VOL 4 (2020) NO 4

e-ISSN : 2549-9904
ISSN : 2549-9610

INTERNATIONAL JOURNAL ON INFORMATICS VISUALIZATION

Comparative Analysis and Design of Cybersecurity Maturity Assessment Methodology Using NIST CSF, COBIT, ISO/IEC 27002 and PCI DSS

Diah Sulistyowati[#], Fitri Handayani[*], Yohan Suryanto[#]

[#] *Universitas Indonesia, Depok, Indonesia*
E-mail:diah.sulistyowati@ui.ac.id, yohan.suryanto@ui.ac.id

** National Cyber and Crypto Agency, Depok, Indonesia*
E-mail: fitridupam@gmail.com

***Abstract*— Data or Information security in today's digital era is crucial in every organization that needs to pay attention. Management of organizational information is one of the components in realizing Good Corporate Governance. The measure of an adequate level of protection is an indicator of the cybersecurity awareness aspects of an organization's business processes in the short, medium, and long term, especially in the field that deals with information and communication technology (ICT). To make this happen, it requires a security standard that is appropriate and follows its needs to help organizations know the maturity level of cybersecurity in protecting its information security. The ABC organization is one of the Government agencies that manage the critical infrastructure and Indonesian digital economies. The organization has currently implemented several international security standards through its planning, implementation, evaluation document, and ICT activities. However, based on the national information security readiness assessment, information security management readiness results are still not optimal. In this study, an analysis of the NIST, ISO 27002, COBIT, and PCI DSS security standards has been carried out, which are ABC organizational security standards in managing ICT by assigned tasks and functions. Furthermore, the analysis result is used as materials for drafting a cybersecurity maturity framework through the four standard approaches that have become the basis for ICT management. The proposed concept of twenty-one integrated cybersecurity categories is expected to be a capital in measure ICT management performance in ABC organizations.**

***Keywords*— ICT; Cybersecurity Maturity; NIST; ISO 27002; COBIT; PCI DSS.**

I. INTRODUCTION

In the current digital transformation, cybercrime activity has become a form of crime that has grown and impacts the emergence of increasingly varied and relatively complex cyber incidents. Cybercriminals carry out some attacks in hacking/ stealing large amounts of data and money from companies around worldwide. Indonesia is one of the countries with a record of cybercrime cases, which in 2019 became the country with the highest malware attack rate in the Asia Pacific region. The potential economic losses in Indonesia resulting from cybersecurity incidents can reach the US $ 34.2 billion. This figure is equivalent to 3.7 percent of Indonesia's total Gross Domestic Product of US $ 932 billion. It is based that large-scale organizations in Indonesia may experience economic losses of US $ 16.3 million, 200 times greater than the average financial losses of a medium-scale organization [1]. Meanwhile, based on the annual report of the National Cyber and Crypto Agency (BSSN) in 2019, there were around 290 million cyberattacks identified, with the highest number of attacks being 137.4 million attempts to leak data, followed by 117.9 million trojan attacks, 12.5 million attacks on port 80 as well as 6.4 million attacks on name servers [2].

Cybersecurity is a part of information security that protects information assets from threats to information that is processed, stored, transmitted by interconnected information systems. Efforts to protect cybersecurity are to prevent, overcome and reduce the impact of damage or harm to the system [3]. To improve cybersecurity in Indonesia, one of the strategies that need to be formulated is preparing a cybersecurity maturity model that can measure an organization's cybersecurity capabilities and place its position on a scale appropriate to actual conditions. An Organization's cybersecurity maturity level becomes an indicator and evaluation material to improve or increase

compliance at a certain level as initiated by the Software Engineering Institute (SEI) with Mitre Corporation in November 1986. The development of a maturity framework process that has been prepared aims to improve existing software processes and other processes [4]. At present, there are various other international cybersecurity maturities framework standards such as NIST, ISO, COBIT, PCI DSS, and others referred to by other countries/organizations as controls in improving cybersecurity implementation of the ABC organization, which has also implemented them. This study aims to analyze the four standards used by the ABC organization and develop an integrated framework concept that can be used to improve performance in ICT management.

II. Literature Review & Method

A. *Maturity Cybersecurity Model*

Referring to Cybersecurity Capability Maturity Model (C2M2) Program that released by the Department of Energy (DOE) of the US (2019), the Maturity Model is a set of characteristics, indicators, or patterns representing capabilities and development in a particular science field. Maturity models can be prepared by adopting existing standards or combining several best practice standards. The cybersecurity maturity model will assist in providing direction for the Organization to undertake independent assessments. Implementing the maturity model will provide benchmarks that can help organizations evaluate improvement organizational aspects [5]. C2M2 is on adopting and managing cybersecurity practices related to information assets, information and operating technology, and the environments. Usability model is [6]:

1) Strengthening the organization's cybersecurity capabilities;
2) Allows organizations to consistently and effectively evaluate and measure cybersecurity capabilities;
3) Sharing knowledge, best practices, and relevant references across the organization;
4) Allows organizations to prioritize actions and investments to enhance cybersecurity.

C2M2 assists organizations to evaluate and identify areas of weakness and strength that can guide the development of a cybersecurity program. This cybersecurity maturity model can be a scalable tool for implementing the National Institute of Standards and Technology (NIST) Cybersecurity Framework.

B. *NIST*

Originally named the Bureau of Standards, NIST's goal was to ensure a consistent standard of size and function as laboratory standards. NIST was used extensively in the cybersecurity sector in the 1970s [7]. One of NIST's best practices for cybersecurity management, NIST Cybersecurity Framework (NIST CSF). NIST CSF components are more appropriate for technology organizations to use because of their scope of technical control, log analysis, and incidents (8). The latest update was published on April 16, 2018, through version 1.1. The current framework provides a comprehensive assessment consisting of three essential components, namely [7]:

1) *Core*

This component is divided into five risk management functions to provide a high-level overview of the organization's cybersecurity situation.

a) Identification: Development of complete knowledge about the cyber environment, particularly systems, assets, data, and capabilities.
b) Protect: Appropriate deployment and development to limit potential cybersecurity crash events.
c) Detection: Developing and implementing appropriate activities to identify cybersecurity events quickly.
d) Respond: Develop and implement appropriate activities to avoid the unwanted impact of cybersecurity events.
e) Recovery: Development and recovery activities to maintain resilience plans and restore capabilities that may be compromised by a cybersecurity incident.

These five functions are divided into 23 categories and 108 sub-categories, with each sub-category, is a list of external reference materials.

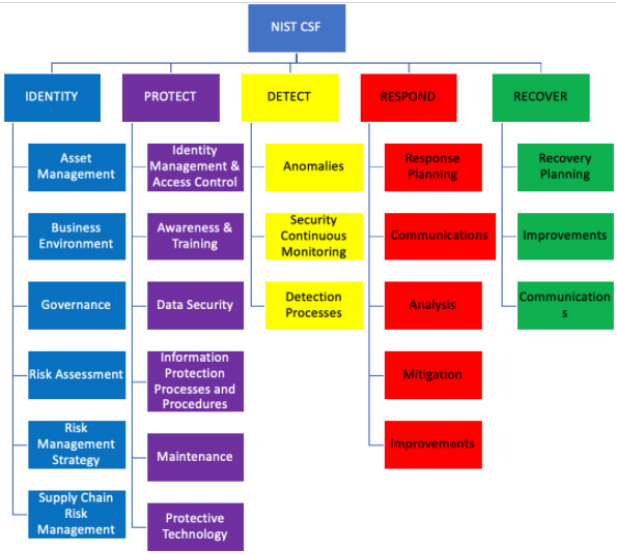

Fig. 1 Function and Category NIST CSF [6]

2) *Profile*

The framework profile represents the adjustments and priorities of activities and results for various industries and organizations according to their needs. Profiling is expected to increase cybersecurity readiness and help organizations analyse existing gaps. Furthermore, we can create a profile by looking for the categories/ subcategories most important to them from mapping.

3) *Implementation Level*

The implementation level is a feature that can help an organization measure where it is positioned within the framework: aware of risks and threats, recurring, and adaptable.

C. *ISO/IEC 27002*

The International Standards Organization (ISO) has adopted an information security management system from BS 7799 to ISO/IEC 27000. This system is a systematic approach to managing and controlling organizational information systems to maintain three main aspects, namely confidentiality, integrity, and availability of information. ISO/IEC 27002 is one of the derivatives of ISO/IEC 27000,

which serves as a guide to explain the implementation of information security implementation using controls to achieve the stated goals [9]. The structure of power presented covers all 11 security areas, as defined in ISO/IEC 27001. ISO/IEC 27002 does not require a particular form of control but leaves it up to the user to select and implement the right control according to their needs, taking into account the results of the risk assessment he has done [10]. Power from ISO 27002 2013 has 18 sections, according to Figure 2. The section contains 14 security control clauses, 35 security categories, and 114 controls, which are expected to assure information security by implementing these controls.

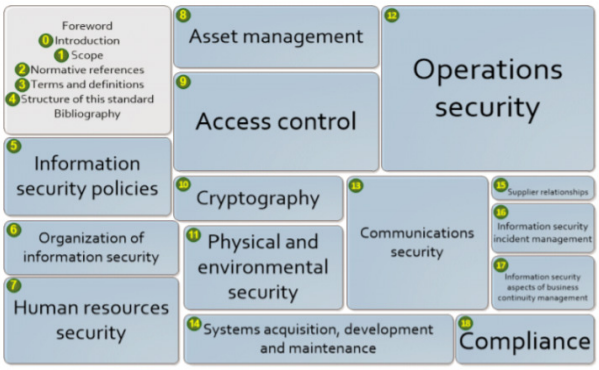

Fig. 2 Control Objective ISO 27002: 2013

D. COBIT

COBIT is a governance framework and information and technology management that is managed as a whole company. It contains the components and design factors for building and maintaining the governance system that the organization needs [11]. COBIT 5 was published in 2012, and to keep it relevant, 2019 saw an update to ensure more effective version control. Become the COBIT 2019 Framework: Governance and Management Objectives or also known as the COBIT 2019 Core Model. COBIT 2019 makes a clear distinction between management and governance processes in which it describes comprehensively 40 governance and management objectives. The 2019 COBIT product range is open-ended. The development of new guidelines, training, and resources to support the 2019 COBIT product range is continuously assessed based on market demand and managed through the ISACA product roadmap [9]. In COBIT 5, there are seven enablers as the main component to achieve governance objectives to create value from information technology. COBIT 2019 uses the same grouping consisting of one governance domain and four management domains. An environment main has a name with a verb that describes the primary purpose/ and the field of activity contained therein. COBIT 5, the division of 5 domains into the organization's IT processes into two main process areas, namely [12]:

1) Governance contains five governance processes determined by practice in each evaluation process, direct, and monitor (EDM).
2) Management, containing four domains, aligning with the area of responsibility of plan, build, run, and monitor, and provide a comprehensive IT scope from end-to-end, including:
   a) Align, Plan, and Organize (APO), including alignment, planning, and setting so that IT can contribute to achieving business goals,
   b) Build, Acquire, and Implement (BAI), including the process of building, acquiring, and implementing systems that support business processes,
   c) Delivery, Service, and Support (DSS), including delivering, service, support, or providing business process,
   d) Monitoring, Evaluation, and Assessment (MEA), includes monitoring, evaluating, and managing processes/ by independent monitoring agencies from both inside and outside the organization.

At COBIT 2019, there are seven enablers as components of governance.

Fig. 3 COBIT Component of a Governance System [12]

E. Payment Card Industry Data Security Standard (PCI DSS)

PCI DSS is a global data security standard on payment cards (credit, debit, ATM) for all entities that process, store, or transmit cardholder data and/or sensitive authentication data transmitted online [13]. The PCI DSS consists of technical and operational requirements that process payment transactions, software developers, application manufacturers, and devices used in these transactions to improve payment card account data security [14]. PCI DSS provides basic security requirements that can help businesses build security programs and determining what steps to take. There are three (3) steps to follow the PCI DSS standard:

1) Assess, identify card owner data, record Information Technology asset inventory along with the business process in processing payment cards, and analyze vulnerabilities that could potentially reveal cardholder data.
2) Remediate, make improvements to the identified vulnerabilities. In this case, by not storing unnecessary cardholder data and implementing a secure business process.
3) Report, perform the two-stage documentation above/ and send a corrective note. The next process is to send a compliance report to the bank concerned to secure the card used.

The PCI DSS certification requirements also cover third-party data centre facility providers as a means of storing or backing up cardholder customer data. PCI DSS issues more than 250 (two hundred and fifty) sub-requirements, which are grouped into 6 (six) objectives and 12 (twelve) main requirements to get certification that an organization has implemented the PCI DSS security standard [15].

F. Research Methodology

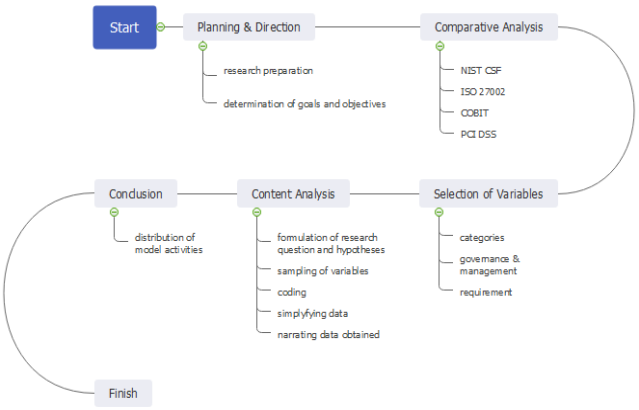

Fig. 4 Stage of Research

III. Analysis and Result

A. Comparison Analysis

The following comparisons analysis have been made:

TABLE I.
COMPARISON OF THE FOUR FRAMEWORKS

Features / Model	Focus Area	Functions/ Objectives	Categories and subcategories
NIST CSF	1. cybersecurity standards and risk management 2. check level implementation and deployment	1. Identification 2. Protect 3. Detection 4. Respond 5. Recovery	consist of 23 categories and 108 subcategories
ISO/IEC 27002	Standards and procedures related to information security and control	1. Application of an Information Security Management System based on ISO/IEC 27001; 2. Developing new management information	14 security control clauses consist of: 1. Information security policies 2.Organization of information security, 3.Human resources security 4.Asset management 5.Access control 6.Cryptography 7. Physical and Environmental security. 8.Operation Security 9.Communications security 10.System acquisition, development & maintenance 11.Supplier relationships 12.Information Security incident management 13.Information security aspect of business continuity management 14. Compliance
COBIT	Auditing of procedure to information security and control	1. One governance domain are grouped in the EDM 2. Four management domains: APO, BAI, DSS, MEA	There are 40 governance and management objectives
PCI DSS	Identification of weaknesses in Web site security processes, procedures and configurations	1. Maintaining a Secure Network and Systems 2. Protection of Cardholder Data 3. Maintain a Vulnerability Management Program 4. Implement Strong Access Control Measures 5. Perform and Network Test Regularly 6. Maintain an Information Security Policy	Consist of 12 requirements with over 300 sub-requirements

The next analysis process is to do the coding process, based on table II the variables used as the basis for drafting the framework integration concept are to use each framework's categories. Each variety of the four frameworks is codified with the provision that A is the category code for the NIST model, B is the ISO 27002 model code, C is the COBIT model category code, and D is the PCI DSS model. The following is an example of coding in the ID column in the following table:

TABLE II.
CODIFICATION FRAMEWORK PROCESS

No	Model/Categories	ID
	NIST	
1	Asset Management	A1
2	Business Environment	A2
3	Governance	A3
	ISO 27002	
1	Information Security Policies	B1
2	Organization of information security	B2
3	Human resources security	B3
	COBIT	
1	Ensured Governance Framework Setting and Maintenance	C1
2	Ensured Benefits Delivery	C2
3	Ensured Risk Optimizations	C3
	PCI DSS	
1	Install and maintain a firewall configuration to protect cardholder data	D1
2	Do not use vendor-supplied defaults for system passwords and other security parameters	D2
3	Protect stored cardholder data	D3

The next step is to analysing the categories of each framework, referring to the table II results then one of the necessary frameworks used is the NIST model, is by seeing that the framework has the same business process as the ABC Organization, so the next step is to conduct content analysis. The meaning contained in the activities of each category is generated with the following examples.

TABLE III.
FRAMEWORK CATEGORIES

No	Categories	ID A	ID B	ID C
1	Asset Management	A1	B4	C4, C28
2	Risk Assessment	A4	B13	C3, C33

In the table above, it can be interpreted that the A1 category in the NIST model has the same meaning/content as the category for B4 on the ISO 27002 model and on C4, C28 in the COBIT model. Then in the A4 category, the NIST model has the same meaning/content with the category B13 on the ISO 27002 model and in C3, C33 on the COBIT model. So that the results of the mapping of all categories are as follows:

TABLE IV.
THE RESULT CONTENT ANALYSIS FRAMEWORK

No	Categories	ID A	ID B	ID C	ID D
1	Asset Management	A1	B4	C4, C28	
2	Business Environment	A2	B8	C5, C7, C24, C31, C37	
3	Governance	A3	B1	C1, C2, C9, C40	D12
4	Risk Assessment	A4	B13	C3, C33	
5	Risk Management Strategy	A5		C17, C36	
6	Supply Chain Risk Management	A6		C15, C22, C26, C30	
7	Identify Management and Access Control	A7	B5, B7	C8, C10, C18	D7, D8, D9, D10
8	Awareness and Training	A8	B2	C27	
9	Data Security	A9	B6	C11, C19, C20, C23	D3
10	Information Protection Processes & Procedures	A10	B3	C6, C12, C16, C25, C29, C32, C34	D1, D2, D5
11	Maintenance	A11	B10	C35	D6
12	Protective Technology	A12	B14	C14, C21, C39	D4
13	Anomalies and Events	A13			
14	Security Continuous Monitoring	A14			
15	Detection Processes	A15			D11
16	Response Planning	A16			
17	Communications	A17, A23	B9, B11, B12	C13, C38	
18	Analysis	A18			
19	Mitigations	A19			
20	Improvement	A20, A22			
21	Recovery Planning	A21			
Categories Total		**23**	**14**	**40**	**12**

A. *Result Design Proposed.*

The following concepts generate categories of distribution frameworks, and an explanation of each type is generated from combination of NIST CSF, ISO 27002, COBIT and PCI DSS

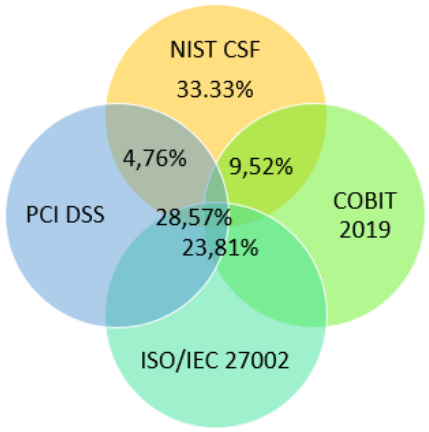

Fig. 5 Activity Distribution Framework

TABLE V.
CYBERSECURITY MATURITY CATEGORY DESCRIPTION

No	Categories	Description
1	Asset Management	Management identifies organizational assets, including optimal personnel, data, devices, systems, and facilities to achieve organizational goals and are part of its risk strategy.
2	Business Environment	A series of strengths that affect the organization's business in the form of mission, objectives, stakeholders, and its activities ranging from the aspects of strategy setting, performance management, and monitoring of its suitability to be subsequently used in the direction of shared roles, responsibilities, and cybersecurity risk management.
3	Governance	The stages in organizational decision making by considering a set of policies, procedures, and processes used to manage and monitor regulatory, legal, risk, environmental, operational, and organizational renewal requirements to be understood and informed on the scope of cybersecurity risk management.
4	Risk Assessment	Management of the organization's business continuity through cybersecurity risk management, which includes mission, functions, assets, both personnel and infrastructure, business processes, and reputation
5	Risk Management Strategy	Determination and management of priority scales, constraints, risk tolerance, and organizational assumptions are then used to support operational risk decision making.
6	Supply Chain Risk Management	Determination of priority scales, constraints, risk tolerance, and organizational assumptions is then used to support risk-making decisions by going through the supply chain risk management process.
7	Identify Management and Access Control	The management stages of identification and restriction and monitoring of access to physical and logical assets and facilities for legitimate users, processes, and devices are following the

No	Categories	Description
		assessed risks of unauthorized access to permitted activities and transactions.
8	Awareness and Training	Management of organizational information security knowledge through personnel and partners provided cybersecurity awareness education and training in carrying out cybersecurity-related duties and responsibilities consistently through established policies, procedures, and agreements.
9	Data Security	Management of the Information and technology framework following the organization's risk strategy in protecting the confidentiality, integrity, and availability of information.
10	Information Protection Processes & Procedures	The process of maintaining the scope of resource management and procedures to protect information systems and organizational assets
11	Maintenance	Maintenance, development, and repair of industrial information and control system components are carried out following policies and procedures to ensure security.
12	Protective Technology	"Efforts to ensure the security and resilience of systems and assets, through technical security management are carried out by related policies, procedures, and agreements.
13	Anomalies and Events	The process of detecting anomalies and the potential impact of an incident / determining an early warning system of an event that is likely to occur
14	Security Continuous Monitoring	Monitoring implementation information systems and assets to identify cybersecurity vulnerabilities and verify and take effective action as a form of protection.
15	Detection Processes	Maintenance of the detection process and the implementation of periodic testing to detect abnormal events.
16	Response Planning	The planning stages of maintenance of processes and procedures to ensure the response to a detected cybersecurity incident.
17	Communications	A form of coordination activity for both internal and external stakeholders to maintain and manage incident management.
18	Analysis	The analysis process is undertaken to ensure an effective response in support of recovery activities.
19	Mitigations	A series of activities carried out to prevent, reduce their effects, and resolve incidents.
20	Improvement	Efforts to improve from the learning process in the period obtained from current and previous detection/response activities to improve in the future period
21	Recovery Planning	A rational recovery planning process to ensure the recovery of systems or assets due to cybersecurity incidents.

IV. CONCLUSIONS

Based on the content analysis carried out on the four NIST frameworks, ISO 27002, COBIT, and PCI DSS, a new framework is formed that can be used by ABC organizations in measuring the maturity level of its cybersecurity. The framework consists of 21 categories that can be the basis for mapping the improvement of ABC's organizational maturity capabilities. In further research, a validation process can be carried out against the framework that has been produced. Besides, subcategory mapping can also be done to obtain a more comprehensive conceptual framework.

REFERENCES

[1] The World Bank Group, "World Bank's Asia Pacific GDP Information", 2020, available: https://data.worldbank.org/indicator/NY.GDP.MKTP.CD

[2] Pusat Operasi Keamanan Siber Nasional, Badan Siber dan Sandi Negara, Annual Report January-Desember 2019, Indonesia Cyber Security Monitoring Report

[3] Straub Jeremy. 2020, "Software Engineering: The First Line of Defense for Cybersecurity", IEEE 11th International Conference on Software Engineering and Service Science (ICSESS)

[4] Mohammed Idi and Musa Bade Aliyu, 2019 "Cybersecurity Capability Maturity Model For Network System", International Journal of Development Research

[5] rivas G., et all. 2020, "A NIS Directive compliant Cybersecurity Maturity Assessment Framework", IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC)

[6] Putra Adyan P.G. et all, 2020, "Maturity Assessment of Cyber Security in The Workforce Management Domain: A Case Study in Bank Indonesia", International Conference on Information Technology Systems and Innovation (ICITSI)

[7] Overview Of The Nist Cybersecurity Framework, May 2018, available: (https://1path2020b.websitetotalcare.com/blog/overview-of-the-nist-cybersecurity-framework

[8] Roy P Prameet, "A High-Level Comparison between the NIST Cyber Security Framework and the ISO 27001 Information Security Standard", IEEE, 2020

[9] Motii Malik, Semma Alami. 2017, "Towards a new approach to pooling COBIT 5 and ITIL V3 with ISO/IEC 27002 for better use of ITG in the Moroccan parliament", International Journal of Computer Science Issues, Volume 14, Issue 3

[10] Jufri Mt., Hendayun M., Suharto T. 2017, "Risk-assessment based academic information System security policy using octave Allegro and ISO 27002", Second International Conference on Informatics and Computing (ICIC)

[11] Rizal A.A., Sarno R., Sungkono K.R. 2020, "COBIT 5 for Analysing Information Technology Governance Maturity Level on Masterplan E-Government", International Seminar on Application for Technology of Information and Communication (iSemantic)

[12] ISACA, COBIT 2019 Framework: Governance and Management Objectives, ISACA, 2019

[13] Dupuis M., Bejan C., Bishop M., David S. 2019, Lagesse B, "Design Patterns for Compensating Controls for Securing Financial Session", IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation

[14] Elluri L., Nagar A., Joshi K.P. 2018 "An Integrated Knowledge Graph to Automate GDPR and PCI DSS Compliance", IEEE International Conference on Big Data (Big Data)

[15] PCI DSS Quick Reference Guide, Understanding the Payment Card Industry Data Security Standard version 3.2.1, 2018 available: https://www.pcisecuritystandards.org/documents/PCI_DSS-QRG-v3_2_1.pdf.