# alilingan_2018_IOP_Conf._Ser._3A_Mater._Sci._Eng._306_0121 10.pdf

*by*

---

# Incident Management in Academic Information System using ITIL Framework

View the article online for updates and enhancements.

# Incident Management in Academic Information System using ITIL Framework

**V R Palilingan[1] and J R Batmetan[2*]**

[1]Universitas Negeri Manado, Tondano 95618, Sulawesi Utara, Indonesia
[2]Universitas Sari Putra Indonesia, Tomohon, 95416, Sulawesi Utara, Indonesia

*john.reimon@gmail.com

**Abstract**. Incident management is very important in order to ensure the continuity of a system. Information systems require incident management to ensure information systems can provide maximum service according to the service provided. Many of the problems that arise in academic information systems come from incidents that are not properly handled. The objective of this study aims to find the appropriate way of incident management. The incident can be managed so it will not be a big problem. This research uses the ITIL framework to solve incident problems. The technique used in this study is a technique adopted and developed from the service operations section of the ITIL framework. The results of this research found that 84.5% of incidents appearing in academic information systems can be handled quickly and appropriately. 15.5% incidents can be escalated so as to not cause any new problems. The model of incident management applied to make academic information system can run quickly in providing academic service in a good and efficient. The incident management model implemented in this research is able to manage resources appropriately so as to quickly and easily manage incidents.

## 1. Introduction

The academic system is an important part of the university. Academic systems in various universities have been managed with information-based systems to make it easier, faster and more effective in winning large academic data. The academic information system has become a backbone in 60% of large and advanced universities in Indonesia. More than 80% of the services provided by the University can be served using an academic information system. These services include Study Plan Card (KRS), Study Result Card (KHS), lecture schedule, teaching materials, assignments and other academic services. Academic information systems have been used to improve productivity [1] academic services at universities [2]. In conducting good academic services, universities need to provide adequate technology infrastructure and meet the needs of users [3] who use the service. The hope is to have a good and continuous service guarantee [4] with good quality.

Academic services require quality and accurate service management including service to incidents that arise. The incident process needs to be set so that no service interruption is provided [5]. Many of the incident issues that arose have not been adequately addressed, 70% of incidents are still handled without clear procedures and still rely on individuals who work only on the basis of previous experience. This is precisely 60% of them have not been able to resolve the incident and leave only the problems that make the academic system becomes disrupted and not running properly. The absence of operational standards of incident management and incident management procedures makes 80% of incidents only handled manually and very slow to complete while 20% of incidents are left

unresolved. This then creates a new problem in the academic system so that the system becomes disturbed.

To solve the problem, some researchers have suggested the following strategy: information system incident should look at aspects of the management by ITIL framework or some framework to solvem the problem [6]. The suggested strategy is effective and can be implemented and easy to adopt by framework of e-governanca [7, 8]. However, some problems still persist. Incident management in information system cannot explain in detail about how to use the application so that some incident have difficulty to solved [9, 10]. Furthermore, incident management becomes complicated and sophisticated [11], thus creating conflicts with limited use to adoption by ITIL framework.

Here, the purpose of this study was to find the right way of incident management in academic information system. These novelty makes the academic information system incident  for developing countries that have many limitations using framework to solved the problem. The incident management in academic information system, including indentification, Incident logging, Incident categorization, Incident Priorization, Initial diagnosis, incident escalation, Investigation and diagnosis, resolution and recovery, Incident closure, Incident management report, and Incident Management evaluation. Every Incident faced should be handled so it does not matter much. The method of treatment to be used in this study is to implement incident management in accordance with the Information Technology infrastructure library (ITIL) framework.

## 2. Methods

There are many model frameworks [6] IT governance [7, 8] one of which is Information Technology Infrastructure Information Service (ITIL) [8]. The ITIL framework contains the best IT governance framework in use today [9]. This framework has stages that are systematically [8] explained in its entirety. Stages are as follows Service Strategy: the stage of strategic transformation of IT management services into a strategic strategy of the organization. Service Design: this stage contains the direction and direction of the IT service management guide in accordance with the strategy that has been made before. This stage is a continuation of the previous service strategy. This stage is also built into the satisfaction of customer satisfaction. Transition Services [10]: This stage contains the transition process from the old governance model to the new governance model created in the Service Design stage. Service Operations [10]: This stage contains best practice steps in IT service management. Continual Service Improvement [11]: This section contains the management of feedbacks obtained from customers [12]. The inputs obtained in the analysis can then be implemented in a pre-made stage so that the system becomes better and the results are improved [13]. Thus the system can improve the results of the Strategy, Service, Transition Services, and Service Operations (see Figure 1).
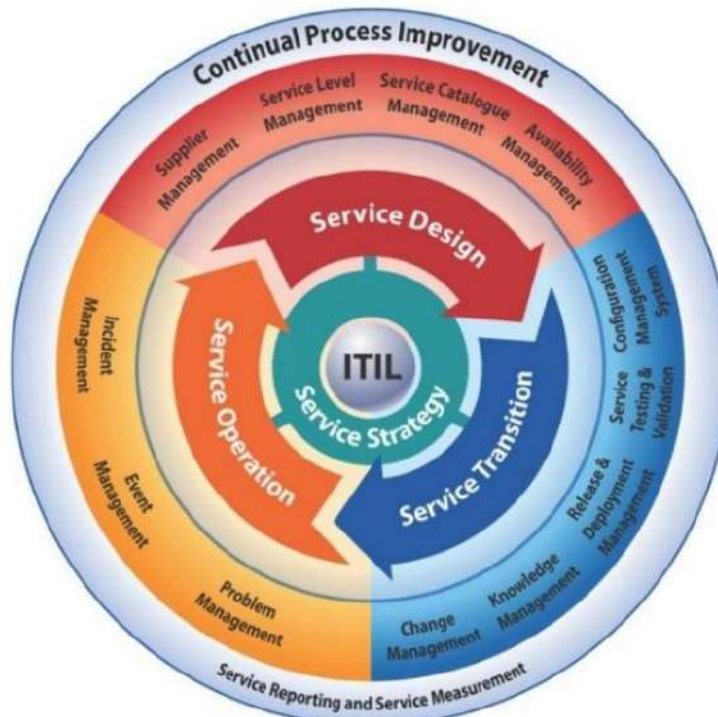
**Figure 1.** ITIL framework.

Incidents can be defined as an interruption or quality reduction of IT services [9]. Even the slightest incident has not caused significant problems in the system such as a system configuration error can be called an incident. Problem solving an incident may be called incident management. Incident processes can be detected more quickly through automatic detection of an event management tool, and can also be through technician reports, and service desks [14]. The ITIL v3 framework has incident management and is placed on the Service Operation cycle [15]. After an incident occurs, the system should be able to restore the IT service conditions to normal as soon as possible without leaving new problems that have a greater impact on the system. Thus an incident management is required that minimizes the negative impacts of the organization's main business activities. The normal state of IT services can be called a predefined state in an SLA (Service Level Agreement).

According to the ITIL v3 framework, the activities in incident management are 1). Incident identification the incident management process begins with identification. 2). Incident logging this step is required for each type of incident, both large and small. 3). Incident categorization in making incident categories requires a special process between the IT manager and the organization management [16, 17]. It aims to generate incident categories and priority handling in line with the organization's business processes. 4). Incident priority the incident priority step is based on a pre-made categorization. 5). Initial diagnosis The initial diagnosis of an incident must be carried out by any person initially connected with the incident, whether it is a service desk, a technical staff, or an automated device such as event management. 6). Incident escalation Incident escalation is an act of raising the level of incident handling. 7). Investigation (investigation and diagnosis) Investigation measures are conducted to find the source of the problem from the incident. 8). Resolution (resolution and recovery) this step is an action taken to resolve an incident. 9). Closing (incident closure) the closing step is the steps undertaken by the service desk and associated technician staff to ascertain whether the incident has been properly addressed (see Figure 2).
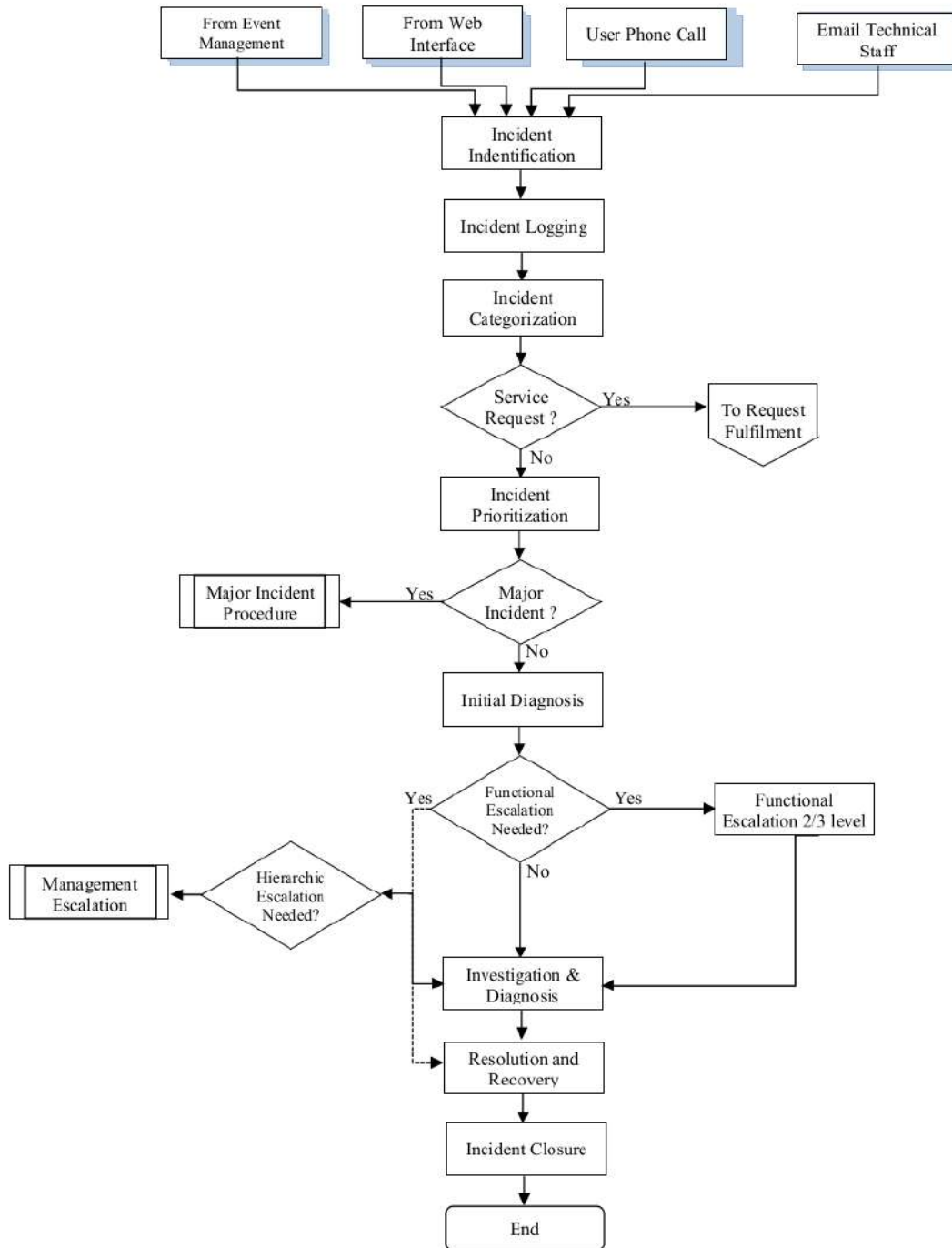
**Figure 2.** Incident management with ITIL.

This study uses the incident management method of service operation on ITIL v3 framework. The steps taken are as follows: 1). Preliminary; In this stage, the definition of background, problem formulation, problem definition, research objectives and benefits and the methodology used to solve the problem, namely the making of document management of incident management process. 2). Information Collection and Analysis; at this stage, the review activity of the University Information Technology governance document is carried out. Selin also conducted a study of ITIL framework literature. 3). Preparation of Governance Documents; in this step, the preparation of governance documents is based on the results of the analysis in the previous step. The documented procedures will consist of details of incident management activities, and incident category, incident priority, metric and CSF (Critical Success Factor), SLA (Service Level Agreement) and RACI charts. In addition to the attachments above, will also be created a flow chart that describes each activity undertaken. 4). Document Verification; in this stage will be verified each part of the document management to determine whether each activity in the document is in accordance with its purpose and can be implemented. 5). Document Validation; in this phase, validation of the governance document will be conducted to determine whether the main objective of the incident management process has been fulfilled with this document. 6). Conclusion; in this stage will be the formulation of conclusions of the overall steps taken and the results obtained.

## 3. Results and Discussion

The results of IT governance document analysis show that not all programs in the IT Strategic Plan document have supporting document management. For programs that already have document management, it is known that the document has not been standardized and the development is done solely by each sub-section. This resulted in the implementation of the program is often not maximal and its performance can not be measured. Table 1 below summarizes the help desk management program documents and IT support performed by the IT Support sub-section.

Completion of incidents occurring, the settlement using best practices on the ITIL framework according to table 1 shown below.

**Table 1**. Document details incident management.

| No | Activity | Product |
|---|---|---|
| 1 | Organize service centers and technical assistance for all IT users | IT services and technical assistance |
| 2 | Coordinate the implementation of IT operational services and technical assistance with IT Helpdesk solver | Implementation of services and technical assistance |
| 3 | Evaluate the operational issues of system, application, network and communication system received | Operational evaluation reports on systems, applications, networks and communications systems |
| 4 | Deliver IT service information to those who need it for the issues that have been submitted to the IT Helpdesk | Information IT services |
| 5 | Compile and manage database handling/solutions to IT operations problems | Database of troubleshooting |
| 6 | Provide, administer access rights and authority associated with the domain (intra / xnet), internet, email and desktop (administrator) | Implementing IT System Administrators associated with domains, email and desktops |
| 7 | Manage group archives and documents | Management of archives and documents |

After the analysis to refine the document management by rebuilding the details of each activity in the program. These details define each activity objective of the program, the performance indicators for the purpose, the forms, and documents required to carry out the activity, the details of the activity execution steps, the RACI diagram of activity and the activity flow diagram. Details of the management document display the following activity details (see Table 2).

**Table 2.** Activity details incident management.

| Activity | Objective | Performance Indicator |
|---|---|---|
| 1.Incident identification | 1.1 Ensure that each incident can be identified before it has negative implications for the ongoing business process. | Incidents that have negative implications before they can be reported. |
| | 1.2.Ensure incident cards with "Not completed" status are opened and distributed | Incident cards reopened each day. |
| 2.Incident logging | 2.1 Ensure that recording of information from incident reports is entered as a basis for the implementation of the incident handling process. | a) The time required to record incident information. b) Complain from U because HO is not in place at time of reporting c) reports entered by phone d) incoming reports via email e) reports that come in the helpdesk table |
| | 2.2 Ensure the information is fully recorded and the source verified. | a) the incident card is fully recorded b) incident cards with verified sources |
| | 2.3 Ensure a summary of incidents and incident card search keywords is made | a) an incident card that has the right keywords |
| 3.Incident categorization | 3.1 Ensure the categorization of incident reports is appropriate and done in a short period of time. | a) Incident reports falling into the correct category. b) the time required to categorize incident reports |
| 4. Incident priorization | 4.1Ensuring incoming incident reports is given priority of appropriate handling and is done in a short period of time. | a) Incident reports given the appropriate priority. b) The time required to prioritize incident reports. |
| | 4.2 Ensure the delegation of incident handling has the right staff to handle it. | a) Events where staff at HO level are not available. b) escalation of HO to HS due to staff's inability |
| 5. Initial diagnosis | 5.1 Ensure early diagnostic action is performed at HO level in a short time. | a) Time required in the initial diagnostic action. b) HO error in initial diagnosis. |
| | 5.2 Ensure that leaders / officials receive priority on-site handling. | a) Availability of HO staff for on-site handling. |
| | 5.3 Ensuring early diagnostic measures may provide input for incident handling Overall and if possible it could provide a solution to the incident | a) Incident reports found the solution in the initial diagnosis. |
| 6. incident escalation | 6.1 Ensure the escalation process is done in a short time to meet the target SLA Time of incident handling. | a) The time required to establish an incident escalation. b) Incidental reports that are late in escalation. |
| | 6.2 Ensure that escalation is carried out with due consideration to the action taken. | a) Escalation through consideration of IM. |
| | 6.3 Ensure the selection of persons responsible for post-incident handling escalation | a) Availability of staff to handle combined incidents. |
| 7.Investigation and diagnosis | 7.1 Ensure thorough and in-depth investigations to find the source of incident problems. | a) The time required for the investigation of incident reports. b) A complete incident description prior to the investigation. c) Investigative action carried out to meet U again to complete the description of the incident. |
| | 7.2 Ensure that investigative and diagnostic activities are carried out according to standards and meet targeted SLAs of handling time. | a) The time it takes to conduct investigative and diagnostic activities. |

Table 2. Cont.

| | | |
|---|---|---|
| | 7.3 Ensuring that solutions are found is appropriate for the intended incident. | a) A solution found after investigation and diagnostic activities by HS. b) Solutions found after investigation and diagnostic activities by SM. c) Solutions found after investigation and diagnostic activities by NM. d) Solutions found after investigation and diagnostic activities by MM. e) handling is given to suppliers |
| 8. resolution and recovery | 8.1 Ensure solutions to incidents are tested and can be implemented | a) The solution being implemented is the true solution to the incident. b) Solutions that can not be implemented. |
| 9. Incident closure | 9.1 Ensure closure activity is carried out. | a) Incident card with "Not completed" status but actually already found and already implemented the solution. b) Appropriate incident handling of target SLA handling time. |
| | 9.2 Ensure complaints of U are accepted. | a) A complaint from the Incident Reporter (U) on the given solution. |
| 10. Incident management report | 10.1 Ensure daily recapitulation is performed. 10.2 Ensure monthly recapitulation is performed. | a) completeness of recapitulation |
| | 10.3 Ensure that an incident response report is prepared as an evaluation of future action measures. | a) Completeness of the report. b) timeliness of report submission |
| 11. Incident Management evaluation | 11.1 Ensure that evaluations are undertaken on a monthly basis to improve the quality of incident handling. | a) Evaluation meetings conducted during the working year. b) Surveys conducted during the working year. |
| | 11.2 Ensure evaluation results are followed by each party at the level of incident handling. | a) Evaluation results are not followed up. |

This result shows the entire incident management process, displays the incident management process of helpdesk and IT support along with the input to implement it, and the resulting output is:

- Input
  1. Incident report from IT employee / user leader, 2. Interview reports from inspection staff (reporting via telephone, email or directly to the helpdesk desk)
- Process
  1. Incident identification, 2. Incident logging, 3. Incident categorization, 4. Incident priority, 5. Initial diagnosis, 6. Incident escalation, 7. Investigation and diagnosis, 8. Resolution and recovery, 9. Incident closure, 10. Incident management report, 11. Incident management evaluation
- Output
  1. Solution, 2. Problem Management, 3. Configuration Management, 4. SLA Management, 5. Capacity Management, 6. Availability Management, 7. Monthly reports of incident handling, 8.9. Performance evaluation report.

This study aimed to answer the research question: what types of requirements should be taken account in building an incident management system in academic information system. Basic functional requirements of the incident management system are: Submit request, Check the request status, create request, Assign request, Update request, Relate request, Configure settings, Create reports, Maintain knowledge base, Maintain workflow, and Maintain registers. Besides incidents, the system should handle service requests, problems and requests for change. Regarding data requirements, 23 incident attributes were identified. The main contribution of this study lies in showing how IT service management (ITIL) concepts affect the tool specification and requirements.

Both case study and action research methods were used in this study. The case organization was an IS academic department of a university. However, there are some limitations to this study. A case study as a research method has been criticized for a number of reasons. It has been claimed that a case

study lacks the academic rigor (the control of research), research results based on case studies cannot be generalized, and that a case study requires a lot of resources and experienced case study researchers. To add the amount of control to the study, we used a project diary where notes of each meeting were stored. Regarding the generalization of results, it is true that we cannot draw statistical conclusions from case study results. Data for this study was collected from one case organization. However, we obtained a good overview of the case organization by using multiple data collection methods, such as discussions with persons who had different perspectives to customer support and maintenance work: an IS manager, process managers, designers responsible for the incident management tool development, and service desk workers. Incident management in academic information system.within IT service management is a new and interesting research field that requires more academic research. Further research (with more case organiza- tions) is needed to investigate the design, deployment and the introduction of incident management systems in academic information system.

## 4. Conclusions

The conclusions made based on the research that has been done are as follows: The governance document developed for some of the objectives of the help desk management program and IT support, i.e. the incident management process. This governance document contains 11 (eleven) activities consisting of 9 (nine) activities based on the ITIL framework and 2 (two) additional activities as required by the organization i.e. reporting and evaluation. Implementing the program is divided into 7 (seven) parties namely Incident Reporter (U), Helpdesk Operator (HO), Helpdesk Specialist (HS), Incident Manager (IM), Software Manager (SM), Network Manager (NM) And Maintenance Manager (MM). The RACI diagram shows the duties and responsibilities of each of the above-mentioned parties in each step of the activity. Activities developed from the ITIL framework, the implementation is continuous and continuous. While the reporting and evaluation activities are carried out at the beginning and end of the month only. The governance matrix is built to be the conclusion of the entire program process. The matrix contains each activity in the following programs, objectives, performance indicators, forms and documents required for the execution of activities, and the RACI diagram.

## References

[1]  B Phillips 2013 Information Technology Management Practice: Impacts upon Effectiveness *J. Organ. End User Comput.* **25**(4) pp 50–74.

[2]  R Ajami and I Technology 2013 IT Governance in Higher Education Institutions in UAE *Int. J. It/bus. Alignment Gov.* **4**(2) pp 1–18.

[3]  R. Pereira 2012 Designing a New Integrated IT Governance and IT Management Framework Based on Both Scientific and Practitioner Viewpoint *Int. J. Enterp. Inf. Syst.* **8**(4) pp 1–43.

[4]  S H Parisa Aasi, and Lazar Rusu 2014 Culture Influence on IT Governance *Int. J. It/bus. Alignment Gov.* **5**(1) pp 34–49.

[5]  A Nabiollahi, R A Alias, and S Sahibuddin 2010 A Service Based Framework for Integration of ITIL V3 and Enterprise Architecture *IEEE* pp 1–5.

[6]  N Mohamed 2012 A conceptual framework for information technology governance effectiveness in private organizations *Int. Manag. Comput. Secur.* **20**(2) pp 88–106.

[7]  M Vicente and N Gama 2014 A Business Motivation Model for IT Service Management *Int. J. Inf. Syst. Model. Des.* **5**(1) pp 83–107.

[8]  M Mora and R V O Connor 2014 An Extensive Review of IT Service Design in Seven

International ITSM Processes Frameworks *Int. J. Inf. Technol. Syst. Approach* **7**(2) pp 83–107.

[9]   B C Potgieter 2002 *Evidence that use of the ITIL framework is effective* pp 160–167.

[10] S Sahibudin and M Ayat 2008 Combining ITIL , COBIT and ISO / IEC 27002 in Order to Design a Comprehensive IT Framework in Organizations Mohammad Sharifi Centre for Advanced Software Engineering ( CASE ), University Teknologi Malaysia *Second Asia International Conference on Modelling & Simulation* pp 749–753.

[11] J Järveläinen 2013 International Journal of Information Management IT incidents and business impacts : Validating a framework for continuity management in information systems *Int. J. Inf. Manage.* **33**(3) pp 583–590.

[12] M Marrone, F Gacenga, and A Cater-steel 2014 IT Service Management : A Cross-national Study of ITIL Adoption IT Service Management : A Cross-national Study of ITIL Adoption *Commun. Assoc. Inf. Syst.* **34** pp 865–892.

[13] A Cater-steel and M Toleman 2007 *The Role of Universities in IT Service Management Education* pp 369–382.

[14] M Jäntti 2009 Defining Requirements for an Incident Management System : A Case Study *Fourth International Conference on Systems* pp 184–189.

[15] A A Norita Ahmad, Noha Tarek Amer, and Faten Qutaifan 2013 Technology adoption model and a road map to successful implementation of ITIL *J. Enterp. Inf. Manag.* **26**(5) pp 553–576.

[16] I A Tøndel, M B Line, and M G Jaatun 2014 Information security incident management: Current practice as reported in the literature *Comput. Secur.* pp 1–27.

[17] M Marrone and L M Kolbe 2011 Uncovering ITIL claims : IT executives ' perception on benefits and Business-IT alignment *Inf Syst E-Bus Manag.* **9** pp 363–380.

ORIGINALITY REPORT

# 13%
SIMILARITY INDEX

# 9%
INTERNET SOURCES

# 14%
PUBLICATIONS

# 0%
STUDENT PAPERS

PRIMARY SOURCES

**1** www.uku.fi
Internet Source
**8%**

**2** J R Batmetan, V R Palilingan. "Higher Education Students' Behaviour to Adopt Mobile Learning", IOP Conference Series: Materials Science and Engineering, 2018
Publication
**6%**

Exclude quotes          On                    Exclude matches          < 5%

Exclude bibliography     On