Baltic J. Modern Computing, Vol. 12 (2024), No.3, 286-303
https://doi.org/10.22364/bjmc.2024.12.3.05

An Approach of ICT Incident Management Based on ITIL 4 Methodology Recommendations

Dalė DZEMYDIENĖ[1], Sigita TURSKIENĖ[1],
Irma ŠILEIKIENĖ[1,2]

[1]Institute of Regional Development Šiauliai Academy Vilnius University, Vilniaus str. 88, LT-76285 Šiauliai, Lithuania
[2]Department of Information Technologies Faculty of Fundamental Sciences Vilnius Gediminas Technical University -Vilnius Tech, Saulėtekio ave. 11, Vilnius, Lithuania

dale.dzemydiene@mif.vu.lt, sigita.turskiene@sa.vu.lt,
irma.sileikiene@vilniustech.lt

ORCID 0000-0003-1646-2720, ORCID 0000-0002-2019-6712,
ORCID 0000-0002-1185-0970

Abstract. The main goal of this research is to develop an approach for management of incidents of IT infrastructure library following the recommendations of the ITIL 4 methodology. This approach is provided for solving of ICT incidents more efficiently in an educational institution, focusing on the value creation of ICT services and their maintenance. When ICT infrastructure disruptions occur, ways and appropriate measures must be found to deal with incident management issues. The methods of recognition of the ICT incidents are included in decision support subsystem by applying classification and prioritization methods. The issues of choosing the right software in order to more effectively automate the management are proposed by analysing the process of solving emerging ICT infrastructure incidents. Functional capabilities of Spiceworks Help Desk software are explored to help in registration and management of the incident resolution cases caused by ICT disruptions. The article examines ITIL incident management practices and methods of solving ICT incidents in an educational institution, which become one of the most important in ensuring the smooth and uninterrupted work of interoperable systems of education institution.

Keywords: information technology infrastructure library **(**ITIL); information communication technologies (ICT); ICT incident management.

1. Introduction

The violations of information technology infrastructure library (ITIL) components are increasing nowadays and different types of ICT incidents can disrupt various links of infrastructure of ICT and the activity processes of services and their uninterrupted work in the institution. As the number of incidents in cyberspace increases, the problem of ensuring the smooth operations of ICT infrastructure arises in business enterprises, public sector and in educational institutions, where a consistent working process is carried out. This requires the continuous operation of the functions of interoperable systems, provided by ICT infrastructure services (Axelos Limited, 2019; 2020; ITIL4 Practice guide, 2023). In an educational institution, it is important to ensure uninterrupted work of ICT chains and to effectively manage ICT services, especially focusing on incident management practices and technologies.

ITIL incidents refer to various ICT infrastructure disruptions and ICT service interruptions, such as, for example, disruption of the main server of the institution, power outages, computer network violations, violations of individual software modules, etc. and service performance degradation (Axelos Limited, 2021). Most often, incident management is integrated into the entire ICT service management process (Gillingham, 2023; Darby, 2022; Dzemydienė et al., 2022; Kaplan, 2023). The purpose of ITIL incident management is to ensure the timely restoration of services to normal working conditions by restoring damaged ICT provision services, minimizing the impact of the breach resulting from various disrupted chains (Dzemydienė et al., 2023).

The article presents ICT incident management recommendations based on the ITIL v4 methodology. The goal is to create an incident management and resolution algorithm that would enable effective incident management according to the set priorities. A method of incident prioritization is proposed, which is integrated into decision-making in the course of eliminating service disruptions. The research includes the analysis of computerized incident management systems and the application of these tools in solving cases of ICT disruption in an educational institution and managing their resolution process.

Spiceworks Help Desk software was chosen for solving ICT incidents and performing the main management steps, which is free, has an easy-to-use interface, has automated incident registration and management, network monitoring, report generation and the ability to integrate with other ICT management systems, integrated remote access to user device function.

Innovative ICT, such as service-oriented architecture, cloud technologies, application of templated scenarios, creation of open data access, provides opportunities for more intensive development of data exchange and reuse of data and increases the efficiency of services. The legal acts of the Republic of Lithuania and the directives of the European Union (EU) oblige to move to more effective forms of digitization and integrative possibilities of information systems (IS) (Lithuania's Progress Strategy "Lithuania 2030", 2012).

The legal and technical base in the public sector is sufficiently prepared, harmonized and meets EU requirements and standards for the use of official systems (Lithuania's Progress Strategy "Lithuania 2030", 2012). However, educational institutions are still hesitant to move to the innovations and opportunities of innovative tools. There is a sense of digital differentiation in the use of administrative tools. There is a lack of an integrated, coordinated approaches, which can enable the adaptable application of information resources, their implementation in the infrastructure of educational institutions at all levels.

The specificity of the management of educational institutions means that employees of all levels share the coordination of management, working groups and activity planning. Participating at each level, the main customers - teachers, middle managers, managers - are interested persons who strive for the implementation of common goals, and their work principles are transferred to the operational processes of information systems (IS) that enable the development of automated systems. The benefits of ICT management in education have implications for better collaboration between the school as an administrative unit, parents and external institutions and local authorities. The management of ICT services influences the productivity and efficiency of the work of an organization, company or institution, the dependence on paper documents decreases, an organized information and service transmission system is created, which considers the needs of the institution (DESI, 2022). Institutions that do not implement ICT service management innovations have risk for losing of the ability to effectively manage complex processes.

The aim of this research is forwarded for development of approach of implementation of ITIL 4 methods for analysis and maintaining of the infrastructure of ICT of educational institution. The objectives of this research are concerning the development of constructional structure of description of activities of educational institution for developing of ICT library following to requirements of the ITIL 4 methodology. The set of recommendations are provided for analysis of ICT infrastructure management services by showing more possibilities of modern ITIL 4 methodology application tools. The objectives are realized by showing the possibilities through the solving some problems of ICT service management according to detecting of ICT incidents and realizing them. The results are related to the development of ICT functional capabilities for the modernization of the work of secondary education institution, by demonstrating the advantages of ICT management services. The results of experimental research enable to provide recommendations for selection of ICT infrastructure management tools and demonstrate their functional advantages. The experimental results with additional forms of integrated information systems (IS) helps to form a new understanding of value acquired through ICT infrastructure development and services efficiency. The article describes how the development possibilities of ICT management services are accesses, and how it is possible to implement by the certain methodology and tools, which become significant in the works of educational institution. The implementation strategy of methodology of ITIL 4 is recommended for the application for ICT infrastructure management services by realizing optimization of administrative processes in the educational institution.

The content of this article is separated in chapters. In 2 Chapter is presented the review of practices of IT incident management and describes main principles. The 3 Chapter presents the main stages of our proposed method for categorization of incidents during diagnostic stage and algorithm which is implemented into the management of ICT incidents. The 4 Chapter is devoted for representation of experimental research results of proposed methodology for management of ICT incidents in the infrastructure of concrete educational institution. In Conclusions we are summarized our obtained results and present the recommendations of ICT management for educational institutions.

2. Review of practices of management of ICT incidents and ITIL 4 methodology recommendations

The continue and not interrupted ICT work implies effectiveness of economy and work of business enterprises (Dzemydaitė and Naruševičius, 2023; Dzemydienė et al., 2022).

But we deal with the problem of ICT interruptions. In the past, detection of ICT incidents was mainly based on information from end users and ICT professionals.

Various ICT incident resolution methodologies are offered in scientific and practical activities (Palilingan and Batmetan, 2018; Danby, 2022; Thirhappa, 2023). However, it is the ITIL methodology and its latest version - ITIL 4 implies into the value of ICT and covers the most important aspects of ICT incident management (Axelos Limited, 2020; ITIL 4 Practice Guide, 2023). ICT incident management methodologies and specialist practices attempt to ensure that periods of unplanned service unavailability or degradation are kept to a minimum (Shepherd, 2019, Howells, 2020). This is made possible by two main factors: early detection of incidents and rapid restoration of their normal operation. ITIL v4 refers to incident management as a service management practice that describes the key activities, inputs, outputs and roles of those involved in the resolution process (Thirthappa, 2023; Key ITIL Concepts, 2023). Based on these guidelines, institutions are advised to create an incident management process that meets their specific requirements and operational specifics (ITIL 4 Practice Guide, 2023). Many incident management practices are divided into certain phases, with the key steps of incident management and periodic incident review important, and where each step is followed by an abstract sequence of actions (ITIL 4 Management Practices, 2023).

Modern good management practices suggest detecting and logging incidents as soon as they occur, before they affect users. Implementation of this method for ICT incidents management (Axelos Limited, 2021) has many advantages, according to:

- shortened duration of service unavailability or deterioration;
- higher quality raw data supports the correct response and resolution to incident resolution, including automatic inclusion of a resolution method, based on the resolution of previous analogous cases;
- some incidents remain invisible to users, thus improving user and customer satisfaction;
- some incidents can be resolved before they affect the agreed service quality of customers, improving perceived service and officially reported service quality;
- incident-related costs can be reduced.

The incident detection process is enabled by monitoring of conditions of ICT work, event management practices and implementing of right software for managing of incidents. Our proposed approach is based on the inclusion of event categorization method for diagnosis and management process that differentiate incidents from informational events and alerts.

Effective incident resolution can become a permanent way of dealing with significant issues in their aftermath. If the incident is not resolved in a timely manner, the issue remains in an error state and should be addressed through documentation when related incidents occur. Each documented solution should include a clear definition of the symptoms to which it applies. In some cases, the solution to the ICT incident can be automated. For other incidents, you need to find a way to fix the error. This is part of error control. Error control activities manage known errors, which are issues for which initial analysis has been completed; this usually means that faulty components have been identified. Error control also includes the identification of potential permanent decisions that may be subject to a change request, but only if this can be justified by the costs, risks and benefits.

Table 1. List of components of ITIL implemented in X Educational institution

The ICT infrastructure of X Educational institution						
		Hardware and Computer networks			**Systematic standardized software**	**Applicational software**
No	**Activities/ functions**	**Types of Networks (WAN, LAN, WIFI, INT)**	**Computer Work Stations**	**Other Technology**	**Operation systems. Cyber Security systems**	**Application Software Systems and Web Tools**
1.	Management of information and communication	WAN, LAN, INT (until 1 Gb/s, WIFI (~ 1 Mb/s, - ~200 Mb/s). INT - fiber optic connection through LITNET	1. Ethernet 144 and more stationary working educational and teaching stations. 2. Wi-Fi – ~600 laptops and smart devices.	Software of Internet control: 1. Ethernet routers and switches, ~ 4 controlled and ~ 6 not controlled; 2. Wi-Fi access through MIKROTIK RB760iGS routers and switches UNIFI US24P250, 26 Wi-Fi points UNIFI U7LR.	Operation systems: 1. Stationary work station OS – MS Windows 10/11. 2. Smart devices with OS Android.; 3. Smart devices with iOS. Security systems: 1. In stationary work and educational stations – standard MS Windows OS safety toolkits 2. LITNET supported Ethernet and Wi-Fi Internet access data monitoring and filtering system using Fortigate with UTM software.	LITNET provides a monitoring and filtering system for Ethernet and Wi-Fi connection to the Internet Arrangement of Internet explorer systems and interoperable connection software for Data bases and data warehouses
1. 1	Internet and cloud for communication and information sharing	WAN, LAN, INT (~ 1 Gb/s, WIFI (~ 1 Mb/s, ~200 Mb/s). INT fiber optic connection via LITNET	All PCs and smart devices		In „Google For Education platform applied safety and filtering systems	The Google For Education platform provides applications for stationary work and learning places and smart apps for phones, tablets and smart screens. Office 365 platform provided to schools by emokykla.lt. The official page of the organization - program PyroCMS, Inc 0.17 s | 14 mb v3.3.3
1. 2	Management of web site of the institution		All jobs and Cloud service stations		Only employees authorized by the institution can connect to the content management systems (CMS) and domain management system of the website.	1. Web platform for managing of web site of educational institution;2. the internet system: iv.lt -web client system for internet site management and domain control and internet service support plan realization.3. The system wolet.lt - virtual server services for web site hosting

The effectiveness of incident solutions should be evaluated each time a solution is used, as the solution can be improved based on the evaluation (Palilingana and Batmetan, 2018). Problem management activities are very closely related to incident management. Practices must be designed to work together in the value chain of organization. The activities of these two practices can be complementary (for example, determining the cause of an incident is a problem management activity that can lead to incident resolution), but they can also conflict (for example, investigating the cause of an incident can delay the actions needed to restore service). Examples of links between problem management, risk management, change enablement, knowledge management and continuous improvement include.

ICT specialists, which are responsible for diagnosing problems, often need the ability to understand complex systems and think about - how various failures could have occurred. Cultivating this combination of analytical and creative skills requires mentorship and time, as well as appropriate training. For these needs applicable became the construction of ITIL as componential and multi-layered infrastructure library, from which the ICT specialists can decide about destroyed components and their relationship with other software components and their dependencies. The part of such components of ITIL in concrete X Educational institution is presented by their relationships in Table 1. All components of ICT library are analysed in our previous work (Dzemydienė et al., 2023).

There are important to extract the set of activities, which are applied in the ICT incident management practices. The activities, which are related to ICT incident management and highlighted as the most important and described in the practice recommendations are shown in Table 2.

Table 2. Different incident management activities related to ICT incident management practices

Activity	Related practices
Investigating the causes of ICT incidents	Such works are solving in problem management stage
Communication with users	Activities in responsibility of ICT Service department
Implementation of changes to products and services	Such works are solved in stages of change enablement; deployment management; project management; release management; software development management
Monitoring the activities of technologies, teams and suppliers	Continues monitoring and event management with software
Management of improvement initiatives	Continuous improvement
Management and fulfilment of service requests	Management of service requests implement the Help desk software
Restoring normal operations after a disaster	Responsible the Service Continuity Management

As the ITIL 4 methodology is universal and flexible, its recommendations only indicate the direction and not specific solutions.

3. The approach of formalization of the decision support activities for solving ICT incident management problems

Problem management activities can be organized as a specific case of risk management: they aim to identify, assess and control risks in any of the four dimensions of service management. It is useful to adopt risk management tools and techniques for problem management. Implementing a solution to a problem is often outside the scope of problem management.

Issue management typically initiates resolution through change enablement and participates in post-implementation review and approving and implementing changes (Figure 1).

Therefore, the ITIL4 incident management flow chart (Figure 1) has 6 steps, which often do not answer all the questions that arise. Therefore, according to the specified direction, it is recommended to create sequences of decisions, actions and processes that meet the needs of your institution.

The algorithm allows actions to be taken when a certain incident occurs and specifies a sequence of actions to resolve the incident. Since ITIL 4 recommends describing the processes by adapting them to your organization, the incident management process of a specific organization can change significantly. In addition, problem management can use knowledge management system information to investigate, diagnose, and resolve problems. Problem management activities can identify opportunities for improvement in all four dimensions of service management. In some cases, solutions can be treated as improvement opportunities, so they are entered into a continuous improvement register (CIR) and continuous improvement methods are used to prioritize and manage them, sometimes as part of backlog products. Many problem management activities rely on employee knowledge and experience rather than following detailed procedures.

The component-based ICT infrastructure of education institutions is shown in Figure 2. It shows that a modern school has a substantial ICT infrastructure, including managed and used information systems, IT services and hardware (here, LMS – Learning Management System, LDAP/AD -LDAP or Active Directory; DMS- Document Management System; CMS- Content Management System, SMTP – e-mail server). This IT infrastructure is becoming difficult for schools to manage, and therefore requires a centralized Service Desk and software to manage it efficiently and respond quickly to incidents.

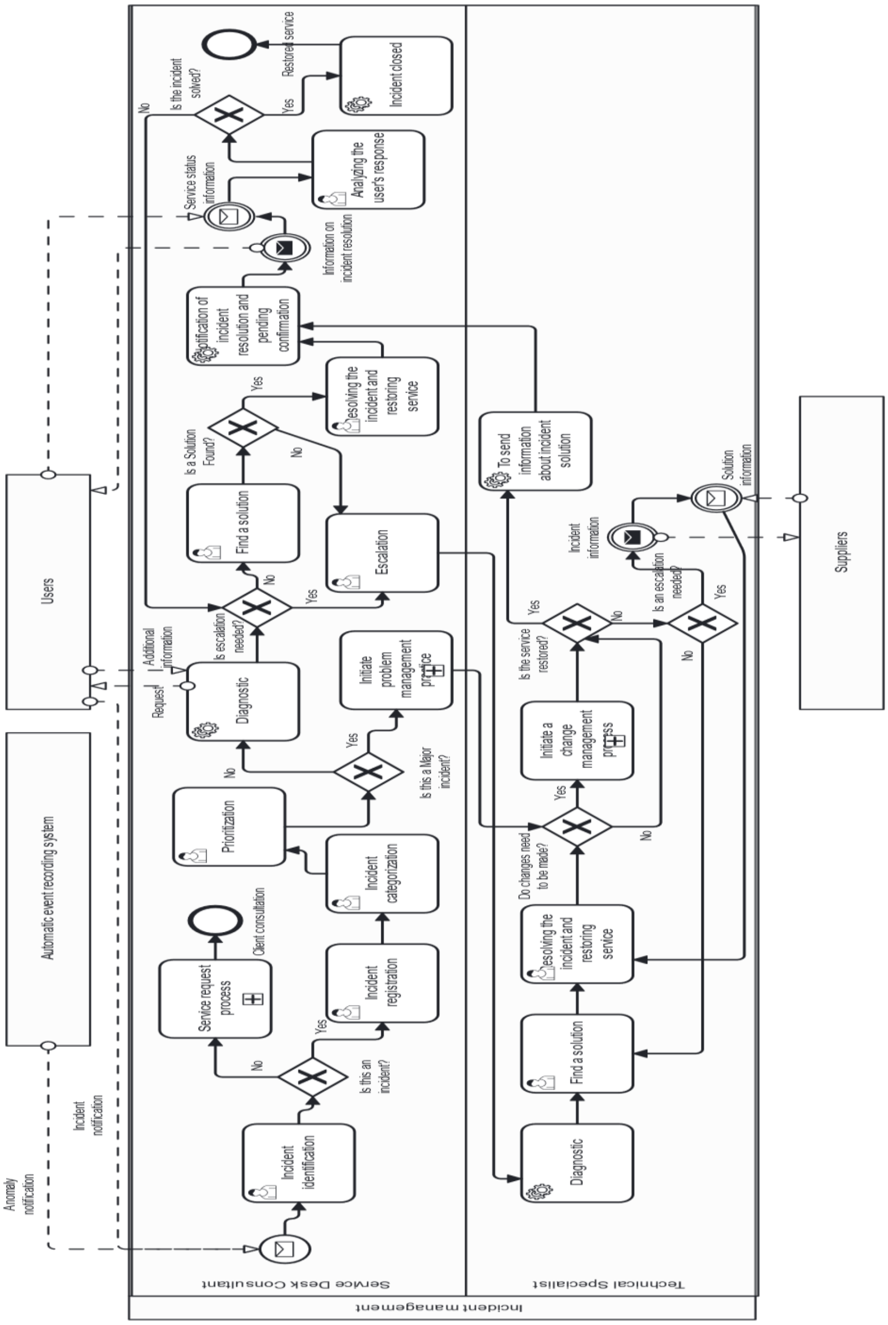


Figure 1. The algorithm of processes of management (including recognition and categorization stages) of ICT incidents (designed by using BPML notation)

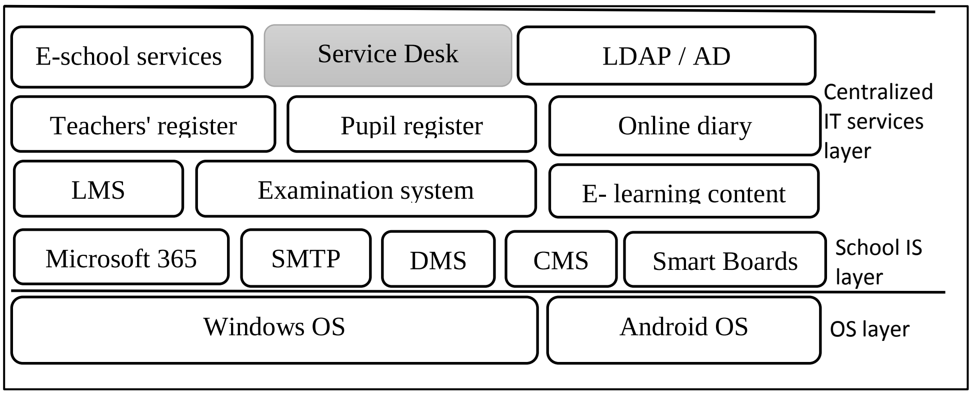


Figure 2. Component-based IT infrastructure of the educational institution

To deal with one of the problems of evaluation of priority of incidents of ICT infrastructure we propose such decision support model in which is introduced the utility function for the different kind of messages about concrete incident. Such messages are evaluated and stored in the weighted context matrix (M_L) for every activated l message (m) about incidents from n layer of ICT infrastructure.

$$M_L = \begin{pmatrix} d_{L_{11}} & d_{L_{12}} & \dots & d_{L_{1n}} \\ d_{L_{21}} & d_{L_{22}} & \dots & d_{L_{2n}} \\ \dots & \dots & \dots & \dots \\ d_{L_{l1}} & d_{L_{l2}} & \dots & d_{L_{ln}} \end{pmatrix} \tag{1}$$

The utility of the messages about incidents can be weighted in a function which assigns a value to each message about incident to be disseminated. The value is calculated by the equation (2):

$$d_{L_{ij}} = (Ty_j + H_j + Ex_j) m_i cr_i Pr_i, \; i = 1,\dots,l, \; j = 1,\dots,n \tag{2}$$

where Ty is the type of destroyed data which values are from the section [1;3]. The values form such section are obtained as follows: (1— the incident is evaluated as not so much important, 2—important, 3—very important). H is the parameter in the interval [0, 1] showing two possibilities:

if the data should be used for historical saving (1) or not (0). Ex is the parameter in the interval [1–4] showing the destroying software infrastructural level (1— for level of Operation systems; 2— for level of IS and own administration systems; 3— for level of other IT services; 4— for level of centrally administrated systems and services) and cr is the coordinates of the software location.

The priority of the message (Pr) is calculated by formula: $\mathrm{Pr}_j = 1 + \frac{\mathrm{I_j}}{\mathrm{A_j}}$ and it is normalized with values falling in a predetermined interval [1–3], where 3 means that the message about the incident priority is critical and it must be disseminated immediately, 2 means that the message about the incident have medium priority, and 1 means that the message about the incident is not important and can be suspended or rejected. $\mathrm{I_j}$ is importance of the message about incident in the interval [0, 1] where 0 is when very high importance is related message and 1 is not so much importance related message. $\mathrm{A_j}$ is message age function with normalized values in predetermined interval [1, 2, 3] which is calculated by (3) where $\mathrm{T_M}$ is difference between current and message compilation time.

$$A = \begin{cases} 1, \text{if } \mathrm{T_M} > 5s \\ 2, \text{if } 1 < \mathrm{T_M} < 5s \\ 3 \text{if } \mathrm{T_M} < 1s \end{cases} \tag{3}$$

The predictive utility of the incident message is based on assigning of weights by a function that assigns a value to each message, enabling to recognize the priority of incidents and to be passed to the recipient entity. The value is calculated according to the formula (2).

According to ITIL recommendations, after registering an incident, it is suggested to move to its categorization stage (Figure 2). This phase consists of a 2-part incident categorization and prioritization. During the categorization phase, incidents are grouped by importance and complexity. Greater granularity is also possible to facilitate their management and analysis (Table 3).

Categorization helps isolate and group incidents based on their nature, such as software errors, equipment failures, or service disruptions. It is important to prioritize disruptions, considering the impact of the incident on the operation of the educational institution and its urgency.

In the prioritization phase, incidents are analysed according to impact and urgency and their levels in order to manage and resolve them more effectively (Table 3).

Priorities are divided according to the impact of the incident on the operation of the institution and according to how quickly the incident needs to be resolved. The impact level indicates how strongly the service disruption affects the organization's operations and the organization's users. Urgency indicates a measure how long it will be until an incident has a significant impact on the business. It is important to decide how long an incident affected the service itself, whether it is completely disrupted and cannot be used at all, whether the service can be used partially, etc. Each organization should develop descriptions of impact, urgency and priorities based on its activities.

Table 3. Categories for assignment of priorities for importance of incidents

		Impact on the disruption of the institution activities			
	Priority	Critical	Tall	Average	Low
Priority according to urgency	Critical	1	1	2	3
	Tall	1	2	3	3
	Average	2	3	3	4
	Low	3	3	4	5

5-level priorities are most commonly used according to (Danby, 2022):

Priority 1 - awarded when an ITIL incident resolution response can be provided within 10 minutes and incident resolution can take up to 3 hours.

Priority 2 - is given when an ITIL incident resolution response can be provided within 20 minutes and the incident resolution duration is up to 6 hours.

Priority 3 - given when an ITIL incident resolution response can be provided within 1 hour, incident resolution duration up to 2 working days.

Priority 4 - given when an ITIL incident resolution response can be provided within 5 hours, incident resolution duration 5 working days.

Priority 5 - given when an ITIL incident resolution response can be provided within 1 day, incident resolution duration up to 2 weeks.

When dealing with incidents, it is very important to assess whether the incident may affect other areas of a measure how long it will be until an incident has a significant impact on the business ICT. During the elimination of the consequences of the incident, the possibility of the spread of the incident and the possible impact on other areas of ICT are investigated.

After eliminating the incident, it is necessary to document it, i.e., to describe what incident happened and to supplement the knowledge base with the methods of solving it. The knowledge base must describe the resolution of the incident related to the signs of the occurrence of the incident.

4. Experimental research of the approach for ICT incident management in an educational institution

According to the recommendations of the ITIL 4 methodology, it is important to properly create a knowledge base covering as many typical procedures as possible, which describes the execution processes and the occurrence of certain incidents and their resolution methods. An educational institution needs to implement standardized cyber security measures and it is important to follow them. The incident management process is considered successful, the result of which is the resolution of the incident in a fast and optimal way, minimizing the impact on service users. The institution, considering its ICT infrastructure and services provided, must create clear and effective incident resolution procedures.

During the experimental study, incidents in the educational institution were recorded using the Help Desk system. Before recording incidents, it is necessary to describe exactly what will be considered an incident. Axelos (2019) compiled guidelines that enable an incident recognition scheme (Figure 3) that indicates when an event can be recorded as an incident and when an event is not considered an incident.

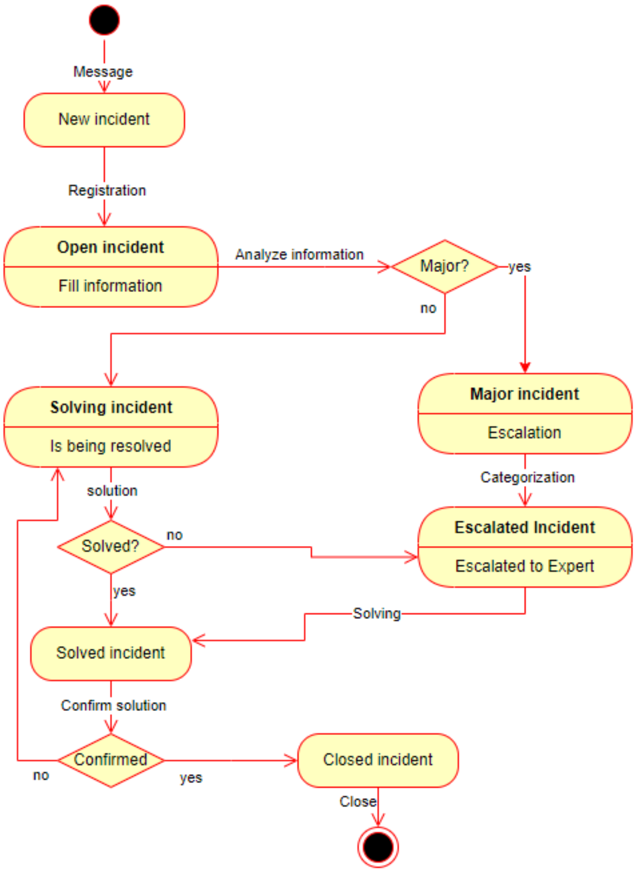


Figure 3. The algorithm of ICT incident solving

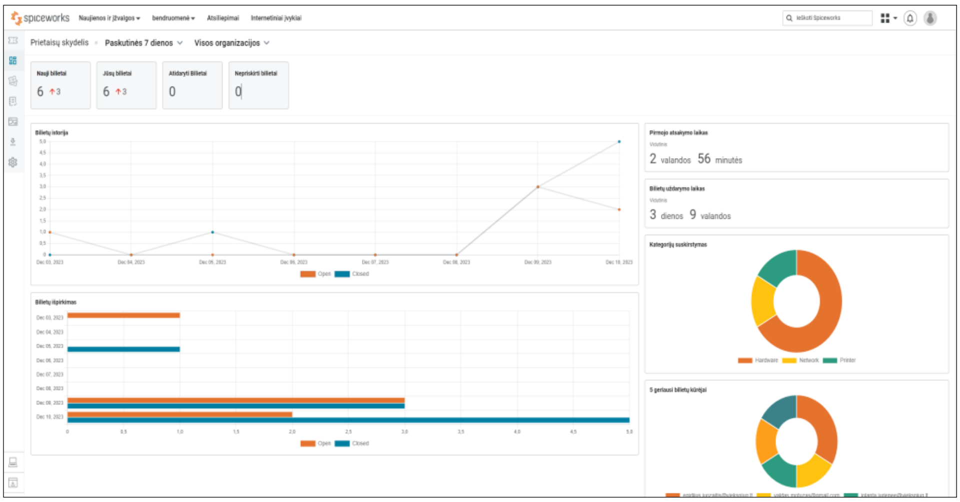
Once an event is determined to be classified as an incident, it is logged in the Help Desk system. Incident management requires a clear description of the process. In the ITIL incident management diagram (Figure 3), it can be seen that incident management is divided into three parts. The first part is registration in the Help Desk system, after which registered incidents are categorized and prioritized. After the incident is resolved, a report and response are prepared to responsible staff and users about the complete resolution of the incident.

If it is determined that it is an incident that requires specialized assistance for its solution and the defined category and assigned priority, the management of the incident is transferred to the institution's ICT technical support. After investigating the incident and reviewing the available knowledge base article, a solution is found to restore the service and, if necessary, additional knowledge base article is added. If the incident cannot be resolved, it is transferred to other specialists, for example for internet providers, technical support of various registers, administrators of e-school accounts, administrators of e-services, etc.

Because ITIL 4 is focused on the user and value creation, almost all events are treated as incidents. In the educational institution, it was decided to follow such an approach that any disruption of ICT services during which the user faces disruptions and inconveniences of disruption of ICT services will be considered as an incident. The scheme of the incident recognition algorithm (Figure 3) was used as the main tool for deciding the type of incidents that occur.

Categories whose violations affect priority assignment can be:

- Software failure;
- Network failure;
- Printer failure;
- Computer system software failure;
- Failures of projectors and smart screens;
- Email mail failures;
- Other equipment failures.



Nauji bilietai 6 ↑3

Jūsų bilietai 6 ↑3

Atidaryti Bilietai 0

Nepriskirti bilietai 0

Pirmojo atsakymo laikas
Vidutinis
2 valandos 56 minutės

Bilietų uždarymo laikas
Vidutinis
3 dienos 9 valandos

Figure 4. The monitoring of ICT incidents in Help Desk – Spice work package

However, within the institution, the teams involved in incident resolution are limited in resources and are often involved in other types of work at the same time. Some incidents should be prioritized over others to minimize the negative impact on users and optimize the use of resources (Axelos Limited, 2019).

In the educational institution, it is recommended to give priorities according to 3 levels:

- High-level - response to ICT incident resolution is possible within 15 minutes, incident resolution time up to 2 hours.
- Medium level - response is possible within 30 minutes, incident resolution time up to 8 hours.
- Low level - response is possible within 1 hour, incident resolution time up to 3 days.

After creating the priority matrix, it is necessary to determine the feedback and solution time intervals for each level. The organization must clearly define which incidents are high-level and which are low-level priorities based on urgency and impact. There can be no ambiguity. It is recommended to divide the level of impact of the incident according to how many users experience the inconvenience caused by the incident.

Possible categorization of incidents and examples of incidents by priority level:

- High level - failure of the institution's server, failures of the main network switches or routers. Those failures affect a large group of workers.
- Medium level - failure of the computer in the training class, Internet problems in one class. These are equipment failures or ICT service disruptions that affect a very small number of users, but have a significant impact on their operations.
- Low level - network printer failure, institution library computer failure. These failures do not significantly affect the educational process of the institution.

The Spiceworks system provides an opportunity to solve different types of faults (Figure 5). This system can help not only when administering several departments of the institution, but also when you want to test new configuration settings or changes and you don't want to distort the data in actual work.

During the entire 3-month incident registration period, 22 potential incidents were reported, of which 18 were reported by phone, 3 were reported by email, and one was reported through the incident reporting portal. During the experiment, it turned out that registration by phone is the easiest and most reliable method for employees of the institution.

Of the 22 reports of potential incidents received, 9 were false incidents. A false incident can be defined as the inability to properly use ICT services due to improper user actions.

Of the 13 registered incidents, their failure categories were distributed as follows:

- 6 network failures;
- 3 printer failures;
- 2 computer equipment failures;
- 1 failure of projectors and smart screens.
- 1 email failure.

The registered incidents were divided according to priorities: High priority - 5, Medium priority - 5 and Low priority - 3. The percentage of high priority incidents is unusually high, because the network failures affected a large part of the users, so the solutions to the incident had to be implemented quickly.

Incident management metrics are an important part of ICT service management as they help organizations monitor how effectively ICT disruptions and incidents are handled. Metrics can cover a variety of aspects, from the number of incidents to the time it takes to resolve them. Table 4 provides key practice metrics that should be applied depending on the institution's context, such as incident priority levels, expected incident resolution periods.

From the list of key incident management evaluation parameters, it follows that the weakest point is in automation. Both the early detection of incidents and their automatic resolution are not properly included in the institution's incident management. There is no clear indication of user satisfaction with incident management and resolution, as there is no integrated assessment tool in incident management reports. Incident management and resolution times do not exceed the times assigned to the priority levels.

A maturity model is used to check how one of the good practices can be applied in the ICT management of the institution. The ITIL Maturity Model defines the following competency levels for any management practice:

Table 4. Main parameters of incident removal detected during the experimental 3 months period

Practiced success factors	Main evaluation parameters	Results
Detect incidents early	Time from incident occurrence to detection.	Δt is 1 working day period
	Percentage of incidents detected by event monitoring and management.	0%
Fast and efficient resolution of incidents	The time from the detection of the incident to the start of the diagnosis.	High level, when Δt< 11 min.
	Time of diagnosis.	Intermediate level, when Δt < 25 min.
	Number of assignment changes.	Low level, when Δt < 1 hour
	The percentage of waiting time in the total incident management time	High level , when Δt < 15 min.
	First time solution frequency.	Intermediate level, when Δt < 30 min.
	Fulfillment of the agreed solution time.	Low level, when Δt < 45 hrs.
	User satisfaction with incident management and resolution.	Is expressed in grade [0;5]
	Percentage of incident that was resolved automatically.	0%
	Percentage of incidents resolved before notifying users.	77%
Continuous improvement of incident management	Incident resolution percentage using previously identified and recorded solutions.	100%
	Percentage of incidents resolved using incident patterns.	There are no exact data
	Improving key practice indicators over time.	0%
	Balance between incident resolution speed and efficiency metrics.	0%

Δt – is time duration spending on the process

Level 1. The practice is not well organized; it is executed as initial or intuitive. It may occasionally or partially achieve its goal through an incomplete set of activities.

Level 2. The practice systematically achieves its goal through a core set of activities supported by specialized resources.

Level 3. The practice is well defined and achieves its purpose in an organized manner, using dedicated resources and relying on inputs from other practices that are integrated into the ICT service management system.

Level 4. The practice achieves its goal in a highly organized manner, and its results are continuously measured and evaluated in the context of the service management system.

Level 5. Practice continuously improves organizational skills related to its purpose.

For each practice, the ITIL Maturity Model defines criteria for each capability level from level two to level five. According to these criteria, the practice's ability to fulfil its purpose and contribute to the institution's ICT service value system can be assessed (Axelos Limited, 2019).

The most important aspects of implementing ITIL incident management practices in an educational institution according to (Thirthappa, 2023) are:

• Inclusion of regular instructions for user’s instructions: clear instructions must be provided on how to report incidents and what to do in the event of an incident.

• Organizing the feedbacks: is necessary to regularly collect feedback from users and adjust processes based on the information received.

• Applying the flexibility of adaptation of alternative software during incident’s solving process: IT specialists have to be able to adapt to changing needs and circumstances in the educational environment.

• Forming of innovative organizational ICT culture: in ICT culture that values openness and learning, employees are more likely to actively participate in incident management processes, share ideas and learn from incidents. The culture encourages a proactive approach to incident management, emphasizing learning and improvement rather than assigning blame.

• Organizing of responsible employee training: provides employees with the necessary skills and knowledge to effectively respond to incidents, helps to better understand the incident management process. In a culture that encourages learning and development, employees are better equipped to handle incidents, allowing for faster and more effective decisions.

The involvement and commitment of managers and leaders promotes a fair and effective incident management culture. They can invite open communication, support learning opportunities, and lead by example.

Conclusions

An approach of ICT incident management is proposed in this article. The approach includes all stages of ICT incident management: from the ICT service management analysis of the educational institution, until identifying of the weak links for proper incident management. Among the weaker ones, we can mention the unforeseen procedures that must be solved by ICT employees, in the event of technical disturbances, the failure registration and decision-making process is not carried out, the training of employees is not carried out systematically or not at all, attention is not paid to the creation of the institution's ICT culture.

In order to solve information technology infrastructure incidents, we apply the ICT incident management practices recommended in the ITIL 4 methodology, providing for specific steps to eliminate incidents, assigning responsible persons and choosing appropriate software tools for incident management, and training employees on how to react to incidents of the appropriate type.

Based on best practice metrics, it is recommended to create a knowledge base to store knowledge about incident resolution actions.

The experimental study showed that it is often difficult to determine the time interval between the occurrence of an incident and its registration, because incidents are registered only when users encounter disruptions in ICT services. Monitoring and event management practices, monitoring systems, and incident management software were used to address this issue, which enabled easier identification of incident types and immediate initiation of the resolution process.

Based on the data of the conducted research in accordance with the recommendations of the ITIL 4 methodology, it is proposed to organize incident management in an educational institution starting with incident registration, classification, decision-making, and solving the incident. Then the preparation of reports and the expansion of the knowledge base are prepared. Regularly review and improve incident management processes based on research and experience. This includes updating the processes, tools and methods used. Promote cooperation with other educational institutions and ITIL experts, sharing best practices.

References

AXELOS Limited (2019). ITIL Foundation: ITIL v4 Edition. ISBN: 9780113316069.

AXELOS Limited (2020). ITIL 4: Create, Deliver and Support: First edition 2020. ISBN: 9780113316328.

AXELOS Limited (2021). ITIL® Practices in 2000 words: Incident management, service desk, and service request management.

Danby, S. (2022). ITIL Priority Matrix: How to Use it for Incident, Problem, Service Request, and Change Management. Access by Internet [2023-09-10]: https://blog.invgate.com/itil-priority-matrix

Dzemydaitė, G., Naruševičius, L. (2023). Exploring efficiency growth of advanced technology-generating sectors in the European Union: a stochastic frontier analysis. Journal of Business Economics and Management, 24(6), 976-995. https://doi.org/10.3846/jbem.2023.20688

Dzemydienė, D., Dzemydaitė, G., Gopisetti, D. (2022). Application of multicriteria decision aid for evaluation of ICT usage in business. Central European Journal of Operations Research, 30(1), 323-343. https://doi.org/10.1007/s10100-020-00691-9

Dzemydienė, D., Turskienė, S., Šileikienė, I., Baltrukaitis, A., Kazlauskienė, A. (2022). Development of ICT infrastructure management services for educational establishments (in Lithuanian). ALTA’22. Advance learning Technologies and Applications. Annual International conference for education : Conference proceedings 30th of November, 2022 / edited by Danguolė Rutkauskienė. Kaunas: Kaunas University of Technology. p. 125-147. https://ndma.lt/alta2022/wp-content/uploads/2023/04/ALTA'22%20proceedings.pdf

Dzemydienė, D., Turskienė, S., Šileikienė, I. (2023). Development of ICT infrastructure management services for optimization of administration of educational institution activities by using ITIL-v4. Baltic Journal of Modern Computing, vol. 11, no. 4, p. 558-579. DOI: 10.22364/bjmc.2023.11.4.03.

Gillingham, J. (2023). Key ITIL Concepts That One Should Know. Access by Internet [2023-10-22]: https://www.invensislearning.com/blog/key-itil-concepts/

Howells, C. (2020). ITIL Practices. Access by Internet . [2023-08-14]: https://cdn.ymaws.com/www.itsmfusa.org/resource/resmgr/ITIL4_Session_4-ITIL_Practic.pdf

ITIL®4 Practice Guide (2023), Incident Management. Access by Internet [2023-08-14]: https://www.scribd.com/document/600322911/Practice-Incident-management-ITILv4

ITIL®4 Management Practices. Access by Internet [2023-08-11]: https://www.knowledgehut.com/tutorials/itil4-tutorial/itil-management-practices-processes

Kaplan, S. (2023). What Is Organizational Culture and Why Is It Important? Access by Internet [2023-08-14]: https://www.psychologytoday.com/us/blog/the-power-of-experience/202312/what-is-organizational-culture-and-why-is-it-important

Key ITIL Concepts That One Should Know. Access by Internet [2023-09-17]: https://www.invensislearning.com/blog/key-itil-concepts/

Palilingan, V.R.; Batmetan J.R.(2018). Incident Management in Academic Information System using ITIL Framework. IOP Conference Series: Materials Science and Engineering, Volume 306, 2nd International Conference on Innovation in Engineering and Vocational Education,25–26 October 2017, Manado, Indonesia IOP Conf. Ser.: Mater. Sci. Eng. 306, 012110, DOI 10.1088/1757-899X/306/1/012110

Shepherd, H. (2019). ITIL 3 vs. ITIL 4 – What has changed and what is new? Access by Internet [2023-09-16]: https://advisera.com/20000academy/blog/2019/07/04/itil-3-vs-itil-4-what-has-changed-and-what-is-new/.

Thirthappa, K. (2023). Building a culture of incident response. Access by Internet [2023-11-12]: https://spike.sh/blog/building-a-culture-of-incident-response.

Received June 18, 2024, revised August 30, 2014, accepted September 13, 2024