the ITIL V4 framework (initial, managed, defined, quantitative, optimizing).

4.1.2 Identification of 4 Dimensions of ITIL V4

The dimensions in the ITIL V4 framework describe who are the parties involved in creating the value of a service. The process of identifying dimensions in this information security risk management assessment aims to adjust the assessment instrument, target the right respondents, and connect the results of the capability level assessment to the real context according to the case study. The identification of 4 ITIL Dimensions in academic services is shown in Table 6.

4.1.3 Mapping of Practice Success Factor (PSF)

Before assessing the capability level of each practice, it is necessary to map the Practice Success - Factor (PSF) consisting of the criteria and dimensions to be assessed. This study focuses on two practices that will be assessed, namely Information Security Management Practice and Risk Management Practice. Based on the maturity model from Axelos (2021), the focus area of this assessment is included in the category of strategic focus areas on organizational resilience, with the mapping of the assessment focus as shown in Table 7.

PSF mapping is performed on each practice, namely information security management and risk management. Mapping consists of PSF, criteria, and dimensions involved. There are 5 PSFs determined in this study, 4 PSFs for information security management practices, and 1 PSF for risk management practices.

4.1.4 determine the level of capability

The capability level of each practice is obtained from the calculation of the questionnaire scores that have been filled out by 125 respondents and 25 questions. The data used are only data from questionnaires that are declared valid and reliable. The questionnaire instrument is made based on PSF mapping, criteria and 4 dimensions. The 4 dimensions are Organization & People (OP), Information & Technology (IT), Value Streams & Processes (VP), and Partners & Suppliers (PS). Each PSF is scored and its capability level is determined. The results of the capability assessment of each practice are shown in Table 8 and Table 9.

Table 9 show the results of the PSF assessment with each score on the criteria and its level. The score is calculated based on the average value obtained by each criterion based on the results of the questionnaire. The level indicates the level of capability in each criterion.

Table 5. Reliability Test Result

Cronbach Alpha Value	Number of Statements	Reliability Limit Value	Description
0,940	25	0,6	Reliabel

Table 6. Identification of 4 Dimensions of ITIL V4

No.	Dimension	Riil context
1.	Organizations & People	• Institutional leaders (Rector, Dean, IT Director): as the director of information security policy. • IT management team: technical implementers of IT system and service security • Lecturers and Education Staff: As users and service managers • Students: Main users of IT-based academic systems or services • SPI Unit: As supervisors of compliance with procedures and policies
2.	Information & Technology	• Academic Information System, e-learning • Student and lecturer database • IT network and infrastructure • Security tools • System and data documentation
3.	Partners & Suppliers	• Cloud service providers • Hardware and network procurement partners • External auditors • National identity service providers (eg: PDDIKTI)
4.	Value Streams & Process	• Academic system service process. • System change request flow. • Data backup and recovery procedures • Security incident and disruption reporting flow. • Information security risk evaluation and audit process.

Table 7. Mapping strategic focus areas, objectives, and practices.

Strategic focus area	Objectives	*Practices assessed*
Organizational resilience	Managing risk, security and compliance	1. Information security management, 2. Risk management

Table 8. Criteria and dimension of PSF.

No	ID	PSF	Criteria	Dimension
1.	PSF01	Implementation of effective information security policies and controls	1. Documented security policy exists	OP
			2. Default controls are inadequate, needs improvement	IT
			3. User authentication is implemented	IT
			4. Role-specific access management	VP
			5. Formal security policy exists	OP

Copyright ©2025, JSINBIS, p-ISSN: 2502-2377, e-ISSN: 2088-3587
On-line: http://ejournal.undip.ac.id/index.php/jsinbis/article/view/72634

No	ID	PSF	Criteria	Dimension
			6. Policy evaluation and updating is performed	OP
			7. Multi-factor authentication is used	IT
			8. Policy is aligned with threat trends	IT
2.	PSF02	Information security awareness and culture throughout the organization	1. Users are aware and understand security risks	OP
			2. User awareness initiatives	OP
			3. Security practice guidelines available	OP
			4. Security as part of work culture	OP
			5. High level of user awareness	OP
3.	PSF03	Compliance with regulations, standards and policies	1. Considering security standards	OP
			2. Audit is conducted periodically	PS
4.	PSF04	Response and recovery to information security incidents	1. Incident handling procedures are available	VP
			2. Standard incident procedures are in place	VP
			3. Regular system security checks	IT
			4. Real-time monitoring of threats	IT
			5. Remediation mechanisms based on feedback	VP
5.	PSF05	Systematic information security risk management.	1. Risks are identified proactively and systematically	VP
			2. Start identifying potential risks	VP
			3. Connected to institutional strategy	OP
			4. Evaluations are conducted regularly	VP
			5. Aligned with international standards	PS

Table 9. level capability of information security management and risk management practice.

No	ID-Criteria	Dimension	Score	Level
1.	PSF01-1	OP	3,11	3
2.	PSF01-2	IT	3,21	3
3.	PSF01-3	IT	3,15	3
4.	PSF01-4	VP	3,35	3
5.	PSF01-5	OP	3,42	3
6.	PSF01-6	OP	3,55	4
7.	PSF01-7	IT	4,12	4
8.	PSF01-8	IT	3,65	4
9.	PSF02-1	OP	3,15	3
10.	PSF02-2	OP	3,14	3
11.	PSF02-3	OP	3,45	3
12.	PSF02-4	OP	4,21	4
13.	PSF02-5	OP	3,58	4
14.	PSF03-1	OP	3,46	3
15.	PSF03-2	PS	3,03	3
16.	PSF04-1	VP	3,16	3
17.	PSF04-2	VP	4,27	4
18.	PSF04-3	IT	3,44	3
19.	PSF04-4	IT	3,44	3
20.	PSF04-5	VP	4,32	4
21.	PSF05-1	VP	3,53	4
22.	PSF05-2	VP	3,12	3
23.	PSF05-3	OP	4,05	4
24.	PSF05-4	VP	3,49	3
25.	PSF05-5	PS	3,26	3

Table 10. Level capability assessment result of PSF

No.	ID	PSF	Score
1.	PSF01	Implementation of effective information security policies and controls	3,44
2.	PSF02	Information security awareness and culture throughout the organization	3,50
3.	PSF03	Compliance with regulations, standards and policies	3,24
4.	PSF04	Response and recovery to information security incidents.	3,72
5.	PSF05	Systematic information security risk management.	3,49
Average			3,48

After the results of the assessment of each criterion are carried out, the calculation of the level of capability or ability for information security management and risk management practices is obtained, which is shown in the Table 10.

Based on Table 10, it can be seen that the average PSF value for all criteria is 3.48. This value indicates that the practice of information security management and risk management is at level 3 (Defined).

4.1.5 Maturity Level results based on organizational implementation aspects

The assessment of the level of maturity of the practice is not only seen based on the ability of each service practice but also based on the overall aspect of the organization. The collection of data obtained from the questionnaire produces an instrument that can be mapped based on the maturity aspect. With the same instrument, the organization can be assessed based on several categories as shown in Table 11.

Each aspect is measured based on an average score, which is then categorized into maturity levels. Each level provides an overview of the extent to which the academic service process has developed and is consistently applied in the organization. In the initial

Copyright ©2025, JSINBIS, p-ISSN: 2502-2377, e-ISSN: 2088-3587
On-line: http://ejournal.undip.ac.id/index.php/jsinbis/article/view/72634

aspect, the score is 3.3 with the description starting to be implemented. The process is in the early stages of implementation, but is not yet consistent. managed aspect, with an average score of 3.2 with the description that the process has been standardized, but has not yet reached structured documentation or evaluation.

Defined, has a documented category and the description is that the process has reached the documentation stage, indicating that the practices carried out already have clear standards.

Then the quantitative aspect has a score of 4.1, which is optimal, with the statement that the process is running effectively and consistently, indicating that

Table 11. Maturity Level results based on organizational implementation aspects.

Aspect	Average score	Category	Description
Initial	3,3	Started to be implemented	The process has been implemented, but is not yet consistent
Managed	3,2	Started to be measured	Planning and performance measurement have been carried out
Defined	3,7	Documented	The process is running according to standards and continues to be improved through evaluation but is running partially
Quantitative	4,1	Optimal	The process is running effectively and consistently, there is an increase in performance
Optimizing	4,2	Sustainable	The process is running effectively and consistently

the organization has been able to optimize existing process standards. Finally, the optimizing aspect has a score of 4.2, which is sustainable, meaning that the process has reached a high level of effectiveness and consistency, indicating that the organization has been able to maintain the sustainability of the implemented practices.

4.2. Discussion

4.2.1 Maturity level of security risk manajement

The maturity level of security risk management in information technology services in higher education environments based on the ITIL V4 framework shows diversity in implementation in each dimension. In the initial dimension with an average score of 3.3, the risk management process has begun to be implemented, but is not yet consistent across academic service units. This shows that although there is initial awareness of the importance of risk management, its implementation still requires strengthening of uniform standards and procedures. Research by (Al-Ashmoery et al., 2021) and (N. K. Gunawan et al., 2020) emphasizes that inconsistent initial implementation of risk management can lead to security protection gaps in educational institutions.

In the dimension managed, with an average score of 3.2, the process is starting to be standardized but does not yet cover all aspects of information technology services. Uneven standardization is a major challenge, especially in ensuring that all academic service units have clear guidelines. In accordance with the findings of (Hidayah et al., 2019) and (Hikam et al., 2024), higher education often faces obstacles in integrating security standards due to differences in needs and technology infrastructure between units. The defined dimension, with an average score of 3.7, shows that most processes have been documented and evaluated. However, this evaluation has not been carried out comprehensively or routinely.

The quantitative dimension with a score of 4.1 reflects a high level of optimization. The process has been running effectively and consistently in many academic service units. These results support the study of (Hikam et al., 2024) which states that optimizing the risk management process in higher education not only improves security but also builds student trust in technology-based academic services. In the sustained dimension, with the highest score of 4.2, the risk management process has been running consistently and effectively. This optimizing shows that the institution has achieved operational stability that supports the security of information technology services. These results are reinforced by the findings of (Fajri & Harwahyu, 2024), which reveal that the sustainability of the risk management process is highly dependent on technological support and institutional policies.

Overall, the gap analysis shows the largest gaps in the initial and explored dimensions, which require strengthening in terms of training, counseling, and the preparation of standard operating procedures.

Figure 5 is a radar chart (spider chart) that illustrates the results of the analysis of the maturity level of security risk management in information technology services in higher education environments. The explanation of the radar chart is as follows:

a. Axis and Score

The graph shows the score values in various aspects or dimensions of the assessment, with a score range (possibility) from 1 to 5. Each point on the graph represents the score results of the various indicators or components being evaluated.

b. Consistency and Distribution of Scores

Scores ranging from 4.31 to 4.44 indicate a high level of maturity in various aspects of risk management. This shows that higher education

Copyright ©2025, JSINBIS, p-ISSN: 2502-2377, e-ISSN: 2088-3587
On-line: http://ejournal.undip.ac.id/index.php/jsinbis/article/view/72634

institutions have fairly good processes and are close to achieving optimal standards in most dimensions.

c. Minimum and Maximum Score Patterns

A notable score drop (around 3.9) on a specific indicator suggests this area—part of the initial or Managed dimension—still requires improvement, as it's often a weak point in early implementation stages.

d. Relationship with Maturity Level

Overall, high scores (4.31 and above) across most dimensions indicate that IT services in higher education have reached Quantitative or even Optimizing levels, though some lower scores highlight the need for further improvement to ensure consistency and sustainability.

e. Recommendations Based on Score Patterns

Improvement efforts should target the lowest-scoring dimensions (Initial and Managed) to ensure standardized and consistent risk management, with emphasis on training and policy development to boost performance.

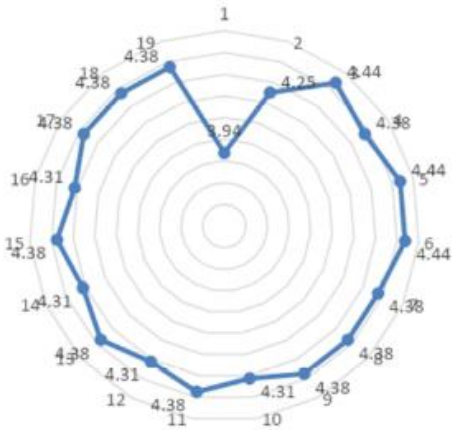


Figure 5. radar chart

4.2.2 Gap Analysis of capability levels and Uinversity targets.

After getting the average value of maturity in information security and risk management practices, it is then compared with the target expected by the University based on security standards. Based on equation 5, the Gap is obtained as shown in Table11. Table 12 shows the current condition for the capability level in information security and risk management practice showing level 3 (defined) while the target to be achieved by the University is at level 4 (Quantitative), so there is a gap of 1 level. With this gap, recommendations for improvement are needed to achieve the expected value.

Table 12. Gap analysis of capability and targets.

No.	Management practices	Capability level		
		Curent	Expectation	Gap
1.	Information security and risk management practices	3,48	4,00	0,52

4.2.3 Gap Analysis of Security Risk Management in IT Services in Higher Education Environment with ITIL V4 Framework Risk Management

Security risk management in information technology (IT) services in higher education environments, the results of this study indicate a significant gap between current conditions and desired implementation based on the ITIL v4 framework. Based on the maturity levels consisting of initial, explored, defined, improved, and sustained, it was found that academic services at Diponegoro University were at the initial or explored level, with a few reaching defined or more. This reflects the need for significant improvement in the implementation of IT security risk management to ensure better protection of student data and academic services.

- At the initial level, IT security risk management at Diponegoro University is still carried out sporadically and is not well structured. Some parts do not even have formal policies for risk management, and threat identification efforts are often carried out reactively after an incident occurs.
- At the Managed level, Diponegoro University has adopted a more proactive, risk-based approach, though mitigation efforts remain limited to basic technologies. This aligns with Sukums et al. (2023), who noted that many universities acknowledge risks but lack advanced protection solutions, creating a gap between needs and capabilities.
- At the defined level, Diponegoro University has established formal risk management policies, including systematic risk identification, control implementation, and periodic evaluation. However, as noted by Setyaningsih et al. (2023), many universities, including Diponegoro, have yet to fully implement comprehensive mitigation and monitoring procedures.
- At the quantitative level, Diponegoro University has successfully implemented more sophisticated controls and monitoring systems based on the latest technology, such as AI-based intrusion detection and automatic recovery systems.
- The optimizing level illustrates that Diponegoro University has been able to manage security risks sustainably with an integrated process in every operational aspect. However, there are several components that need to be improved. Research by Alhawari et al. (2018) shows that the sustainability of risk management depends on the support of all levels of the organization, as well as continuous evaluation and improvement. This shows that although there are institutions that are trying to achieve sustainability, their achievements are still limited.

The results of the gap value show that, although the IT security risk management maturity at Diponegoro University has reached the Defined level, existing gaps point to underlying issues such as weak

alignment between IT strategies and institutional governance, limited infrastructure, and insufficient staff understanding of ITIL V4. Additionally, the decentralized nature and academic independence typical of higher education may obstruct consistent implementation of standardized frameworks. These insights highlight the importance of stronger leadership commitment, interdepartmental collaboration, and strategic integration of ITIL practices into institutional policy and performance systems.

4.2.4 The significance of security risk management assessment in IT services.

The study found that the capability level of risk management and information security practices is at the Defined level. This highlights the importance for higher education institutions to align their IT practices with ITIL V4 standards, particularly within the domains of Risk Management and Information Security Management. Such alignment is crucial to address current challenges in managing IT risks, protecting sensitive data, and ensuring compliance with regulations like the ITE Law and the Personal Data Protection Act. The findings confirm the value of ITIL V4 in assessing and improving IT services, consistent with Pratama & Umaroh (2024), who applied ITIL V4 to design asset management at a university's financial bureau using capability assessment from COBIT 2019, and with Febrian, et al. (2024), who used ITIL V4 to evaluate maturity and design operational procedures for incident management in an academic information system.

The significant contribution of this research is because it focuses on two important practices in General Management Practices—risk management and information security management, which are crucial but have not been widely discussed in the context of higher education. So that the results of this research are not only evaluative, but also provide practical and applicable contributions in developing better IT security governance in the higher education environment.

5. Conclusion

Based on the research results referring to the ITIL V4 framework, by conducting an assessment based on the capability level and organizational aspects, it can be concluded that the maturity level of security risk management in Information Technology (IT) services in higher education environments for academic services is at level 3 (Defined). These results indicate that Diponegoro University has begun to realize the importance of IT security risk management, where practices are well defined, processes and activities are documented and standardized.

The level of identified gaps indicates that the management of IT security risk management in higher education environments is still not up to the expected standards according to ITIL V4. to increase capability levels and meet standards based on the ITIL V4 framework, as a recommendation, Diponegoro University needs to focus on strengthening formal policies related to risk management, clarifying roles and responsibilities, enhancing technological infrastructure, conducting routine audits, and fostering strong organizational support with continuous evaluations to ensure effective and sustainable IT security risk management practices.

This study focuses on evaluating the capability level of information security and risk management practices within the General Management Practice of ITIL V4. For broader insights, future research could explore related service management practices—such as change control, incident management, and problem management—and assess the overall maturity of the Service Value System (SVS).

References

Ahmad, N., & Shamsudin, Z. M., 2013. Systematic approach to successful implementation of ITIL. *Procedia Computer Science*, *17*, 237–244. https://doi.org/10.1016/j.procs.2013.05.032

Al-Ashmoery, Y., Haider, H., Haider, A., Nasser, N., & Al-Sarem, M., 2021. Impact of IT Service Management and ITIL Framework on the Businesses. *International Conference of Modern Trends in ICT Industry: Towards the Excellence in the ICT Industries, MTICTI 2021*, *January 2022*. https://doi.org/10.1109/MTICTI53925.2021.9664763

Al Faruq, B., 2020. Integration of ITIL V3, ISO 20000 & ISO 27001:2013forIT Services and Security Management System. *International Journal of Advanced Trends in Computer Science and Engineering*, *9*(3), 3514–3531. https://doi.org/10.30534/ijatcse/2020/157932020

Axelos, 2019. Foundation ITIL ® ITIL 4 Edition ITIL ® OFFICIAL PUBLISHER. In *The Stationery Office*. https://www.axelos.com

Axelos, 2021. An Overview of the ITIL ® Maturity Model. *Axelos.Com*, *September*, 31. https://www.axelos.com/for-organizations/itil-maturity-model

Aziza, N., 2023. Metodologi penelitian 1 : deskriptif kuantitatif. *ResearchGate*, *July*, 166–178.

Fajri, K. S. Al, & Harwahyu, R., 2024. Information Security Management System Assessment Model by Integrating ISO 27002 and 27004. *MALCOM: Indonesian Journal of Machine Learning and Computer Science*, *4*(2), 498–506. https://doi.org/10.57152/malcom.v4i2.1245

Febrian, Dany Salisah, Febi Nur Megawati, M., M. Afdal, & Marsal, A., 2024. Evaluation Of Maturity Level And Design Of Incident Management Sop In Academic Information System Using Itil V4.

Jurnal Teknik Informatika, *5*(4), 337–344.

Gunawan, H., Irianto, A. B. P., & Negara, J. G. P., 2024. Implementation of Sustainable Service Improvement in Organizations Using Framework Information Technology Infrastructure Library (Itil). *Procedia Computer Science*, *234*, 748–755. https://doi.org/10.1016/j.procs.2024.03.061

Gunawan, N. K., Hadiprakoso, R. B., & Kabetta, H. 2020. Comparative study between the integration of ITIL and ISO / IEC 27001 with the integration of COBIT and ISO / IEC 27001. *IOP Conference Series: Materials Science and Engineering*, *852*(1), 0–5. https://doi.org/10.1088/1757-899X/852/1/012128

Herlinudinkhaji, D., & Kurnia Ramadhani, L., 2023. Tata Kelola Layanan Teknologi Informasi dengan ITIL V4 untuk Estimasi Layanan. *Remik*, *7*(1), 452–457. https://doi.org/10.33395/remik.v7i1.12058

Hidayah, L. N., Puspitaningrum, A., Febianti, T., Oktavfiantika, N. N., Nurdin, A. L., Ayuningtyas, B. S., & Fathushahib, F., 2019. Audit Infrastruktur Teknologi Informasi Berbasis Itil V.3 Domain Service Design I Pada Sipmas Di Lppm It Telkom Purwokerto. *Indonesian Journal of Business Intelligence (IJUBI)*, *1*(1), 39. https://doi.org/10.21927/ijubi.v1i1.896

Hikam, M. L. B., Dewi, F., & Praditya, D., 2024. Analisis Manajemen Risiko Informasi Menggunakan Iso/Iec 27005:2018 (Studi Kasus: Pt.Xyz). *JIPI (Jurnal Ilmiah Penelitian Dan Pembelajaran Informatika)*, *9*(2), 728–734. https://doi.org/10.29100/jipi.v9i2.4709

Ilyasa, M. K., & Bisma, R., 2022. Analisis Manajemen Insiden dan Masalah Layanan IT pada Balitbang Jatim. *Journal of Emerging Information Systems and Business Intelligence (JEISBI)*, *03*(1), 50–58.

Lopes, S. F. S. F., 2021. The importance of the ITIL framework in managing Information and Communication Technology services. *International Journal of Advanced Engineering Research and Science*, *8*(5), 292–296. https://doi.org/10.22161/ijaers.85.35

Pratama, R. Y., & Umaroh, S., 2024. An IT Asset Governance Model Design Using COBIT 2019 And ITIL V4 Framework at BKU Itenas. *E3S Web of Conferences*, *484*. https://doi.org/10.1051/e3sconf/202448402006

Putri, I. R. D., & Nuryana, I. K. D., 2024. Analisis Manajemen Insiden dan Masalah Pada Helpdesk Terhadap Perbaikan Kualitas Pelayanan Publik Berdasarkan Framework ITIL V4 (Studi Kasus : Dispendukcapil Kota Kediri). *Journal of Emerging Information Systems and Business Intelligence)*, *05*(01), 173–181.

Rais,F., Ramadhani, M.N., Ubaidillah, M., Christian, J., Farisi, A., Informasi, S., Ilmu, F., & Multi, U. 2024. *Analisis Metode Audit Infrastrukt It Pada Bidang Pendidikan, Pemerintahan, Dan Perusahaan: Sebuah Tinjauan Literatur Sistematis*. *1*(3), 18–27.

Selig, G. J., 2008. Implementing IT Governance A Practical Guide to Global Best Practices in IT Management. *Van Haren Publishing*, *December*, 1–23.

Selvi Sabrina, Ilhamsyah, N. M., 2019. Tata Kelola Layanan Sistem Informasi Menggunakan Framework Itil Versi 3 Domain Itscm. *Coding Jurnal Komputer Dan Aplikasi*, *7*(01). https://doi.org/10.26418/coding.v7i01.30836

Setyaningsih, A. F., Prabowo, W. A., & Saintika, Y., 2023. Evaluasi Manajemen Layanan Teknologi Informasi menggunakan Itil V4. *Jurnal Teknologi Informatika Dan Komputer*, *9*(1), 160–173. https://doi.org/10.37012/jtik.v9i1.1375

Sukums, F., Wamala-Larsson, C. W., & Kisenge, R., 2023. Assessment of ICT services using the Information Technology Infrastructure Library Framework at Muhimbili University of Health and Allied Sciences, Tanzania. *East African Journal of Science, Technology and Innovation*, *4*(3), 1–14. https://doi.org/10.37425/eajsti.v4i3.643

Yurisca Bernanda, D., & Pangrestu, C., 2021. Evaluation of Server Storage Rack Using ITIL Framework (Case Study: Network Access Provider). Cogito Smart Journal |, 7(2), 2021.