DESIGNING AN INFORMATION SECURITY FRAMEWORK FOR THE INDONESIA WATER INDUSTRY SECTOR

Hidayatul Muttaqin, Kalamullah Ramli
Department of Electrical Engineering University Indonesia Depok, Indonesia
hidayatul.muttaqin11@office.ui.ac.id, Kalamullah.ramli@ui.ac.id

Abstract

The majority of Indonesia's water industry sectors have implemented smart water management systems as part of their business development, which has an indirect impact on enterprise information security. However, in general, water sector enterprises continue to place a low priority on information security, and the development of information system frameworks is based on generic norms employed by financial firms. There has been no research on information security frameworks especially built for water firms in Indonesia that use information security standards in the utilities sector. This article proposes a solution in the form of a new framework for Indonesian water firms that combines international information security requirements in the utilities sector with Indonesian government rules. This approach of development combines worldwide standards with national rules. The Cybersecurity Capability Maturity Model (C2M2) and ISO 27019 are two international standards commonly used by utility businesses globally. Government Regulation or Peraturan Pemerintah (PP) Number 71 of 2019 on the Implementation of Electronic Systems and Transactions is the relevant national regulation. The framework addresses information technology, telecommunications, and operational technology, with four approach categories: governance and ecosystem, protection, defense, and resilience. According to the research findings, the newly integrated framework can be applied and is worthy of recommendation. This framework also meets the standards for information security and can be used by Indonesian water corporations.

Keywords: smart water management system, information technology, operational technology, water sector, c2m2, ISO 27019, pp. 71/2019

Introduction

Water companies, like electricity, gas, and oil firms, are in the utility industry. Water firms in Indonesia have a long history, dating back to the colonial era and extending to the present day. [1]

Based on the conclusions of the United Nations Conference on Environment and Development (UNCED) in Brazil in 1992, known as the "UNICED Agenda 21," Chapter 18 underlined the importance of comprehensive and sustainable water management systems. [2] To reach this goal, water firms must use technology to improve their management procedures and make them more professional and transparent. The Smart Water Management System (SWMS) is one such technology that can increase the efficacy, efficiency, and quality of services offered by water corporations.

However, the use of this technology also has negative impacts, including the potential exposure of company information if users fail to comply with information security
regulations, the risk of information security threats due to non-compliant configurations, and the high risks associated with company information and data. An example of cyber threats in the water sector is observed in the United States. Due to the high number of threats, it became the third priority for the U.S. Department of Defense in 2015. [3] [4] According to a report by SCADAfence.com and Stefano Galelli's paper in 2020, the United States experiences the largest cyber incidents in the water sector each year. [5] Figure 1 in the SCADAfence.com report depicts various cybersecurity issues. The most recent cyberattack in Florida, U.S., in 2021 targeted the computer system of a water company, leading to a 100-fold increase in the concentration of additives, posing a threat to consumers. [6] Swift detection mechanisms applied through automated detection systems helped prevent this attack. [7]

Water firms must build an effective framework design that includes three essential mechanisms: predictive, preventative, and corrective actions to prevent the recurrence of cyber-attacks. [8] [9] According to the BSSN report, there is no particular data available on the number of assaults especially targeting water sector enterprises in Indonesia till 2022. However, the December 2022 report gives a breakdown of attacks by sector. [10] The government sector, particularly local government institutions, has seen the most cyberattacks. This highlights the need for water businesses being diligent in maintaining information security, as many are extensions of local government operations. Under Indonesian law, these expansions are classified as regional-owned enterprises, or BUMD (Badan Usaha Milik Daerah).

![Figure 1. List of cyber attacks](image)

In Indonesia, water businesses do not prioritize information security. Water firms' performance is evaluated in four areas, based on data from relevant ministries: financial, service, operational, and human resources. Water company performance reports for 2021 and 2022 analyzed 389 organizations, describing them as either healthy or struggling enterprises. [11][12] This means that the assessments prioritize the improvement of financial and operational circumstances for water businesses, which are designated as National Vital Objects (OVN) that provide public services. As a result, information system planning is frequently regarded as a supporting function rather than an enabler of the company's business activities. As a result, key performance indicators (KPIs) for information systems are limited to business-as-usual activities. If, on the other hand, information systems are considered as facilitators, this approach will motivate information systems to develop and supply value-added services to a greater variety of users and customers. Water corporations would be forced to develop more complete strategies, align goals, adhere to standards, and monitor progress using relevant frameworks as information systems become market driven. [13] This mental shift would encourage information systems to evolve and focus on information security, building a solid
framework to address any difficulties that may occur.

Until present, no research has been completed on the information security framework specifically developed for water firms in Indonesia. This is one of the reasons why, despite the existence of several key frameworks and derivative frameworks specifically designed for the utility sector with a broader scope (including IT and OT networks), water companies continue to use information security frameworks used by financial companies. These frameworks have been applied in several nations around the world, including Europe, the United States, Australia, and Singapore. ANSI/ISA-62443, NIST SP 800-82, the Cybersecurity Capability Maturity Model (C2M2), NERC Critical Infrastructure Protection (CIP), and ISO 27019 are some of these frameworks.

The management of information security is of critical relevance in this paper. By combining frameworks for information security system control management, cybersecurity management, and government regulations, the author develops methods for developing a framework for water firms in Indonesia. The primary goal is to control and defend all firm assets, protecting them from the ever-increasing information security dangers that Indonesia faces each year, and to develop a resilient information security system for the company.

**Literature Review**

A. Smart Water Management System (SWMS)

Since 2008, SWMS technology has been introduced, combining information technology (IT), telecommunications technology, and industrial control system (ICS) technology. IT technology includes the processing, delivery, and utilization of hardware or software for a company's core electronic transactions. IT technology, also known as enterprise technology, is ready-to-use and replaceable, with a normal lifespan of 3 to 5 years, and it typically runs on popular operating systems such as Windows, Linux, and Solaris. Storage devices, computing systems, infrastructure, and data centers and clouds are examples of IT systems.

The processing, delivery, and usage of hardware or software to manage and control industrial processes is referred to as ICS, often known as operational technology (OT). This technology, which is commonly used in the industrial or manufacturing sectors, is specifically built for use in long-term or multi-year operations, utilizing specialized protocols. Robotic devices, programmable logic controllers (PLCs), sensors, supervisory control and data acquisition (SCADA), and computer numerical control (CNC) are examples of such systems. [14][15][16]

Telecommunications technology facilitates the process of connecting sensor data in rural locations. This technology is not restricted to cellular technology but has recently grown to encompass Internet of Things (IoT) support networks such as the Low Power Wide Area Network (LPWAN). This network contains wireless networks used for specific purposes, such as machine-to-machine communication and IoT device connectivity. The ability of LPWAN to transport data with minimal power consumption and cost, as well as long-range wireless communication, is an advantage.

Water firms can benefit from the use of telecommunications technology in obtaining telemetry data from ICS or OT technologies. IT technology will process this telemetry data to generate new data that can be evaluated. Identifying leaks,
monitoring water flow (volume, pressure, and supply), monitoring the movement of water pump valves, geolocation needs, and other benefits are examples of the benefits of processed data.

SWMS technology also supports long-term and integrated IT technologies like AI, virtual reality, digital twins, and cloud services. Smart water metering has been implemented as an intelligent system platform in water companies in recent years, enabling automatic chemical treatment to monitor the usage of additive substances in water treatment, track and trace in smart logistics management, smart asset management, and virtual reality for monitoring the condition of water pipe networks based on geographic information systems (GIS).

Figure 2 shows a general overview of how water treatment procedures work. The water treatment procedure is separated into two stages: upstream and downstream. Water treatment is included in the upstream area, which begins with raw water received from rivers, reservoirs, or dams and is then transferred through huge pipes to the water treatment facility and reservoir. The downstream area includes water distribution, which starts with treated water kept in tanks and transferred to the population via distribution pipelines. This representation may appear straightforward, but when discussing the complete process from upstream to downstream, including how the corporation produces profit and oversees pipeline network improvements, it becomes extremely complex. Given this complication, digital technology is critical in streamlining company processes and achieving cost efficiency when compared to human approaches.

Figure 3. Information Technology

As illustrated in Figure 3, certain digital technologies that aid in the water treatment process can be classified into five categories:

1. The Customer Information System (CIS) manages customer-related issues such as checking water bill statements, monitoring water consumption or meter readings, account numbers, payment statuses, complaint management, customer
location coordinates, pipe leakage statuses, customer water sales, and fieldwork management. This system is critical to the company because it is directly related to revenue generation.

2. Various components of the production and distribution system include industrial control systems (ICS), leak detection systems, pipeline network modeling systems, water quality systems, illegal connection prevention systems, and others.

3. Earth mapping is used by the Geographic Information System (GIS) to map, evaluate, and record pertinent information based on specific needs.

4. The Monitoring System is a central monitoring system for ICS technologies such as ICS monitoring systems, pipeline monitoring systems, raw water monitoring systems, and others.

5. Systems that support key operations, such as enterprise resource planning (ERP), human resources information systems (HRIS), and other systems, are referred to as supporting information systems. The ERP system encompasses not just financial aspects but also procurement, logistics, asset management, and project management. The HRIS system focuses on the needs of water company personnel, while additional systems serve operational requirements beyond ERP and HRIS systems, such as information systems for legal documents, supplier management, and operational dashboards.

C. C2M2 Framework

The C2M2 Framework version 2.1 is a framework that firms can use to analyze the condition of their cybersecurity capabilities, with a specific focus on industrial technology, including IT and OT. Another goal is to help organizations assess their own information security maturity in three stages: preparation, self-evaluation, and follow-up activities. The US Department of Energy's Office of Cybersecurity, Energy Security, and Emergency Response (CESER) releases C2M2, with the most recent version in June 2022.

CESER embraces and integrates cutting-edge technology such as supply chain cybersecurity, artificial intelligence (AI), zero trust architecture, and ransomware defense in this current design. It also combines the most recent architectural trends, improves cybersecurity safeguards, enhanced control mechanisms, and best practices based on previous experiences. [17]

C2M2 includes an integrated framework that was upgraded in 2018 with the NIST Cybersecurity Framework (CSF). MIL 0 (not performed), MIL 1 (started), MIL 2 (performed), and MIL 3 (managed) continue to be used in the evaluation process for information security posture maturity and effectiveness. [18][19] The model domain, which consists of a total of ten domains, remains intact from earlier developments:

- Asset, Charge and Configuration Management
- Threat and Vulnerability Management
- Risk Management
- Identity and Access Management
- Situational Awareness
- Event and Incident Response, Continuity of Operations
- Third-party Risk Management
- Cybersecurity Architecture
- Cybersecurity Program Management

D. ISO 27019 Framework

The most recent edition is ISO 27019:2017. ISO 27019:2017 is a
management standard for information security that focuses on industrial utility process control systems for production, transmission, storage, and distribution. ISO 27019 covers the following topics:

- Control procedures whether centralized or dispersed, monitoring technologies, automation technologies, and operational systems.
- All supporting systems, such as data visualization systems for control, monitoring, recording, and reporting.
- All industrial digital controllers and automation devices, such as PLCs, sensors, and actuators.
- Process control communication technologies.
- Advanced Metering Infrastructure (AMI).
- Digitally enabled protection and safety devices.
- Distributed components.
- All software utilized in utility processes; and
- Remote maintenance systems.

ISO 27019:2017 still refers to ISO 27002:2013 in its development. Changes to ISO 27002:2022 are still being developed and have not yet been formally released.

E. Governance Regulation No. 71:2019

Government Regulation (GR) Number 71 of 2019 is a legal document issued by the government that governs the deployment of electronic systems and transactions (EST). It is an update to the preceding GR Number 82 from 2012. The initial rationale for these amendments was to fill the regulatory void left by the failure to enact the Personal Data Protection Law (PDP Law). However, it also encompasses adjustments to accommodate technology improvements and societal needs, such as data center placement, website or site authentication, electronic signatures, electronic certification authority, domain management, and other related issues.

Given the context described in the opening chapter of GR, GR Number 82 of 2012 is no longer in sync with the community’s evolving demands. The goal is to develop regulations in compliance with the terms of Law No. 19 of 2016, which updates Law No. 11 of 2008 and regulates electronic information and transactions.

Water supply businesses are classified as non-governmental state organizations with business capital provided by regional governments, also known as Regional Government-Owned Enterprises (BUMD) under Law Number 23 of 2014. BUMD is listed as a provider of public services in accordance with the state’s mandate in the explanation provided by Government Regulation (PP) Number 96 of 2012. As a result, compliance with Government Regulation Number 71 of 2019 is required when providing services utilizing electronic systems.

Experiment and Simulation

This study followed the step-by-step procedure known as “The Design Evaluation Method,” which Alan Hevner devised in 2004 [22]. The research is
organized into four phases in the figure above:

**Observational Phase**

Data and relevant references to the study problem are gathered during this phase. Papers from local and foreign sources pertaining to cybersecurity in the water supply sector, the C2M2 information security framework, and ISO 27019 are included in the data collection. Government data is also gathered from published reports and the 2019 Government Regulation Number 71. The data is gathered through case studies, field investigations on cyber-attacks around the world, and pertinent topics that drive this research.

**Analytical Phase**

This stage consists of data analysis and optimization. Prior to this, the obtained data is filtered, mapped, and compared using the categorization approach outlined in the ENISA literature [23].

**Governance dan Ecosystem**

The ability to address emerging risks with the help of the relevant ecosystem is critical in the governance process. The pattern of information security governance within a firm also relies on third-party compliance with the company's or organization's processes.

**Protection**

It is the process of putting preventive measures in place to ensure a secure environment in information security. Access and identification management, information security architecture and administration, physical security, and other related factors are all part of this process.

**Defense**

In information security, it is the practice of detecting and guarding against potential attack patterns. This approach focuses on discovering continuing conditions via data analysis. Effective defense communication should be carefully planned in order to improve the quality of incident response, reporting, and collaboration with professionals in this field.

**Resilience**

This category focuses on ensuring operational continuity even amid disasters and crises. The goal of this category is to reduce hazards to an organization's or company's continuous operations.

**Experimental Phase**

This phase involves creating a new framework based on the integration of the C2M2 Utility Framework, ISO 27019, and Government Regulation (PP) Number 71 of 2019. Classification, modeling, and the development of specific actions relevant to the strategy mentioned in section 3.2 are all part of the process.

**Testing & Descriptive Phase**

Through interviews and questionnaire surveys, the testing phase aims to evaluate the new framework's functional and structural elements. According to the book "Research Methods in Education, 5th Edition" by Cohen L. (2000), a minimum sample size of 30 people is recommended for research projects. This phase's descriptive approach involves providing a realistic portrayal of current situations, as well as arguments and recommendations for future improvements. The arguments presented are explanations based on the testing process's evaluation and serve as input for future improvements.

**Result and Analysis**

The observation and analysis processes provide data that is then used as input for the experimental phase. During the experimental phase, a new framework is created that incorporates all components of the three pertinent standards and regulations. The testing
Concerning the recommendation process, while 100% of respondents consider the framework is appropriate for recommendation, only 60% agree that all mandatory components should be implemented. 40% of respondents disagreed with the requirement to complete each aspect, suggesting the necessity for priority in its execution because not all aspects correspond with the business activities of the organization or company.

In terms of framework development, only 86.7% believe the framework should be developed. However, 13.3% disagree, citing the need to wait for the results of the framework's implementation in water firms. This research is critical in assessing whether the framework should be developed further or not.

![Figure 5. Results of the questionnaire & interview for the new framework](image)

**Conclusions**

Based on its compliance with government rules, the research concludes that this framework is suitable for implementation by both water and utility firms in Indonesia. The framework addresses a wide range of complicated issues that can be utilized to reduce risks in IT-OT networks and cyberattacks. The framework is suggested for adoption and development. Research and development are critical to improving its scope. Further study could include developing a way to
assess the usefulness of this paradigm in organizations. This is used to assess the framework's effectiveness and give success indicators, such as indicators of regulatory compliance in the company's business activities. Another example is measuring success indicators in relation to other supporting elements like employee behavior, process management, and so forth.

References


[12] Kementrian PU Direktorat Jendral Cipta Karya (Buku Indonesia Ministry of Public Works and People's Housing (Book: Kinerja BUMD Air Minum 2022)


[14] Cisco Article, Internet of Things,


[16] Water Critical Infrastructure and Its Dependencies, 2020, David Michael Birkett

[18] C2M2 Document version 2.1, Department of Energy, USA


[21] Indonesia Ministry of Communication and Information Article: Ada apa dengan PP Penyelenggaraan Sistem dan Transaksi Elektronik, kominfo.go.id
