JOURNAL OF DATA SCIENCE
eISSN:2805-5160
Vol.2022:16

Analysis of Information Security Resource Requirements in Local Governments

Toto Suharto[1], Aisyah Nuraeni[2], Awan Setiawan[3]

[1,2,3]Informatics, Langlangbuana University, Karapitan No 116, Bandung, West Java, Indonesia.

[*]**Email**: tsuharto@gmail.com

Abstract

Information Security Resources Needs Analysis and Management in Local Government is compiling the information security resource requirements by the Regional Government so the implementation of information security can guarantee the confidentiality, integrity, and availability of information. The lack of related research causes innovation and the fulfillment of information resource needs not to develop. Therefore, this study aims to carry out the local government's information security resources needs with a portrait adapted to existing conditions. In this study, the methodology used is Input-Process-Output and the objects of information security resources are asset security management, human resource management, and knowledge management which carry out city government affairs and must comply with applicable regulations and policies.

Keywords

Analysis, Information security, Resources, Local government

Introduction

In line with the need to provide fast, reliable, and safe public services, the use of information and communication technology (ICT) in the Public Service Provider environment continues to grow. The increasingly widespread use of ICT for public services by utilizing the internet can create vulnerabilities and threats to information security, thereby disrupting the performance of Public Service Providers. Therefore, information security becomes a major aspect that can maintain and secure CIA (confidentiality, integrity, and availability) information. CIA is an information security framework aiming to minimize risks (Ruo Yun, Andrew, Korryn, 2019).

Although cybersecurity is an important and complex issue that must be addressed by all levels of government, so far little research has been devoted to cybersecurity at the local level. (Choodakowska et al, 2022). The Government of Indonesia has accommodated the Implementation of Encryption for Information Security in Regional Governments, namely through the preparation of information security policies, management of information security resources, electronic system security and non-electronic information security, and the provision of information security services. In addition, the management of Information Security resources

Submission: 5 November 2022
Acceptance: 10 December 2022

carried out by regional apparatus consists of managing information and communication technology security assets, human resources management, and knowledge management (BSSN, 2019). Fulfilling the need for information security resources that are not effective causes the implementation of activities to not be carried out properly, and there may be waste or excessive workload on the units that must be responsible (Masombuka er al, 2021).

To manage information security resources in the local government environment, it is necessary to have the readiness and availability of information security policies, budget allocations, as well as an information security organization and human resources. Therefore, in this study, a study will be carried out to explore and evaluate the extent to which local governments are prepared to manage the information security resources needed.

Methodology

The approach used in the analysis and Management of Information Security Resources requirements is the Input-Process-Output (I-P-O) model. The input-Process-Output formulation is an aspect of system theory that states that a system converts inputs into outputs through a set of processes (Galais et al, 2020).

Figure 1. I-P-O Model

An explanation of the implementation of the IPO model is in the following table:

Table 1. I-P-O Model Description

Approach	Process	Description
1. Input	a. Survey Result	Data obtained from the results of data collection (survey or questionnaire)
	b. Existing Regulation	The laws and regulations concerning local government information security resources.
2. Process	a. Analysis of Existing Condition	Analysis of the existing condition of local government information security resources
	b. Regulatory Review	Reviewing the literature to build understanding
	c. Needs analysis	Define the information security resources needed to carry out information security activities in the future
3. Output	Document review of needs analysis and management of information security resources.	

Submission: 5 November 2022
Acceptance: 10 December 2022

Results and Discussion

Based on the I-P-O methodology, the results of this study consist of existing conditions, regulatory review, and analysis of information security needs in local government.

Existing Conditions of Information and Communication Technology Security Assets

ICT security assets have four categories that are used to identify, detect, protect, analyze, respond to and recover information security incidents in electronic systems. Existing conditions were obtained through the results of interviews conducted by units related to assets. The existing conditions are:

Table 2 ICT Security Asset Category

ICT Security Asset Category		Existing Condition
Encryption software	Computer programs and procedures designed to perform an information security service task or function	• Electronic Signature and Certificate • Antivirus • Firewall
Encryption Hardware	The main supporting devices and facilities in running the information security system	• Virtual Private Network • Secure Socket Layer • Transport Layer Security • Monitoring Camera
Encryption Communication Network Device	Device for connecting government via a telecommunications network	• Secure Email
Security Operation Center (SOC)	Units built to carry out security and encryption activities	• Partially implemented in each work unit

Existing Conditions Human Resource Information Security Section

Human Resources in the Information Security Sector needed in the implementation of information security are Pejabat Fungsional Sandiman and Manggala Informatika (PANRB, 2019). Based on the interview, the existing conditions are:

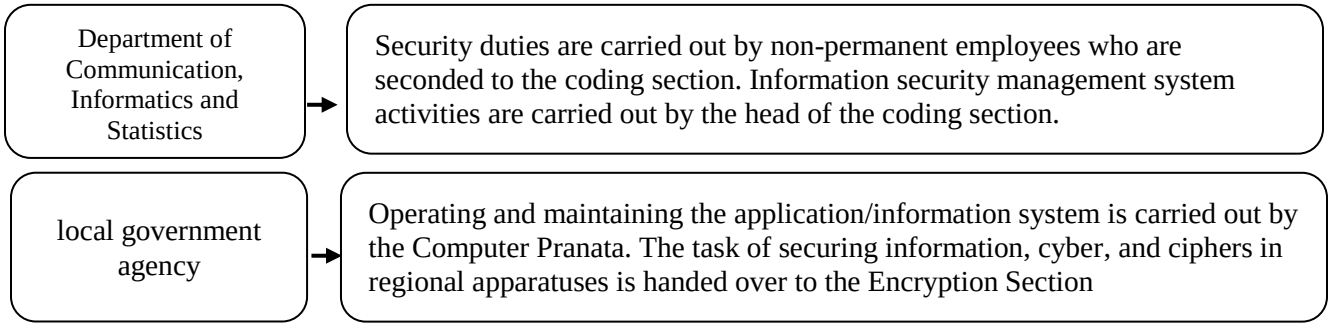

Figure 2. Existing Condition of Human Resource Information Security Section

Human resource management in the field of information security has not been fully implemented based on the preparation and determination of needs as stated in the Government

Submission: 5 November 2022
Acceptance: 10 December 2022

Regulation on the Management of Civil Servants and Government Regulations. The mechanism for competency development, career development, utilization, and provision of coding security allowances has not drafted both regulations and policies of the Office.

Existing Conditions Information Security Knowledge Management

Knowledge management is an effort to improve the organization's ability to manage intellectual assets and the quality of information security services. It supports the decision-making process through collecting, processing, storing, using, and transferring knowledge and technology produced in implementing government information security. (PANRB, 2011).
Based on the interview, all information security knowledge assets have not been managed in a knowledge management system.

ICT Security Asset Needs

ICT security assets need to be available to identify, detect, protect, analyze, respond to, or recover from information security incidents in electronic systems. These three requirements of ICT Security Assets are information security software, hardware, and communication network devices. ICT Security Asset Needs were obtained through the questionnaire conducted by units related to assets, the needs for ICT security assets are described in table 3, table 4, and table 5.

Table 3. Information Security Software Requirements Analysis

Requirements	Description
SIEM (Security Information and Event Management)	Centralized information systems collect real-time security information, from workstations, firewalls, servers, IPS, switches, and routers including information generated from applications.
IDS (Intrusion Detection System)	A method for detecting suspicious activity in a system or network. IDS can inspect inbound and outbound traffic in a system or network, perform analysis and look for evidence of attempted intrusion. IDS products that can be used: Cisco Secure Intrusion Detection System from Cisco Systems, eTrust Intrusion Detection from Computer Associates, Symantec Client Security from Symantec, Snort, etc.
IPS (Intrusion Prevention System)	Intrusion prevention software combines firewall and IDS functions so that it can perform detection and protection functions. Applicable IPS products: SolarWinds Security Event Manager, Splunk, etc.
Electronic Certificate	A certificate containing a signature and identity indicating the status of the legal subjects of the parties in an electronic transaction issued by the provider of the electronic certification.
Forensics tools	Devices for performing digital forensics. Forensics tools that can be used (1) Disk analysis: Autopsy (2) Image creation: FTK imager (3) Memory forensics: volatility (4) Windows registry analysis: Registry recon (5) Mobile forensics: Cellebrite UFED (6) Network analysis: Wireshark Pentest tools
Antivirus / Malware Analysis	Programs to prevent, detect and remove malware. Antivirus products that can be used: Kaspersky Total Security, McAfee Total Protection, Bit Defender Antivirus Plus, etc.

Submission: 5 November 2022
Acceptance: 10 December 2022

Nessus Vulnerability Scanner	Scanning software used to scan network system security and monitor network traffic RTIR (Request Tracker for Incident Response)
CACTI	Open-source software for web-based network monitoring, and graphics tools designed as a front-end application

Table 4. Hardware Requirements Analysis

Requirements	Description
Firewall	analyze packet headers and enforce policies based on protocol type, source or destination address, and source or destination port.
VPN (Virtual Private Network)	A private network connects one network to another by changing the connection path through the server and hiding the data exchange that occurs.
Network Access Control Systems	Solutions that support network visibility and access management through policy enforcement on network devices and users.
Device controls for USBs	Controlling the use of ports for connection purposes using USB.
Counter sensing device	Detects eavesdroppers that are in an active state. Counter-sensing devices that can be used: Broadband Field Strength Detectors, Harmonic Receivers, and Spectrum Analyzers.
Jamming device	Interfering with cellular frequency to cut communication
Monitoring camera	Cameras are used to monitor certain areas.

Table 5. Communication Network Device Requirements Analysis

Requirements	Description
Secure chatting	Chat communication securely by encrypting messages sent.
Secure phone device	Voice security in the form of end-to-end encryption for phone calls and mutual authentication of the calling party against man-in-the-middle attacks.
Secure email (email encrypt)	A highly secure email service, protecting emails from viruses, phishing, malware, trojans, and spam or man-in-the-middle attacks because emails are end-to-end encrypted.
Digital Signature	A signature consists of electronic information that is attached, associated, or linked to other information used for verification and authentication.
Electronic Certificate	A certificate containing a signature and identity indicating the status of the legal subjects of the parties in an electronic transaction issued by the provider of the electronic certification.

Table 6. Security Operation Center (SOC)/NOC Requirements Analysis

Requirements	Description
NOC	Network Operation Center (NOC) for data center

Submission: 5 November 2022
Acceptance: 10 December 2022

ICT Security Asset Management

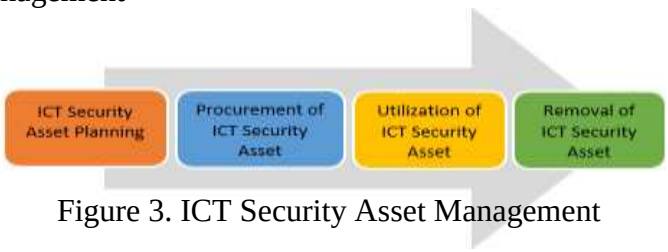

Figure 3. ICT Security Asset Management

ICT security asset management includes a series of processes as shown in Figure 3 (Bupati Bandung Barat, 2017)

Information Security Human Resource Requirements

Based on the questionnaire processing, the minimum qualifications of Human Resource in Information Security required are:

Department of Communication, Informatics, and Statistics

- Manggala Informatika Ahli Pertama
  - Familiar with Operational and requires basic level professional qualifications ranging from Penata Muda level III/a to Penata Muda Tingkat I level III/b.
- Sandiman for the expert category
  - Requires mastery of science, methodology, and analytical techniques.

Other local government agencies

- Sandiman for skill category
  - Requires mastery of technical knowledge and work procedures.

Human Resource Management in Information Security

Human Resource Management in the Information Security Sector is carried out concerning existing regulations, including a series of processes as shown in figure 4.

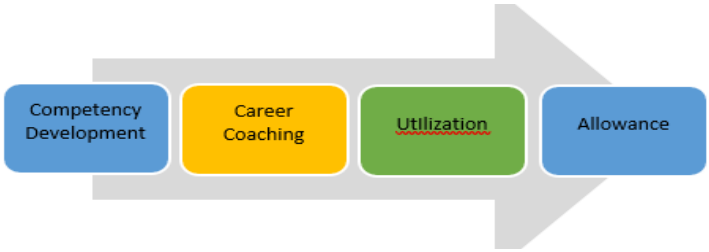

Figure 4. Human Resource Management in Information Security Sector

Information Security Knowledge Requirements

The condition of the availability of knowledge management to transfer information security knowledge. Based on the results of the questionnaire processing, the need for ICT security assets for the Local Government can be described in figure 5.

Submission: 5 November 2022
Acceptance: 10 December 2022

Figure 5. Information Security Knowledge

Management of Information Security Knowledge
Management Information Security Knowledge is carried out concerning existing regulations, including a series of processes as shown in Figure 6.

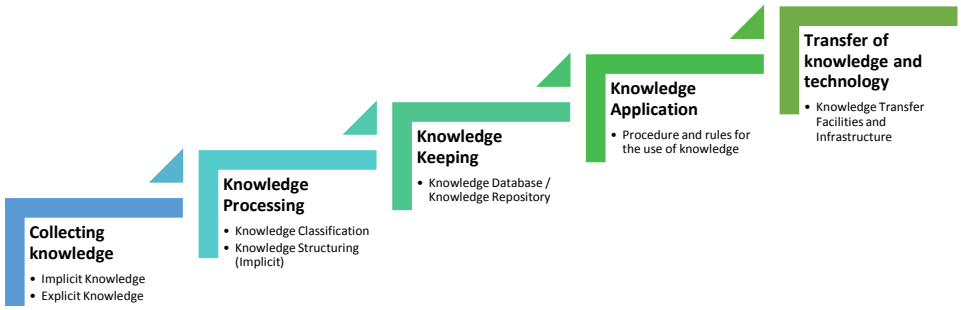

Figure 6. Management of Information Security Knowledge

Conclusion

The Analysis of information security resource needs in local government uses Input-Process-Output Methodology. In this study, the results obtained that the security requirements of ICT assets consist of eight information security software, seven hardware, five encryption communication network devices, Network Operation Center (NOC), and four management processes. The Human Resources needs consist of Manggala Informatika and Sandiman with four management processes. Meanwhile, the need for information security knowledge management consists of seven knowledge points and five management processes.

Acknowledgments

This work is funded by the Communication, Information, and Statistics Office in the West Bandung District of Indonesia.

References

BSSN, Regulation of BSSN Number 10, 2019 about Encoding Implementation for Information Security in Local Governments.

Bupati Bandung Barat, Regulation of West Bandung Regent, Number 18, 2017, about Technical Instructions for Regional Property Management.

Choodakowska, A., Kańduła, S., & Przybylska, J. (2022). Cybersecurity in the Local Government Sector in Poland: More Work Needs to be Done. Lex Localis - Journal of Local Self-Government, 20(1), 161–192. https://doi.org/10.4335/20.1.161-192(2022)

Submission: 5 November 2022
Acceptance: 10 December 2022

Galais, Carol & Martinez, Jose Luis & Font, Joan & Smith, Graham. (2020). Testing the input-process-output model of public participation. European Journal of Political Research. 60. 10.1111/1475-6765.12427.

Lee, S. (2014). Plasma Focus Radiative Model: Review of the Lee Model Code. *Journal of Fusion Energy, 33,* 319–335.

Masombuka, Mmalerato & Grobler, Marthie & Duvenage, Petrus. (2021). Cybersecurity and local government: Imperative, challenges and priorities. 20th European Conference on Cyber Warfare and Security (EWS).285-293. The UK. DOI: 10.34190/EWS.21.501

PANRB, Regulation of Ministry of Administrative and Bureaucratic Reform of the Republic of Indonesia Number 14, 2011 about Management Program Implementation Guidelines.

PANRB, Regulation of Ministry of Administrative and Bureaucratic Reform of the Republic of Indonesia Number 18, 2019 about Functional Sandiman.

Ruo Yun, Andrew, Korryn. (2019). No System Is Secure Using the CIA Triad to Prevent Catastrophe. *Rensselaer*.

Submission: 5 November 2022
Acceptance: 10 December 2022