ISSN 2278-3091

Volume 9, No.3, May - June 2020

International Journal of Advanced Trends in Computer Science and Engineering

Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse157932020.pdf

https://doi.org/10.30534/ijatcse/2020/157932020

Integration of ITIL V3, ISO 20000 & ISO 27001:2013forIT Services and Security Management System

Barra Al Faruq, Hemdani Rahendra Herlianto, SiharParulian Hendrik Simbolon, Ditdit Nugeraha Utama, Antoni Wibowo

ComputerScience Department, BINUS Graduate Program - Master of Computer Science, Bina Nusantara University, Jakarta, Indonesia 11480; barra.faruq@binus.ac.id, hemdani.herlianto@binus.ac.id,sihar.simbolon@binus.ac.id, ditdit.utama@binus.edu, anwibowo@binus.edu

ABSTRACT

IT organizations are responsible for delivering good IT services and maintaining IT security to improve their competitive advantage Both IT security and IT services have their own international standard and framework. When the IT service management system (SMS) and an information security management system (ISMS) are implemented separately, it can lead to consuming high resources and costly. This paper is going to focus on the integration of ISO 20001 as SMS standard, ITIL v3 as the framework, and ISO 27001 as ISMS standard. We are going to discuss how the ITIL V3 can be combined with ISO 20001 and ISO 27001 by scientifically matching the similarities of process, procedure, and resources. This paper contributes to providing a guideline for an IT organization that is going to implement SMS and ISMS standard and framework. In the Appendix section 4, we also provide a table of process, procedures, and resources similarities. Therefore, the organization can use the combined processes in order to reduce the cost of implementing those standards.

Key words: ISO 2000, ISO 27001, and ITIL

1. INTRODUCTION

A company or organization is driven to achieve its vision and mission. Therefore, the management team needs to ensure business sustainability by implementing good corporate governance. Corporate governance consists of two dimensions; conformance and performance [1]. Corporate conformance focuses on complying with laws, internal policies, audit requirements, etc. While corporate performance specifically related to increasing profitability, efficiency, effectiveness, growth, etc. In this case, the leadership board must carry out and adjust the system at the same time. Unsuitable performance and performance without conformance are going to affect the entire company. The Committee of sponsoring organizations (COSO) is one of the conformance management frameworks that can be adopted by organizations to evaluate internal controls [2]. There are several qualified tools that can be adopted to help the board to get effective corporate performance and conformance.

According to achieve good corporate governance, an IT organization or department, as a part of the company, need to implement an IT governance framework[3]. One of the frameworks is the control objectives for information technologies (COBIT). COBIT is an internationally recognized IT Management control framework developed by the ISACA that can assist IT Organization to develop, organize, and execute strategies for IT governance[4][5]. COBIT is operated to measure IT Governance by maturity level. A higher level of maturity in COBIT can be described as achieving a higher maturity level of IT organization and maintaining the continuity of IT governance. In implementing IT service management, the IT department can adopt the best practice for processes and procedures. One well-known framework is information technology infrastructure library (ITIL); where ITIL V3 consists of five stages: service strategy, service design, service transition, service operations, and sustainable service improvement [6].

To improve credibility and reputation, several IT organizations are implementing necessary standards or best practices as part of the IT governance[7]. Some commonly used standards are ISO 20000 (service management system / SMS), ISO 9001 (quality management system), and ISO 27001 for information security. The ISO standards and ITIL are complemented each other. ITIL is having a common objective with ISO 20000 (SMS). As shown in Figure 1 is an example of the relationship between corporate and IT governance structure[8].IT organizations that adopt these standards and international certification granted will gain more benefits like improved customer and business partner confidence and satisfaction.

From Figure 1, there are some challenges to align and integrate several best practices or standards that are needed in IT governance; as each standard has its own focus, and there are no standards that can answer all aspects from end-to-end. When IT organizations adopted several standards and build a couple of teams to work in it, then it will require considerable external and internal resources [9]. The implementation of several best practices has the potential to lead to overlapping and recurring business processes. And management needs assurance that governance has been carried out well and measurably by internal or external parties (certification bodies). As shown in figure 1 is an example of the Relationship of Corporate & IT Governance Structure[4].

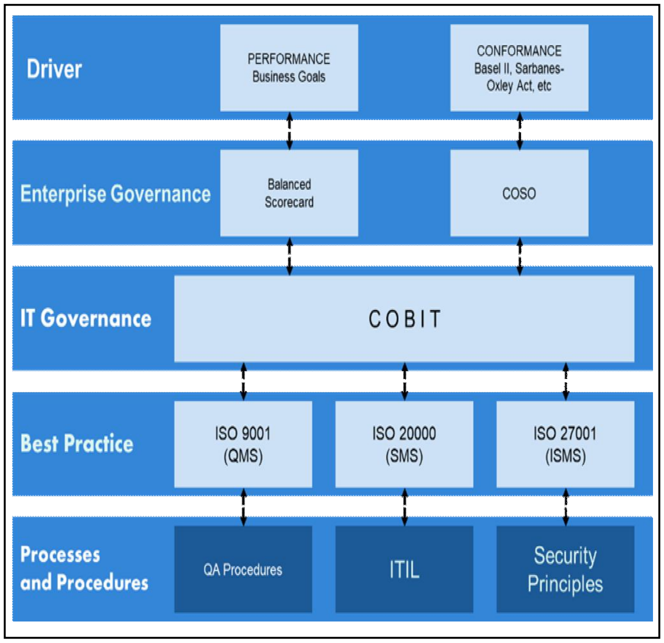

Figure 1: Relationship of Corporate and IT Governance Structure[4]

Companies that implement ISO 20000 as a standard of SMS and ISO 27001 for the information security management system (ISMS), potentially face the four challenges above. The objective of this paper is to propose an integration of ISO 20000, ISO 27001, and ITIL implementations to reduce redundancy and repeated processes.

2. RELATED WORK

The paper proposed improvements to IT governance and evaluate ongoing services accurate improvement using the fuzzy and ITIL framework. The use of the fuzzy ITIL approach model has been found, there searchers could identify the maturity level of continuous service improvement [10].

3. SERVICE AND SECURITY MANAGEMENT SYSTEM

3.1 ISO 27001:2013

ISO / IEC 27001: 2013 is an international standard on ISMS. This standard can help to keep consumer data safe in government departments and in the private's sector. ISO / IEC 27001: 2013 explains the condition to guide information security management by those who are responsible for maintaining security in the organization. SMS is part of a management system based on a business risk approach to manage, implement, operate, monitor, observe, and maintain and improve information security in organizations [11].

ISO 27001: 2013 is a standard document for ISMS. ISMS can provide a general picture of what should be done by a company. In their efforts to implement security concepts information in the company. In general, there are eleven aspects of the usually referred to as control, which must exist in every company its efforts to implement the concept of information security. Control, in this case, is things, can be processes, procedures, policies, and tools that are used as tools prevention of the occurrence of something that is not desired by existence the concept of information security, such as prohibited access to data or confidential company information.

It is the control of company data security. Some of the elements that cover this are security policy, information security organization, asset management, human resource security, physical and environmental security, communication and operations management, access control, procurement, development, and maintenance of information systems, incident information security management, management business continuity and compliance with applicable procedures.

Information security management system standard ISO / IEC 27001. This standard is the result of the revision and transfer of BS 7799-2, which was published by the British Standard Institute in 2002 which was launched for use in conjunction with ISO / IEC 27002. ISO / IEC 27001 is a standard document ISMS, which provides an overview of what companies should do in their efforts to improve, implement and improve information security in companies based on "best practices" in information security.

ISO 27001 2013 was introduced on September 25, 2013 by the international organization for standardization (ISO) and some said it was released in October 2013 [8]. The introduction of ISO 27001: 2013 will officially replace ISO 27001: 2005. Implementation for organizations that have just implemented ISO 27001 was in October 2014 and those who implemented the 2005 deadline to make changes after the introduction of ISO 27001: 2013 (+ / - October 1, 2015) ISO / IEC 27001 requires management to examine organizational information security issues, consider threats, discussions (vulnerabilities), and their effects systematically.

Management systems also require designing and implementing the protection of available information and/or arrangements for other problems that are considered unacceptable. In addition, another management requirement is to adopt a management process that complements information security and continues to meet the organization's information security needs.

The ISO 27001: 2013 standard was developed more synchronously with other ISO versions (e.g. ISO 9001, 20000, 31000). So that there will be an ISO-based management system standard. Changes are quite visible, compared to changes in ISO 9001: 2000 to ISO 9001: 2008. If the article (the number or structure/structure) of the change in ISO 9001 does not change, there are only additional words in some articles, this is very different from ISO 27001, in the article (both from the number and order/structure) changes to a lot and at the annex also experienced a change in number. The field of risk assessment also changes [12].

3.2 ISO 20000:2018

BS 15000 is a precursor of ISO 20000. It was developed to give thebest practice guidelines, which resulted in the ITIL. ITIL provides guidance to users of adequate IT services to help their business process[13].

British Standard Institution (BSI) organizations are the ISO 20000 standard initiatives. Two models are based on ITIL principles and enable IT organizations to have IT services management certified. ISO 20000 promotes "adoption of an integrated process approach to effectively provide managed services to meet business and customer requirements". ISO 20000 does not specify that the requirements must be met following ITIL recommendations so that many ways can be achieved for compliance. ITIL is the most widely used approach to get an ISO 20000 certificate [13].

ISO 20000-1 is the latest version of an IT SMS that applies to all information technology service providers (internal or external) and organizations depending on the information technology business, or simply wants to improve IT SMS[14].

ISO 20000-2 is a code of practice for describing best practices in the service management process within the scope of ISO 20000-1. It is useful for organizations and prepares ISO 20000-1 audits or planning service improvements.

3.3 Information Technology Infrastructure Library (ITIL)

ITIL is a de-facto standard introduced and distributed by government trade offices (OGC) in the UK. The ITIL approach is the most accepted for IT service management. ITIL has a structure of repetitive, multidimensional, and life cycle forms. in addition, ITIL has an integrated approach as required by the ISO / IEC 20000 standard[18].

ITIL has several services that can manage ITIL so that ITIL can run well. Existing services in ITIL include continuous service improvement, service design, service operations, services transition, and services trategy.

a) Service Strategy

The ITIL service strategy is guidance about designing, developing, and implementing service management from the perspective of organizational capabilities and strategic assets. The service strategy serves to understand who IT customers are, what need to be offered to meet customer needs, the system capabilities and IT resource needed to develop service, and the requirements for implementing them successfully.

Examples of service strategies include strategies in the form of financial management. This strategy is designed for IT services that aim to manage the requirements for budgeting, accounting, and charging service providers. Figure 2 represents structure, hierarchy, order, or level of authority[15][16][17].The following is a picture of the services management strategy in Figure 2 shows an overview of the ISO / IEC 20000 document[24].

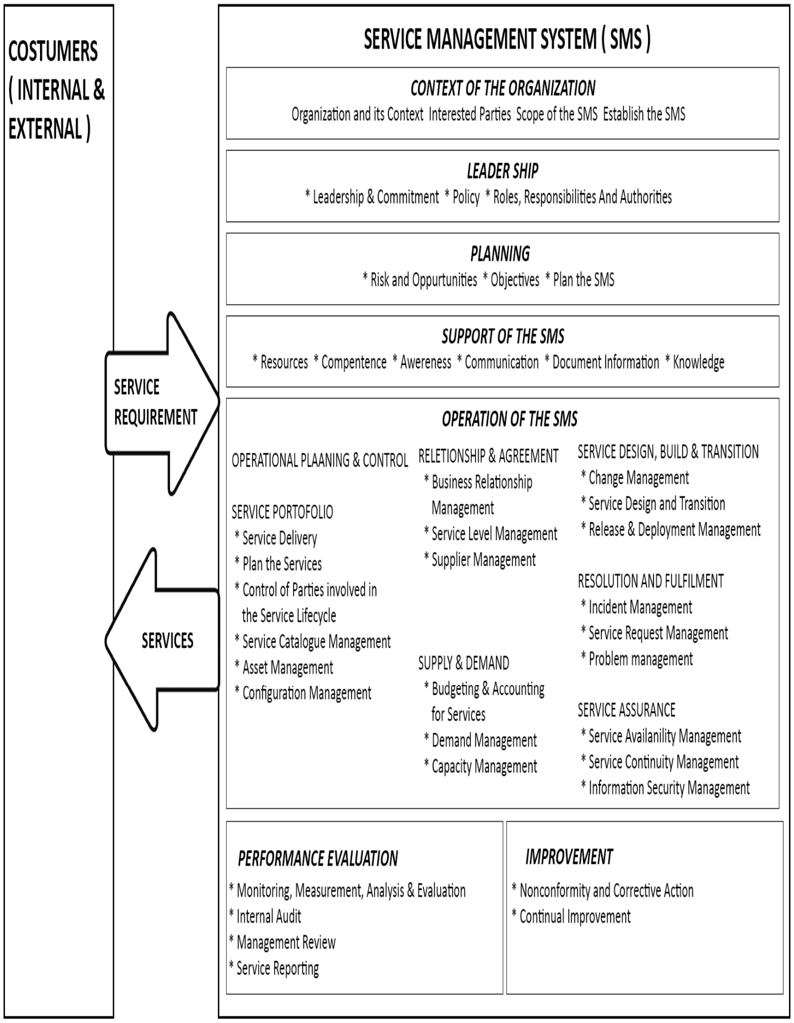
COSTUMERS (INTERNAL & EXTERNAL)
SERVICE REQUIREMENT
SERVICES
SERVICE MANAGEMENT SYSTEM (SMS)
CONTEXT OF THE ORGANIZATION
Organization and its Context Interested Parties Scope of the SMS Establish the SMS
LEADER SHIP
* Leadership & Commitment * Policy * Roles, Responsibilities And Authorities
PLANNING
* Risk and Oppurtunities * Objectives * Plan the SMS
SUPPORT OF THE SMS
* Resources * Compentence * Awereness * Communication * Document Information * Knowledge
OPERATION OF THE SMS
OPERATIONAL PLAANING & CONTROL
SERVICE PORTOFOLIO
* Service Delivery
* Plan the Services
* Control of Parties involved in the Service Lifecycle
* Service Catalogue Management
* Asset Management
* Configuration Management
RELETIONSHIP & AGREEMENT
* Business Relationship Management
* Service Level Management
* Supplier Management
SUPPLY & DEMAND
* Budgeting & Accounting for Services
* Demand Management
* Capacity Management
SERVICE DESIGN, BUILD & TRANSITION
* Change Management
* Service Design and Transition
* Release & Deployment Management
RESOLUTION AND FULFILMENT
* Incident Management
* Service Request Management
* Problem management
SERVICE ASSURANCE
* Service Availanility Management
* Service Continuity Management
* Information Security Management
PERFORMANCE EVALUATION
* Monitoring, Measurement, Analysis & Evaluation
* Internal Audit
* Management Review
* Service Reporting
IMPROVEMENT
* Nonconformity and Corrective Action
* Continual Improvement

Figure 2: Service Management System ISO 20000:2018[24].

In Figure 2 it is explained that it takes several people who can be involved in texting. like leadership whose job is to lead and commit to the company. leadership also has responsibility for policy, company knowledge, and responsibility.

In addition, SMS must also be supported so that SMS can work like a competent human being, the human who is aware, good communication, and good knowledge. SMS is also supported by operational SMS such as operational planning control, portfolio services, relationship and agreement, service design, build, and transition, supply, demand, and there should be an evaluation and improvement to run this SMS.

b) Service Design

The Service Design Module (SD) is a certification for ITIL® Services. The design of IT services includes architecture, processes, policies, and documentation. This design allows a company to design services that can help the needs of the organization. The design process isused in continuous improvement and service development in the IT lifecycle. This design is needed to develop, manage, and integrate service design into the IT services management process. A good design process can produce good services that can improve IT alignment with the overall business and user needs and certification will illustrate the importance of designing consistent service design practices to achieve this[19].

c) Service Transition

IT service transitions are guidelines for implementing and providing services for the transition or temporary suspension of IT services. In the IT service transition, there are seven processes such as change management, change evaluation, release and deployment management, service validation and testing, knowledge management, and transition planning and support.

Through the transition phase the service can move and enable business customers to achieve the desired value. in the Transition can manage changes in control of assets and configuration items (basic components such as hardware, software, etc.) that associated with new and modified systems such as service validation and testing and transition plans to ensure that users, support personnel and the production environment are well prepared to release to production.

d) Service Operation

Service Operation is a lifecycle stage that covers all daily operational activities in managing IT services. Service operation aims to carry out activities related to information technology operations. Inside there are various guidelines on how to manage IT services efficiently and effectively and guarantee the level of performance that has been agreed with the previous customer.

e) Continual Service Improvement

The following main process is part of the ITIL (CSI) continuous service improvement phase in the form of service reviews that regularly review business services and infrastructure services. The purpose of this process is to improve service quality and identify more economical ways to provide services. The CSI works is by evaluating processes regularly and identifying areas where the targeted process metrics have not been achieved, and conducting, benchmarking, auditing, maturity assessments, and periodic reviews. CSI's initiative to determine specific initiatives aimed at improving services and processes, based on the results of service reviews and process evaluations. The results of initiatives are internal initiatives undertaken by service providers or initiatives that require customer collaboration.

4. PROPOSED METHOD

Since 2012 ISO updated their outline of high-level structure for all new and revised management system standards, so there will be some integration between ISO standards. The common structure as shown in Appendix 1. The purpose of our analysis in this research is to review the standards related to ISO / IEC 20000 & ISO / IEC 27001 and their relationship with ITIL V3 as shown in appendix 2 and 3. The method that we used to find the relation between ISO / IEC 20000 and ISO / IEC 27001: 2013 is checklist 20000 & ISO / IEC 27001: 2013 standards will be used as basic analysis. From the first two standards we will review it and find the linkage in description assessment (data collection based on documents) and field assessment (data collection based on observation). Results that collected through these standards will be operated in the integration between ISO / IEC 20000 & ISO / IEC 27001 and its connection with ITIL V3 owned by XYZ institution. Then we developed and designed forms for clauses, requirements, or similar guidelines for ISO / IEC 20000 & ISO /IEC 270001.

Furthermore, we analyze the correlation between standard requirements and business processes. After the correlation has been determined ISO / IEC 20000 & ISO / IEC 270001 there will be a comparison of differences or similarities where the results of that will be described in the form of matrix mapping to determine the potential for the integration process. Figure 3 shows the process overview.

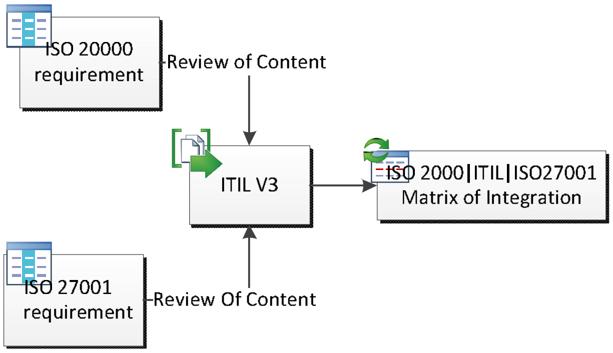

Figure 3. Analyzing Steps

This paper is compiled with a qualitative approach with a content analysis method where the authors analyze all items ISO / IEC 20000-1: 2018 and ISO / IEC 27001-1: 2013 requirements and ITIL® V3. The steps taken are as follows: Registering all the requirements needed for standard implementation, Service Management System (SMS) using ISO / IEC 20000-1: 2011, Mapping between ISO/IEC 20000-1:2011 and ISO/IEC 20000-1:2018[21] . Information Security Management Systems (ISMS) and ISO / IEC 27000-1: 2013. Analyze each of the SMS & ISMS clauses requirements and their relevance to ITIL® V3. Identify and classify clauses with similarity/similarity approaches and differences in requirements and processes in the SMS & ISMS standard. Analyze and develop a form that contains an integration matrix between SMS & ISMS that can be used as a reference in the implementation phase.

Although ISO 27001 and ITIL have different presentations, they share an approach similar to the PDCA cycle[22], which facilitates working with them. ISO 27001 and ITIL relations can be said to have similarities. Table 4.1 is the use of ISO 27001 and ITIL on PDCA as shown in Appendix 2

Table 1:ISO 27001 and ITIL PDCA Cycles

PDCA Cycle	ISO 27001:2013 clauses	ITIL stages
Plan	Clause 4 – Context of the organization Clause 5 – Leadership Clause 6 – Planning Clause 7 – Support	Service strategy Service design
Do	Clause 8 – Operation	Service transition Service operation
Check	Clause 9 – Performance evaluation	Continual service improvement
Act	Clause 10 – Continual improvement	Continual service improvement

The standard ISO 20000: 2018 requirements in the service management process can be mapped to the ITIL Stages. Appendix 3 is a mapping from ISO 20000: 2011 to the ITIL stage.

5. RESULT AND ANALYSIS

This paper explains that all management systems based on ISO standards will use PDCA methodology (Plan, Do, Check, and Act). This methodology explains the relationship between ISO 20000 and ISO 27001 as shown in Appendix 4. From appendix 4 can be concluded that The Board in the organization should commit to adapted SMS and ISMS to the organization and assigned resource for the implementation process; where senior management should be responsible for the implementation process. The implementation team will be creating plans to achieve SMS and ISMS objectives. The plan will also contain risk methodology, risk register, and risk mitigation. From our analysis we also explained about awareness of all participants that implement the ISO standard must be properly educated in information security and service management, know how to communicate the policy that will be used as guidelines to achieve the objective. The team should prepare document and note control, SOPs, and guidelines for all members will be established which allow for management metrics that will set metrics to measure the effectiveness of security controls and determine ISO 20000 metrics to measure process effectiveness. The internal audit process will detect possible nonconformities and determine the level of implementation regarding the reference standard so that it can review the top management of the organization which must review a series of entry points for the standard. Finally, corrective/preventive measures for continuous improvement are about integrated management systems that can develop corrective and preventive actions to treat detected nonconformities.

6. CONCLUSION AND FURTHER WORKS

The conclusion in this paper is that the integration is able to be practically done by matching point by point of each standardization. In the matching process, the points should be able to meet the weight of the calculation so that each of these points has the same value so that it can be said that for that point it can be declared the same. There is a 41.7 % clause that are can be integrated between ISO 20000 and 270001.

Suggestions for future development can be done by adding integration analysis based on the condition of a company's IT organizational structure and matching. It is hoped that integration will save company resources. In the next study the author.

REFERENCES

1. P. P. Connell, B., Mallett, R., Rochet, P., Chow, E., Savino, L., *Enterprise governance: Getting the balance right*. 2004.
2. R. R. Moeller, *COSO enterprise risk management: understanding the new integrated ERM framework*. 2007.

3. H. Nugroho, **CONCEPTUAL MODEL OF IT GOVERNANCE FOR HIGHER EDUCATION BASED ON COBIT 5 FRAMEWORK,** vol. 60, n, pp. 216–221, 2014.
4. I. G. Institute, **Framework Control Objectives Management Guidelines Maturity Models.**, 2007.
5. M. Nyonawan, Suharjito, and D. N. Utama, **Evaluation of Information Technology Governance in STMIK Mikroskil Using COBIT 5 Framework,***Proc. 2018 Int. Conf. Inf. Manag. Technol. ICIMTech 2018*, no. September, pp. 137–142, 2018. https://doi.org/10.1109/ICIMTech.2018.8528138
6. I. Macfarlane, **An Introductory Overview of ITIL ® V3 An Introductory Overview of ITIL ® V3,** 2007.
7. J. A. Villanueva, L. L. Lacatan, and A. A. Vinluan, **Information technology security infrastructure malware detector system,***Int. J. Adv. Trends Comput. Sci. Eng.*, vol. 9, no. 2, pp. 1583–1587, 2020. https://doi.org/10.30534/ijatcse/2020/103922020
8. R. Pereira and M. M. Da Silva, **A maturity model for implementing ITIL V3 in practice,***Proc. - IEEE Int. Enterp. Distrib. Object Comput. Work. EDOC*, pp. 259–268, 2011.
9. S. Kosasi, Vedyanto, and I. D. A. E. Yuliani, **Impacts of IT governance in expanding market shares of online stores,***Int. J. Adv. Trends Comput. Sci. Eng.*, vol. 8, no. 1.5 Special Issue, pp. 339–346, 2019. https://doi.org/10.30534/ijatcse/2019/5681.52019
10. R. Yandri, Suharjito, D. N. Utama, and A. Zahra, **Evaluation model for the implementation of information technology service management using fuzzy ITIL,***Procedia Comput. Sci.*, vol. 157, pp. 290–297, 2019.
11. J. W. Candra, O. C. Briliyant, and S. R. Tamba, **ISMS planning based on ISO/IEC 27001:2013 using analytical hierarchy process at gap analysis phase (Case study : XYZ institute),***Proceeding 2017 11th Int. Conf. Telecommun. Syst. Serv. Appl. TSSA 2017*, vol. 2018-Janua, no. 4, pp. 1–6, 2018. https://doi.org/10.1109/TSSA.2017.8272916
12. K. Prislan and I. Bernik, **Risk Management with ISO 27000 standards in Information Security,** pp. 58–63.
13. A. Chandra, **Iso 20000 and Itil & Correlation Between Them,***Int. J. Comput. Sci. Eng. Inf. Technol*, vol. Res., , pp. 26–45, 2012.
14. I. E. C. Fdis, **ISO / IEC 20000 Understanding the requirements of ISO / IEC FDIS 20000-1 Improve the quality of your service delivery with ISO / IEC 20000-1,** pp. 1–16, 2018.
15. I. Standart, *International Standard ISO / IEC requirements,* 2011.
16. I. S. O. Iec, **Standard is The document is a preview neutered by Reference number is The document is a preview negete rad b,** 2018.
17. ISO, **Guidance On The Application Of Services Management. [Online].** Available: https://www.iso.org/obp/ui/#iso:std:iso-iec:20000:-2:ed-3:v1:en.
18. S. Sahibudin, M. Sharifi, and M. Ayat, **Combining ITIL, COBIT and ISO/IEC 27002 in order to design a comprehensive IT framework in organizations,***Proc. - 2nd Asia Int. Conf. Model. Simulation, AMS 2008*, pp. 749–753, 2008. https://doi.org/10.1109/AMS.2008.145
19. V. Arraj, *ITIL: the basics (white paper)*, no. July. 2013.
20. D. I. S. O. Iec, *ISO / IEC Directives , Part 1 Consolidated ISO Supplement — Procedures specific to ISO*, 2014.
21. F. Standard, **ISO / IEC 20000-1 Understanding the requirements of Improve the quality of your service delivery with ISO / IEC 20000-1**, no. September, pp. 1–16, 2018.
22. K. Prislan and I. Bernik, **Risk Management with ISO 27000 standards in Information Security,** pp. 58–63.
23. BSI, **Introducing Annex SL Whitepaper ISO Revisions,** 2015.
24. E. N. D. E. R. S. Normen-vereinigung, *Information technology Security techniques Information security management systems Requirements.* 2005.

Appendix 1: ISO High-level Structurefor All New andRevisedManagement System Standards[23]

ISO High-level Structurefor All New and Revised Management System Standards
0 Introduction
1 Scope
2 Normative references
3 Terms and definitions
4 Context of the organization
4.1 Understanding the organization and its context
4.2 Understanding the needs and expectations of interested parties
4.3 Determining the scope of the XXX management system
4.4 XXX management system
5 Leadership
5.1 Leadership and commitmen
5.2 Policy
5.3 Organizational roles, responsibilities and authorities
6 Planning
6.1 Actions to address risks and opportunities
6.2 XX objectives and planning to achieve them
7 Support
7.1 Resources
7.2 Competence
7.3 Awareness
7.4 Communication
7.5 Documented information
7.5.1 General
7.5.2 Creating and updating
7.5.3 Control of documented information
8 Operation
8.1 Operational planning and control
9 Performance evaluation
9.1 Monitoring, measurement, analysis and evaluation
9.2 Internal audit
9.3 Management Review
10 Improvement
10.1 Nonconfomity and corrective action
10.2 Continual Improvement

Appendix 2 : ISO 27001 : 2013 Information Security Management System Requirement[24]

ISO 27001 : 2013 Information SecurityManagement System Requirement
0 Introduction
1 Scope
2 Normative references
3 Terms and definitions
4 Context of the organization
4.1 Understanding the organization and its context
4.2 Understanding the needs and expectations of interested parties
4.3 Determining the scope of the information security management system
4.4 Information security management system
5 Leadership
5.1 Leadership and commitmen
5.2 Policy
5.3 Organizational roles, responsibilities and authorities
6 Planning
6.1 Actions to address risks and opportunities
6.1.1.General
6.1.2 Informationa Security risk assesment
6.1.3 Informationa Security risk treatment
6.2 Informationa Security objectives and planning to achieve them
7 Support
7.1 Resources
7.2 Competence
7.3 Awareness
7.4 Communication
7.5 Documented information
7.5.1 General
7.5.2 Creating and updating
7.5.3 Control of documented information
8 Operation
8.1 Operational planning and control
8.2 Information security risk assessment
8.3 Infromation security risk treatment
9 Performance evaluation
9.1 Monitoring, measurement, analysis and evaluation
9.2 Internal audit
9.3 Management Review
10 Improvement
10.1 Nonconfomity and corrective action
10.2 Continual Improvement

ISO 27001 : 2013 Reference control objectives and controls
A5 Information security policies
A5.1 Management direction for information security
A5.1.1 Policies for information security
A5.1.2 Review of the policies for information security
A6 Organization of information security
A6.1 Internal organization
A6.1.1 Information security roles and responsibilities
A6.1.2 Segregation of duties
A6.1.3 Contact with authorities
A6.1.4 Contact with special interest groups
A6.1.5 Information security in project management
A6.2 Mobile devices and teleworking
A6.2.1 Mobile device policy
A6.2.2 Teleworking
A7 Human resource security
A7.1 Prior to employment
A7.1.1 Screening
A7.1.2 Terms and conditions of employment
A7.2 During employment
A7.2.1 Management responsibilities
A7.2.2 Information security awareness, education and training
A7.2.3 Disciplinary process
A7.3 Termination and change of employment
A7.3.1 Termination or change of employment responsibilities
A8 Assetmanagement
A8.1 Responsibility for assets
A8.1.1 Inventory of assets
A8.1.2 Ownership of assets
A8.1.3 Acceptableuse of assets
A8.1.4 Return of assets
A8.2 Information classification
A8.2.1 Classification of information
A8.2.2 Labelling of information
A8.2.3 Handling of assets
A8.3 Media handling
A8.3.1 Management of removable media
A8.3.2 Disposal of media
A8.3.3 Physical media transfer
A9 Access control
A9.1 Business requirements of accesscontrol
A9.1.1 Access controlpolicy
A9.1.2 Access to networks and network services
A9.2 User access management

A9.2.1 User registration and de-registration
A9.2.2 User access provisioning
A9.2.3 Management of privileged access rights
A9.2.4 Management of secret authentication information of users
A9.2.5 Review of user access rights
A9.2.6 Removal or adjustment of access rights
A9.3 User responsibilities
A9.3.1 Use of secret authentication information
A9.4 System and application access control
A9.4.1 Information access restriction
A9.4.2 Secure log-on procedures
A9.4.3 Password management system
A9.4.4 Use of privileged utility programs
A9.4.5 Access controlto program sourcecode
A10 Cryptography
A10.1 Cryptographic controls
A10.1.1 Policy on the use of cryptographic controls
A10.1.2 Key management
A11 Physical and environmental security
A11.1 Securea reas
A11.1.1 Physical security perimeter
A11.1.2 Physical entry controls
A11.1.3 Securing offices, rooms and facilities
A11.1.4 Protecting against external and environmental threats
A11.1.5 Working in secure areas
A11.1.6 Delivery and loading areas
A11.2 Equipment
A11.2.1 Equipment siting and protection
A11.2.2 Supporting utilities
A11.2.3 Cabling security
A11.2.4 Equipment maintenance
A11.2.5 Removal of assets
A11.2.6 Security of equipment and assets off-premises
A11.2.7 Secure disposal or reuse of equipment
A11.2.8 Unattended user equipment
A11.2.9 Clear desk and clear screen policy
A12 Operations security
A12.1 Operational procedures and responsibilities
A12.1.1 Documented operating procedures
A12.1.2 Change management
A12.1.3 Capacity management
A12.1.4 Separation of development, testing and operational environments
A12.2 Protection from malware
A12.2.1 Controls against malware

A12.3 Backup
A12.3.1 Information backup
A12.4 Logging and monitoring
A12.4.1 Event logging
A12.4.2 Protection of log information
A12.4.3 Administrator and operator logs
A12.4.4 Clock synchronisation
A12.5 Control of operational software
A12.5.1 Installation of software on operational systems
A12.6 Technical vulnerability management
A12.6.1 Management of technical vulnerabilities
A12.6.2 Restrictionson software installation
A12.7 Information systems audit considerations
A12.7.1 Information systems audit controls
A13 Communications security
A13.1 Network security management
A13.1.1 Network controls
A13.1.2 Security of network services
A13.1.3 Segregation in networks
A13.2 Information transfer
A13.2.1 Information transfer policies and procedures
A13.2.2 Agreements on information transfer
A13.2.3 Electronic messaging
A13.2.4 Confidentiality or non disclosure agreements
A14 System acquisition, development & maintenance
A14.1 Security requirements of information systems
A14.1.1 Information security requirements analysis and specification
A14.1.2 Securing application services on public networks
A14.1.3 Protecting application services transactions
A14.2 Security in development and support processes
A14.2.1 Secure development policy
A14.2.2 System change control procedures
A14.2.3 Technical review of applications after operating platform changes
A14.2.4 Restrictions on changes to software packages
A14.2.5 Secure system engineering principles
A14.2.6 Secure Development Environment
A14.2.7 Outsourced development
A14.2.8 System security testing
A14.2.9 System acceptance testing
A14.3 Test data
A14.3.1 Protection of test data
A15 Supplier relationships
A15.1 Information security in supplier relationships
A15.1.1 Information security policy for supplier relationships

A15.1.2 Addressing security within supplier agreements
A15.1.3 ICT supply chain
A15.2 Supplier service delivery management
A15.2.1 Monitoring and review of supplier services
A15.2.2 Managing changes to supplier services
A16 Information security incident management
A16.1 Management of information security incidents & improvements
A16.1.1 Responsibilities and procedures
A16.1.2 Reporting information security events
A16.1.3 Reporting information security weaknesses
A16.1.4 Assessment of and decisionon information security events
A16.1.5 Response to information security incidents
A16.1.6 Learning from information security incidents
A16.1.7 Collection of evidence
A17 Information security aspects of BCM
A17.1 Information security continuity
A17.1.1 Planning information security continuity
A17.1.2 Implementing information securitycontinuity
A17.1.3 Verify, review and evaluate information security continuity
A17.2 Redundancies
A17.2.1 Availability of information processing facilities
A18 Compliance
A18.1 Compliance with legal and contractual requirements
A18.1.1 Identification of applicable legislation and contractual requirements
A18.1.2 Intellectual property rights
A18.1.3 Protection of records
A18.1.4 Privacy and protection of personally identifiable information
A18.1.5 Regulation of cryptographic controls
A18.2 Information security reviews
A18.2.1 Independent review of information security
A18.2.2 Compliance with security policies and standards
A18.2.3 Technical compliance review

Appendix 3: ISO 20000 : 2018 Service Management System Requirement[15]

ISO 20000 : 2018 Service Management System Requirement	ITIL V3 Area	ITIL Process
0 Introduction		
1 Scope		
2 Normative references		
3 Terms and definitions		
4 Context of the organization		
4.1 Understanding the organization and its context		
4.2 Understanding the needs and expectations of interested parties		
4.3 Determining the scope of the service management system		
4.4 Service management system		
5 Leadership	Service Strategy	
5.1 Leadership and commitmen	Service Strategy	
5.2 Policy	Service Strategy	
5.2.1 Establishing the service management policy	Service Strategy	
5.2.2 Communicating the service management policy	Service Strategy	
5.3 Organizational roles, responsibilities and authorities	Service Strategy	
6 Planning	Service Strategy	
6.1 Actions to address risks and opportunities	Service Strategy	
6.2 Service management objectives and planning to achieve them	Service Strategy	
6.2.1 Establish Objectives	Service Strategy	
6.2.2 Plan to achieve Objectives	Service Strategy	
6.3 Plan the service management system	Service Strategy	
7 Support		
7.1 Resources	Service Design	Capacity Management
7.2 Competence	Service Design	Capacity Management
7.3 Awareness		
7.4 Communication		
7.5 Documented information	Service Design	Access Management
7.5.1 General	Service Design	Access Management
7.5.2 Creating and updating documented information	Service Design	Access Management
7.5.3 Control of documented information	Service Design	Access Management
7.5.4 Service management system documented information	Service Design	Access Management
7.6 Knowledge	Service Transition	Knowledge Management
8 Operation		
8.1 Operational planning and control		
8.2 Service Portfolio	Service Strategy	Service Portfolio management
8.2.1 Service Delivery	Service Strategy	Service Portfolio management
8.2.2 Plan theservices	Service Strategy	Service Portfolio management
8.2.3 Control of parties involved in the service life cycle	Service Strategy	Service Portfolio management
8.2.4 Service catalogue management	Service Design	Service Catalog Management

8.2.5 Asset management	Service Transition	Service Asset and Configuration Management
8.2.6 Configuration management	Service Transition	Service Asset and Configuration Management
8.3 Relationship agreement	Service Strategy	
8.3.1 General	Service Strategy	Demand Management
8.3.2 Business relationship management	Service Strategy	Demand Management
8.3.3 Service Level Management	Service Design	Service Level Management
8.3.4 SupplierManagement	Service Design	Supplier Management
8.4 Supply and demand	Service Strategy	
8.4.1 Budgeting and accounting for services	Service Strategy	Financial management
8.4.2 Demand Management	Service Strategy	Demand management
8.4.3 Capacity Management	Service Design	Capacity Management
8.5 Service Design, build and transition	Service Transition	
8.5.1. Change Management	Service Transition	Change Management
8.5.2 Service design and transition	Service Transition	Transition Planning and Support
8.5.3 Release & Deployment management	Service Transition	Release and Deployment Management
8.6 Resolutionand Fulfilment	Service Operation	
8.6.1 Incident Management	Service Operation	Incident Management
8.6.2 Service Request Management	Service Operation	Request Fulfillment
8.6.3 Problem Management	Service Operation	Problem Management
8.7 Service Assurance		
8.7.1 Service availability management	Service Design	Availability Management
8.7.2 Service continuity management	Service Design	IT service Continuity Management
8.7.3 Information Security Management	Service Design	Information Security Management Access Management
9 Performance evaluation	Continual service improvement	
9.1 Monitoring, measurement, analysis and evaluation	Continual service improvement	Service Measurement
9.2 Internal audit	Continual service improvement	The 7 improvement process
9.3 Management Review	Continual service improvement	The 7 improvement process
9.4 Service Reporting	Continual service improvement	Service Reporting
10 Improvement	Continual service improvement	
10.1 Non confomity and corrective action	Continual service improvement	The 7 improvement process
10.2 ContinualImprovement	Continual service improvement	The 7 improvement process

Integration of ITIL V3, ISO 20000 & ISO 27001:2013

Appendix 4: Main Clause Integration of ISO 20000, 27000, and ITIL

ISO 20000 : 2018 Service Management System Requirement	ISO 27001 : 2013 Information Security Management System Requirement	Integration? (I:Integrated/ N:Not Integrated)	ITIL Area	Sample of Integration
0 Introduction	**0 Introduction**			
1 Scope	**1 Scope**			
2 Normative references	**2 Normative references**			
3 Terms and definitions	**3 Terms and definitions**			
4 Context of the organization	**4 Context of the organization**			
4.1 Understanding the organization and its context	4.1 Understanding the organization and its context			
4.2 Understanding the needs and expectations of interested parties	4.2 Understanding the needs and expectations of interested parties			
4.3 Determining the scope of the service management system	4.3 Determining the scope of the information security management system			
4.4 Service management system	4.4 Information security management system			
5 Leadership	**5 Leadership**		Service Strategy	
5.1 Leadership and commitment	5.1 Leadership and commitment	I	Service Strategy	• Signed SMS and ISMS Policy • broadcast or announcement of SMS and ISMS Policy • Resource assignment for SMS and ISMS Implementation
5.2 Policy	5.2 Policy	I	Service Strategy	
5.2.1 Establishing the service management policy			Service Strategy	
5.2.2 Communicating the service management policy			Service Strategy	
5.3 Organizational roles, responsibilities and authorities	5.3 Organizational roles, responsibilities and authorities	I	Service Strategy	RACI table for SMS & ISMS Management
6 Planning	**6 Planning**		Service Strategy	Document SMS & ISMS Plan
6.1 Actions to address risks and opportunities	6.1 Actions to address risks and opportunities	I	Service Strategy	• Risk Methodology • Risk Register
	6.1.1. General	I		
	6.1.2 Information Security risk assessment	I		

Integration of ITIL V3, ISO 20000 & ISO 27001:2013

	6.1.3 Information Security risk treatment	I		• Risk Mitigation
6.2 Service management objectives and planning to achieve them	6.2 Information Security objectives and planning to achieve them	I	Service Strategy	SMS & ISMS Objective
6.2.1 Establish Objectives			Service Strategy	
6.2.2 Plan to achieve Objectives			Service Strategy	
6.3 Plan the service management system		N	Service Strategy	
7 Support	**7 Support**			
7.1 Resources	7.1 Resources	I	Service Design	Budgeting on SMS & ISMS implementation
7.2 Competence	7.2 Competence	I	Service Design	Training need analysis
7.3 Awareness	7.3 Awareness	I		• Awareness ISMS Schedule • Awareness module • Induction Process • SMS & ISMS Introduction Training
7.4 Communication	7.4 Communication	I		Communication Policy
7.5 Documented information	7.5 Documented information	I	Service Design	Document control
7.5.1 General	7.5.1 General	I	Service Design	
7.5.2 Creating and updating documented information	7.5.2 Creating and updating	I	Service Design	
7.5.3 Control of documented information	7.5.3 Control of documented information	I	Service Design	
7.5.4 Service management system documented information		N	Service Design	Service catalogue
7.6 Knowledge		N	Service Transition	
8 Operation	**8 Operation**			
8.1 Operational planning and control	8.1 Operational planning and control	N		
8.2 Service Portfolio	8.2 Information security risk assessment	N	Service Strategy	
8.2.1 Service Delivery		N	Service Strategy	
8.2.2 Plan the services		N	Service Strategy	

Integration of ITIL V3, ISO 20000 & ISO 27001:2013

8.2.3 Control of parties involved in the service lifecycle		N	Service Strategy	
8.2.4 Service catalogue management		N	Service Design	
8.2.5 Asset management	A.8 Asset management	N	Service Transition	
8.2.6 Configuration management		N	Service Transition	
8.3 Relationship agreement	8.3 Information security risk treatment	N	Service Strategy	
8.3.1 General		N	Service Strategy	
8.3.2 Business relationship management		N	Service Strategy	
8.3.3 Service Level Management		N	Service Design	
8.3.4 Supplier Management	A.15 Supplier Relationship	I	Service Design	Contract Record
8.4 Supply and demand		N	Service Strategy	
8.4.1 Budgeting and accounting for services		N	Service Strategy	
8.4.2 Demand Management		N	Service Strategy	
8.4.3 Capacity Management	A12.1.3 Capacity management	I	Service Design	• Capacity Policy & Procedure • Capacity Plan document
8.5 Service Design build and transition		N	Service Transition	
8.5.1. Change Management	A12.1.2 Change management, A.14.2 Security in Development and support process	I	Service Transition	• Change Management Policy & Procedure • Security Assessment in Change Request • Security Test Document
8.5.2 Service design and transition		N	Service Transition	
8.5.3 Release & Deployment management		N	Service Transition	
8.6 Resolution and Fulfilment		N	Service Operation	
8.6.1 Incident Management	A.16 Information security incident management	I	Service Operation	• Incident Management Policy & Procedure • Security Incident (Incident Category)

Integration of ITIL V3, ISO 20000 & ISO 27001:2013

8.6.2 Service Request Management		N	Service Operation	
8.6.3 Problem Management		N	Service Operation	
8.7 Service Assurance		N		
8.7.1 Service availability management		N	Service Design	
8.7.2 Service continuity management		N	Service Design	
8.7.3 Information Security Management	A.5 Information security policies	I	Service Design	• ISMS Audit • ISMS Audit Report
9 Performance evaluation	**9 Performance evaluation**		Continual service improvement	
9.1 Monitoring, measurement, analysis and evaluation	9.1 Monitoring, measurement, analysis and evaluation	I	Continual service improvement	• Monitoring risk mitigation • ISMS Objective monitoring • Internal audit ISMS • Management Review plan, procedure, material • Service Level Report
9.2 Internal audit	9.2 Internal audit	I	Continual service improvement	
9.3 Management Review	9.3 Management Review	I	Continual service improvement	
9.4 Service Reporting	A16 Information security incident management	I	Continual service improvement	
10 Improvement	**10 Improvement**		Continual service improvement	• Internal Audit process • Internal Audit record & monitoring • Internal Audit Internal record • Management Review record
10.1 Nonconformity and corrective action	10.1 Nonconformity and corrective action	I	Continual service improvement	
10.2 Continual Improvement	10.2 Continual Improvement	I	Continual service improvement	