Analysis of Information Technology Security Management SWCU SIASAT Using ISO/IEC 27001:2013

Andeka Rocky Tanaamah[1], Friska Juliana Indira[2]

***Abstract*—IT security management is essential for organizations to notice the occurring risks and opportunities because they will profoundly affect the ongoing business processes within the organization. The Satya Wacana Academic Information System, more often called SIASAT, is an IT component playing an essential role in running core business processes at Satya Wacana Christian University under the control of the Information Systems and Technology Bureau. At this time, the implementation of SIASAT has been going well, but there are still some obstacles. Lack of human resources is one of the findings and one it becomes of the most significant risks as it affects the use of infrastructure and information security. This research was conducted using the international standard ISO/IEC 27001:2013, prioritizing information security by taking a planning clause focusing on risk assessment. From the results of this study, there were nine recommendations given. Some of which were the most important, i.e., creating separated standard operating procedure documents for SIASAT, which previously were still affiliated with the Academic Administration Bureau; distributing job descriptions; and providing clear and documented access rights for everyone. It is expected that this research can reduce the occurring risks and can be considered for establishing improvements to enhance academic services in the future.**

***Keyword*—Information Technology, Information System, Information Security Management, ISO/IEC 27001:2013.**

I. INTRODUCTION

In the present day, the role of Information Technology (IT) in an organization in supporting business activities is crucial. Problems related to information security often receive less attention, while they are the most crucial part of the information technology application. The increased internal data transmission and utilization between organizations on an open network will increase the risks of the information being exposed [1]. Information security is defined as a process to protect information and information assets and keep the confidentiality, integrity, and availability of information [2]. Confidentiality is a term used to prevent information disclosure to unauthorized parties. Integrity means that the data cannot be modified. Availability means that information must be accessible whenever and wherever data is required by authorized users [3].

Today, information security is a leading problem for a business. A survey shows that such risks applying to public bodies and private companies, information in the form of paper and electronics, from failure to protect direct data or failure to dispose of archive information may arise from intentional or accidental actions [4]. Risk management is defined as the process of identifying vulnerability and threats in a framework of an organization. In addition, it will produce several measurements to minimize the impact on information resources [5].

One university that is already aware of the application of IT as an essential requirement in conducting academic activities is Satya Wacana Christian University (SWCU). Managed by Bureau of Technology and Information Systems (BTSI), which is under the Assistant Chancellor I of SWCU, this bureau is in charge of developing and serving the needs of academics in the fields of information technology, information system, multimedia (including developing teaching modules), and teaching facilities [6]. One of the information technologies implemented and utilized is the Satya Wacana Academic Information System, better known as SIASAT. It is a mobile web-based information system integrated by several services to facilitate and support academic activities in SWCU. Today, the SIASAT is one of the essential parts that must be used in academic activities both by lecturers and students. The services provided for lecturers are in the form of teaching schedules, guardianship, and grade inputs. Meanwhile, the services provided for students are re-registration, course registration, course requests, study cards, study results, class schedules, grade transcripts, semester billing information, undergraduate thesis or thesis registration, and book borrowing information.

As a bureau providing information systems and information technology to all academic users, BTSI is responsible for data security and the managed information; one of them is in SIASAT. Along with its implementation, weaknesses and threats that arise in the system can disrupt the ongoing academic process. These threats can arise from the outside and within the system itself. Cases related to information security, such as loss of student data during the course registration process, are often encountered; of course, it is detrimental to students because it affects the lecture process for the next semester. Student accounts' hacking, so that related students cannot enter into their accounts, is still common. Up to now, students often complain about servers that are often down during the course's registration process.

Previously, the Yemeni Academy for postgraduate studies (YAGS) employed the ISO/IEC 27001:2013 standard to determine the maturity level of information security. The results of the study indicate that the maturity level is at level 2. The gap value between the current maturity level with the expected maturity value was 3.19. It means that many control

[1,2] *Department of Information Systems, Faculty of Information Technology, Satya Wacana Christian University, Jln. Diponegoro No. 51-60, Salatiga, 50711, INDONESIA (phone: 0298-321212; fax: 0298-324197; e-mail: [1]atanaamah@uksw.edu, [2]682015002@student.uksw.edu)*

weaknesses prevail. Hence, related security policies and procedures must be developed, and a security management system and culture must be implemented [7]. In other studies, ISO/IEC 27001:2013 is also used to implement information security for government digital archives based on cloud computing in the Republic of Indonesia's national archives to reduce the impact of integrity loss, confidentiality, and information availability risks [8]. Likewise, research on the case of applying radio frequency identification (RFID) at FTI-SWCU still found security in the laboratory related to Standard Operating Procedures (SOPs) that had not been documented. Therefore, ISO 27001:2013, which focuses on the Information Security Policy domain, is needed as a direction and management support in the application of information security [9]. DPTSI-ITS also designed SMKI documents based on ISO/IEC 27001:2013 and conducted information security risk management based on ISO/IEC 27005:2013 with the results of the study obtained 60 risks that were not received from a total of 228 identified risks [10].

Referring to the previously mentioned understanding, this study aims at analyzing information technology security management in the Satya Wacana Academic Information System (SIASAT) by utilizing ISO/IEC 27001:2013. It aims to see the condition by conducting risk and chance analyses to find out the impact magnitude on the institution. ISO/IEC 27001:2013 was chosen because it is an international standard that specifically prioritizes the information security factor, which has ten clauses and has an appropriate list of controls to be used as an assessment guideline [11]. Based on the needs required in this study of the ten available clauses, the researcher focused on the planning clause as a guideline for conducting risk assessments. By doing this research, it is expected to be able to see how well the IT services have been provided, to know the extent of the threats and risk opportunities that occur. In addition, it is expected that the results of this assessment can be used when making policy in dealing with risks to improve service performance by BTSI as a responsible service provider bureau.

II. Qualitative Research

A. ISO/IEC 27001:2013

The main focus of this research is to see the implementation of SIASAT in the academic environment and the extent to which information security management is implemented following the ISO/IEC 27001:2013 standard. This study was conducted using a qualitative method by conducting interviews with resource persons related to SIASAT so that the authors could explore any information that would be used as research materials. Interviews were conducted together with two resource persons, i.e., the Head of SWCU BTSI and the Head of SWCU BTSI Information System Division. In conducting the interview, ISO/IEC 27001:2013 was used as a guideline to compile the question list. ISO/IEC 27001:2013 was chosen because it is an accurate standard in providing an illustration of what must be done by an organization in implementing the risk assessment concept and information security control handling that can be adjusted to the organization's needs [12]. This standard adopts the "Plan-Do-Check-Act" (PDCA) model, which involves the stages of identifying risks that must be known well, then analyzing the occurring risk impacts, evaluating, and providing countermeasures against these risks with the output in the form of a document of findings and recommendations [13].

Fig. 1 Research stages diagram.

B. Research Stages

This research stage began with a preliminary study at the BTSI by looking at the system's vision, mission, and workflow. The preliminary stage of this research was started by conducting a literary study by studying books, articles, journals, and other scientific papers related to information security management analysis. A preliminary study considering the vision, mission, and workflow of SIASAT was also conducted to obtain more profound knowledge related to the object of research studies. It was then continued with the second stage of problem identification. The process of identifying problems was carried out to look at the problems occurring in the SIASAT as well as to compile a list of interview questions based on guidance from ISO/IEC 27001:2013. It focused on planning clauses in which it focused on actions to address risks and opportunities and information security and planning objectives following the research focus.

After identifying the problem and compiling the interview question list, the following third stage was continued with data collection by conducting interviews with related resource persons. A voice recorder assisted the interview process served as evidence that can be accounted for and supports this research. In the fourth stage, the interview results that had been conducted were processed into data that was a risks and findings identification of problems occurring in the SIASAT. The risk was measured based on the generated impact or influence on the likelihood of risk [14]. Thus, based on the findings, recommendations for improvement can be given, and the conclusions from the study results can also be drawn. The research stages are presented in Fig. 1.

TABLE I
IDENTIFICATION OF FINDINGS OF RISK AND OPPORTUNITIES IN SWCU SIASAT

Code	Type	Findings	Cause
R 1	Risk	There was no specific Standard Operating Procedures (SOP) for SIASAT.	Up to now, the SIASAT SOP has been following the SOP owned by Administration and Registration Bureau (BARA).
R 2	Risk	The access rights of each user and each part were not clearly documented.	The BTSI single administrator had to permit users to access specific needs.
R 3	Risk	There was no control access document for SIASAT.	There were no human resources specifically appointed to carry out detailed documentation.
R 4	Risk	There was no clearly documented job description division for each section.	The limitation of reliable and skilled human resources to be responsible for having control in SIASAT.
R 5	Risk	IT Infrastructure Damage.	Unexpected natural disasters could damage some existing IT infrastructure.
R 6	Risk	The server was down.	Interrupted network connection from a third-party service provider.
R 7	Risk	Student SIASAT account hacking by other students.	Student negligence in logging in and logging out and not altering the password template from BTSI in following the recommendations.
P1	Opportunity	BTSI had an IT infrastructure that met the qualifications and specifications.	Had good cooperative relationships with service providers and had sufficient funds to carry out demand for needs following the results of joint work meetings with stakeholders.
R 8	Risk	Server Room Security.	In and out accesses of the server room were still not restricted, especially for parties who had special authority outside the BTSI who were still allowed to enter.

TABLE II
LIKELIHOOD ASSESSMENT RESULT

Risk Identification			Inherent Risk
Code	Categories	Consequences	Likelihood Assessment
R 1	Infrastructure	There was no specific standardization in the usage scheme, the person in charge, to the SIASAT maintenance.	Almost Certain
R 2	Infrastructure	It resulted in losses, primarily material that could disrupt the course of business processes.	Unlikely
R 3	Infrastructure	The course registration process would be disrupted.	Likely
R 4	Infrastructure	Service performance could be continuously improved.	Almost Certain
R 5	Human Resources	Some small things that should be the job description of each section would depend on the administrator.	Almost Certain
R 6	Human Resources	Difficulties finding out the job description and access rights clearly when needed.	Almost Certain
R 7	Human Resources	Some people did double job descriptions that interfered with productivity in the main job description.	Almost Certain
P 1	Software	The delay in the process of registration of the course is detrimental to the students themselves.	Almost Certain
R 8	Hardware Security	The possibility of interest misuse by irresponsible parties.	Moderate

III. RESULTS AND DISCUSSION

Based on the results of interviews conducted with key informants, there are several risks and opportunities in the SWCU SIASAT described in Table I.

A. Risk Identification and Inherent Risk

Referring to the standard guideline of ISO/IEC 27001:2013, it is explained that risks and opportunities must be translated into risk categories, types, causes, and consequences. After identifying the risks and opportunities of SWCU SIASAT, in Table II, the criteria assessment process is described. The purpose of this elaboration is to take a deeper look at the identification of risks and opportunities. In addition, it assesses how significant the risks and opportunities are by carrying out an inherent risk analysis process, which includes assessing the likelihood of risk occurrence, assessing the consequences of risk occurrence, and risk level. An inherent risk assessment was conducted to determine the extent of the occurring risks and opportunities used to measure the good and harmful impact on the service of academic activities at the university.

B. Likelihood Assessment

Likelihood assessment is a crucial stage in determining the period of occurring risk or opportunity by looking back at the causes of information technology risks and opportunities. Measurements on the likelihood assessment are divided into five qualitative measurement categories, i.e., almost certain (once or more in one year), likely (once in two years), moderate

TABLE III
CONSEQUENCES ASSESSMENT RESULT

Risk Identification			Inherent Risk	
Code	**Categories**	**Consequences**	**Likelihood Assessment**	**Consequences Assessment**
R 1	Infrastructure	There was no specific standardization in the usage scheme, the person in charge, to the SIASAT maintenance.	Almost Certain	Catastrophic
R 2	Infrastructure	It resulted in losses, primarily material that could disrupt the course of business processes.	Unlikely	Catastrophic
R 3	Infrastructure	The course registration process would be disrupted.	Likely	Moderate
R 4	Infrastructure	Service performance could be continuously improved.	Almost Certain	Catastrophic
R 4	Human Resources	Some small things that should be the job description of each section would depend on the administrator.	Almost Certain	Major
R 5	Human Resources	Difficulties finding out the job description and access rights clearly when needed.	Almost Certain	Minor
R 6	Human Resources	Some people did double job descriptions that interfered with productivity in the main job description.	Almost Certain	Minor
P 1	Software	The delay in the process of registration of the course is detrimental to the students themselves.	Almost Certain	Minor
R 7	Hardware Security	The possibility of interest misuse by irresponsible parties.	Moderate	Minor

TABLE IV
RISK MATRIX

Consequences	**Likelihood**				
	Almost Certain	**Likely**	**Moderate**	**Unlikely**	**Rare**
Insignificant	**H**	**H**	**E**	**E**	**E**
Minor	**M**	**H**	**H**	**E**	**E**
Moderate	**L**	**M**	**H**	**E**	**E**
Major	**L**	**L**	**M**	**H**	**E**
Catastrophic	**L**	**L**	**M**	**H**	**H**

(once in five years), unlikely (once in ten years), and rare (once in fifty years). From the results of the identification of the previous risk findings, likelihood assessment could be done based on the risks and opportunities in the SWCU SIASAT, which is described in Table II.

C. Consequences Assessment

After the Likelihood Assessment was carried out, the next step was the Consequences Assessment stage. The difference between these two assessments is that the likelihood assessment talks about the period while the consequences assessment measures the impact of material losses. However, these two things are interrelated where the likelihood assessment can affect the assessment consequences that arise from the occurring risks and opportunities. The level of consequence assessment is divided into five rating categories, i.e., catastrophic (loss of more than $10 million), major (loss of between $5-$10 million), moderate (loss of between $1-$5 million), minor (loss of between $100 thousand-$1 million), and insignificant (loss of less than $100 thousand).

The results from the consequences assessment of the risks and opportunities of the SWCU SIASAT are described in Table III.

D. Risk Level Assessment

The risk level assessment was carried out to measure the level of risk and opportunity contained in the SWCU SIASAT so that the relevant management would pay attention to it. The risk level assessment is divided into four levels, namely extreme risk (requires immediate action), high risk (requires senior management's attention), moderate risk (specific responsible management), and low risk (managed by routine procedures). The results of this risk level assessment could determine the risk owner who was responsible for evaluating risks and opportunities. The risk matrix was used to facilitate the risk level assessment process described in Table IV, which was based on the likelihood assessment and consequences assessment results that had been carried out previously.

Considering the results of the identification of likelihood assessment and consequences assessment that had been conducted, then an assessment of the level of risk based on the risk matrix to obtain the overall assessment results could be carried out. The overrall assessment result is presented in Table V.

E. Risk Evaluation

The risk and opportunity evaluation stage were carried out by comparing the risk analysis results with the risk criteria prepared previously and making risk analysis the main focus of risk management in the future. The risk evaluation process in this study compared risk analysis results, including likelihood assessment, consequences assessment, and risk level assessment with risk criteria covering risk categories, types of

TABLE V
OVERALL ASSESSMENT RESULT

Risk Identification			Inherent Risk		
Code	**Categories**	**Consequences**	**Likelihood Assessment**	**Consequences Assessment**	**Risk Level**
R 1	Infrastructure	There was no specific standardization in the usage scheme, the person in charge, to the SIASAT maintenance.	Almost Certain	Catastrophic	Extreme Risk
R 2	Infrastructure	It resulted in losses, primarily material that could disrupt the course of business processes.	Unlikely	Catastrophic	Extreme Risk
R 3	Infrastructure	The course registration process would be disrupted.	Likely	Moderate	High Risk
R 4	Infrastructure	Service performance could be continuously improved.	Almost Certain	Catastrophic	Extreme Risk
R 4	Human Resources	Some small things that should be the job description of each section would depend on the administrator.	Almost Certain	Major	Extreme Risk
R 5	Human Resources	Difficulties finding out the job description and access rights clearly when needed.	Almost Certain	Minor	High Risk
R 6	Human Resources	Some people did double job descriptions that interfered with productivity in the main job description.	Almost Certain	Minor	High Risk
P 1	Software	The delay in the process of registration of the course is detrimental to the students themselves.	Almost Certain	Minor	High Risk
R 7	Hardware Security	The possibility of interest misuse by irresponsible parties.	Moderate	Minor	Moderate Risk

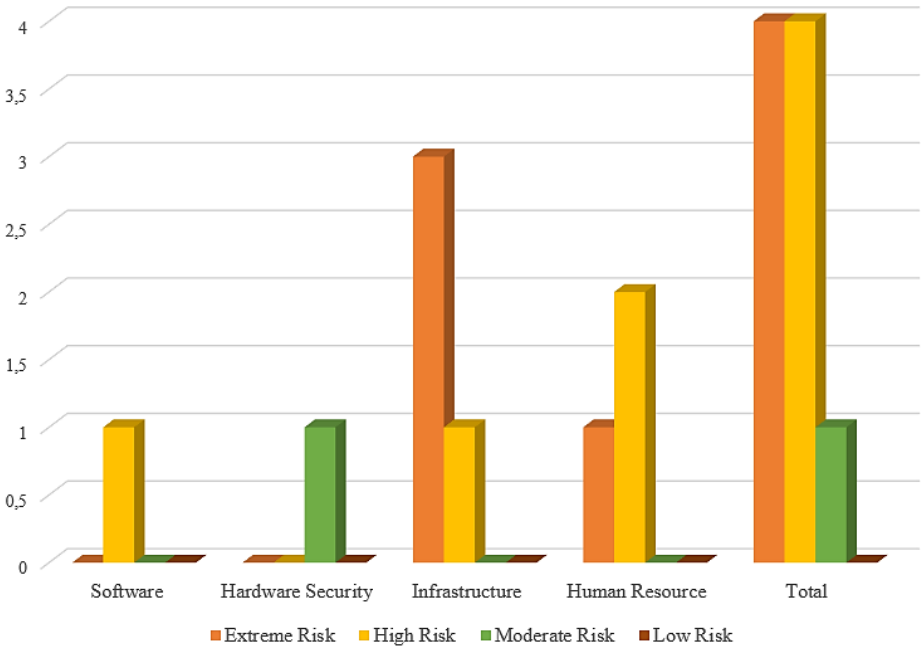

Fig. 2 Comparison chart of risk categories and risk levels.

risks, causes, and consequences. The results of this risk evaluation are presented in the form of a diagram in Fig. 2.

Fig. 2 describes the comparison of risk levels and risk categories as well as opportunities according to the results described in Table V. From the diagram, it can be seen that the numbers of extreme risk, high risk, and moderate risk levels are 4, 4, and 1, correspondingly. The categories that fall into extreme risk were infrastructure and human resources. Categories that fall into high risk include software, infrastructure, and human resources. One category that is included in moderate risk is hardware security. Thus, it can be concluded that SIASAT has high IT risks and opportunities for negative impacts, which in the future can cause obstacles to services that have been implemented and can also experience material losses.

F. Recommendation

From the overall assessment process, the obtained findings along with the risks and opportunities will be given recommendations for future improvements to reduce the impact of the generated risks and opportunities. The recommendations are presented in Table VI.

TABLE VI
RECOMMENDATION

Categories	Findings	Recommendation
Human Resources	The administrator must grant access to users to access specific basic needs.	Clarify and give access rights for each user according to their part and responsibility so that when they need some things, they do not always depend on the administrator.
Human Resources	There were no human resources specifically appointed to carry out detailed documentation.	Look for qualified human resources in preparing access control documents.
Human Resources	The limitation of reliable and skilled human resources to be responsible for having control in SIASAT.	Conduct training for human resources so that they have an IT facility usage standard.
Infrastructure	Up to now, the SIASAT SOP has been following the SOP owned by Administration and Registration Bureau (BARA).	It is necessary to make an SOP that is documented separately between SIASAT SOP and BARA SOP so that it is easier to distinguish when there are arising problems, especially in the SIASAT.
Infrastructure	Unexpected natural disasters could damage some existing IT infrastructure.	Ensure that vital data backups are carried out regularly in separate places and ensure that the installation of IT infrastructure is minimized in locations prone to natural disasters.
Infrastructure	Interrupted network connection from a third-party service provider.	Ensure to choose trusted and stable network service providers and consistently monitoring the network, especially at times before the course registration
Infrastructure	Had good cooperative relationships with service providers and had sufficient funds to carry out demand for needs following the results of joint work meetings with stakeholders.	Always ensure that the use of IT resources is maximized and according to needs.
Software	Student negligence in logging in and logging out and not changing the password template from BTSI in following the recommendations.	Always advise students to change passwords and no longer use the password from BTSI, ensure that students do not recklessly log in on various devices, and remember the logging out process after finishing using SIASAT.
Hardware Security	In and out accesses of the server room were still not restricted, especially for parties who had special authority outside the BTSI who were still allowed to enter.	Providing strict security and confirming who has permission and responsibility to enter and exit the server room.

IV. CONCLUSIONS

Based on the results of the overall analysis of the SWCU SIASAT condition, there were nine findings with eight risks and one opportunity. After assessments on the findings were conducted, it can be concluded that the need for risk handling procedures is mainly related to the employed information technology infrastructure. The response to human resource management also needs to be considered concerning the number and ability of human resources required by BTSI to achieve work effectiveness and efficiency. Information technology risks causing negative impacts also need to be given special attention and handled immediately by considering the recommendations that have been given. Together with university leaders and responsible management, the Head of BTSI, as senior management responsible for the running of this business process, needs to communicate internal problems related to the needs needed by BTSI, especially in handling SIASAT and the related instruments within. Therefore, services run better according to expectations.

REFERENCES

[1] G. Disterer, "ISO/IEC 27000, 27001, and 27002 for Information Security Management," *Journal of Information Security*, Vol. 4, No. 2, pp. 92-100, Apr. 2013.

[2] *Information Technology - Security Techniques - Code Practices for Information Security Management*, International Standard ISO/IEC 17799:2005, 2005.

[3] G. Pavlov and J. Karakaneva, "Information Security Management System in Organization," *Trakia Journal Sciences*, Vol. 9, No. 4, pp. 20-25, 2011.

[4] A. Gillies, "Improving the Quality of Information Security Management Systems with ISO 27000," *The TQM Journal*, Vol. 23, No. 4, pp. 367-376, 2011.

[5] S. Al-Dhahri, M. Al-Sarti, and A.A. Aziz, "Information Security Management System," *International Journal of Computer Applications*, Vol. 158, No. 7, pp. 29-33, Jan. 2017.

[6] (2021) BTSI UKSW. [Online], https://btsi.uksw.edu/pages/sekilas-btsi, access date: Jan. 30, 2021.

[7] A.A. Nasser, "Information Security Gap Analysis based on ISO 27001: 2013 Standard: A Case Study of the Yemeni Academy for Graduate Studies, Sana'a, Yemen," *International Journal of Scientific Research in Multidisciplinary Studies*, Vol. 3, No. 11, pp. 4-13, Dec. 2017.

[8] D. Rutanaji, S.S. Kusumawardani, and W.W. Winarno, "Penggunaan Kerangka Kerja SNI ISO/IEC 27001:2013 untuk Implementasi Tata Kelola Keamanan Informasi Arsip Digital Pemerintah Berbasis Komputasi Awan (Arsip Nasional RI)," *Prosiding Seminar Nasional GEOTIK*, 2018, pp. 131-140.

[9] Y. Darmawan and A.F. Wijaya, "Analisis Sistem Manajemen Keamanan Informasi pada Perguruan Tinggi Menggunakan ISO 27001:2013," *Seminar Nasional Sistem Informasi Indonesia*, 2017, pp. 285-286.

[10] F. Mauladani and D.O. Siahaan, "Perancangan SMKI Berdasarkan SNI ISO/IEC27001:2013 dan SNI ISO/IEC 27005:2013 (Studi Kasus DPTSI-ITS)," *Computer Science Research and Its Development Journal*, Vol. 10, No. 1, pp. 56-67, Feb. 2018.

[11] P.G. Anarkhi, A.H.N. Ali, and I. Kurnia, "Penyusunan Perangkat Audit Keamanan Informasi Aplikasi Berbasis Web Menggunakan ISO/IEC 27001 Klausul Kendali Akses," *Jurnal Teknik POMITS*, Vol. 1, No. 1, pp. 1-5, 2013.

[12] *Information Technology - Security Techniques - Information Security Management Systems - Requirements*, International Standard ISO/IEC 27001:2013, 2013.

[13] ISACA Germany Chapter, *Implementation Guideline ISO/IEC 27001:2013: A Practical Guidline for Implementing an ISMS in accordance with the International Standard ISO/IEC 27001:2013*. Berlin, Germany: ISACA Germany Chapter e.V., 2016.

[14] D.I. Sensuse, A. Syahrizal, F. Aditya, and M. Nazri, "Information Security Risk Management Planning of Digital Certificate Management Case Study: Balai Sertifikasi Elektronik," *Fifth International Conference on Informatics and Computing (ICIC)*, 2020, pp. 1-7.