Planning and Control of Information Security on Infrastructure IT Management Project in Pharmaceutical Industry with ISO27001:2013 Approach

By

Hery Sapto Dwi Nurcahyo
Fakultas Teknik Elektro, Universitas Indonesia
Email: hery.sapto@ui.ac.id,

Yohan Suryanto
Fakultas Teknik Elektro, Universitas Indonesia
Email: yohansuryanto@ui.ac.id

Abstract

The success rate of implementation and development of IT Infrastructure technology on the pharmaceutical industry in Indonesia is greatly influenced by project management readiness. One aspect that receives little attention in project implementation is information security control. This aspect is a critical point that the instance must manage to maintain information security from the confidentiality (C), integrity (I), and availability (A) sides. The data from the pharmaceutical IT security team in 2021 also shows that there have been incidents caused by internal and external threats of 2928 every month and have a close correlation with the IT Infrastructure project. So that in this study a plan and governance of the application of information security controls to IT Infrastructure management projects using the ISO 27001: 2013 approach will be carried out. The application of these security controls is expected to reduce incidents and can be a recommendation to address vulnerabilities to security threats that could affect future business processes.

Keyword: Project Management, IT Infrastruktur, Information Security, ISO27001:2013.

Introduction

Digital transformation is changing the way agencies from different sectors view making investments in technology in supporting businesses to run effectively and efficiently. A large number of technologies in the modern era such as these days makes it necessary for business operators to choose and adapt according to the needs of agencies to have maximum benefit. The selection of appropriate technologies should also be accompanied by thorough project management. In performing project management planning it is very rare for an instance to notice and focus on information security factors. Control over information security will maintain confidentiality (C), integrity (I), and availability (A) over instance data. So it would be good if technology implementation projects were balanced with information security protection so that there were control mechanisms and outcomes that match expectations.

Digital transformation is also taking place in one of the pharmaceutical industries in Indonesia and technology is a tool used to realize it. Whereas the foundation of its own technology is the presence of a qualified IT Infrastructure to accelerate the occurrence of the process. The rapid development of one of these pharmaceutical industries has caused many requests for technology-related projects, especially IT Infrastructure that come from the initiation of users or management. There are a total of 30 IT Infrastructure projects in the pharmaceutical industry undertaken from 2021 to 2025. The project will be worked out by the Corporate IT Infrastructure team consisting of Planning, Project, and Operation. The emergence of many incidents caused by external and internal threats correlates with the IT Infrastructure project undertaken previously to be a real vulnerability and could affect future business processes. The condition is also strengthened by data obtained from the evaluation of the security team of the pharmaceutical industry IT in 2021 that there are incidents caused by 786 external threats and 2142 internal threats every month.

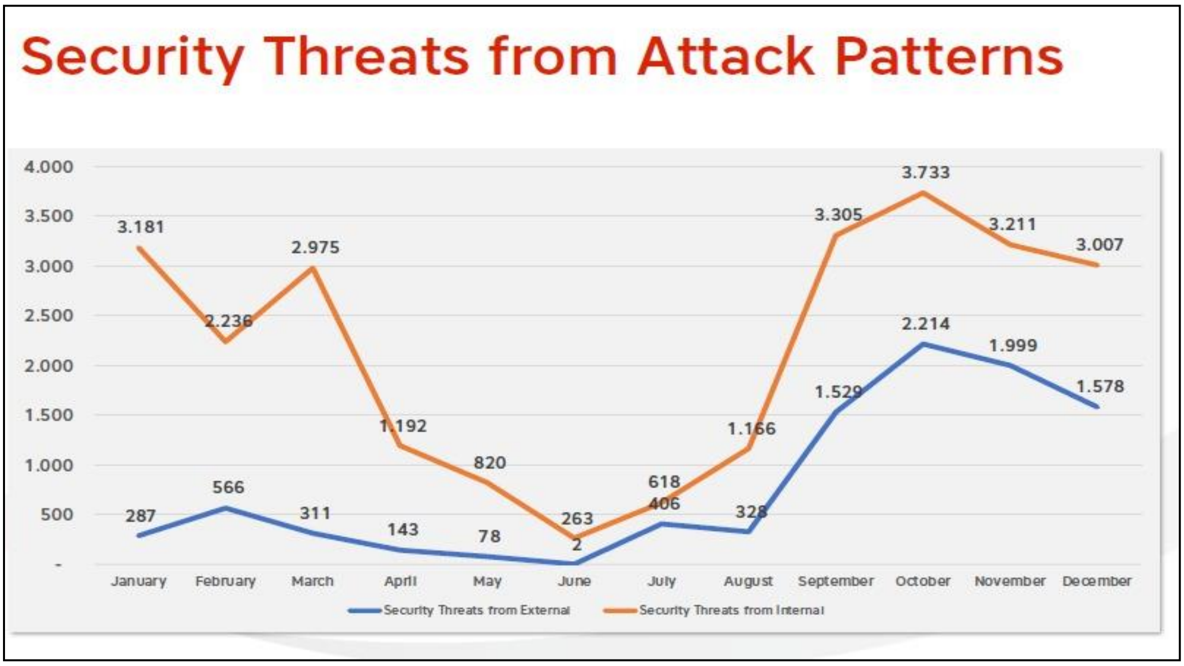


Fig.1. *Summary threat incident 2021*

Data mapping also shows a correlation between incidents that occurred with IT Infrastructure projects over the past 3 years. This data is obtained by creating groups on project workarounds over the past 3 years and correlated with threats in quarter 1 2021 in the IT Infrastructure area consisting of servers, storage, network, and data center facilities.

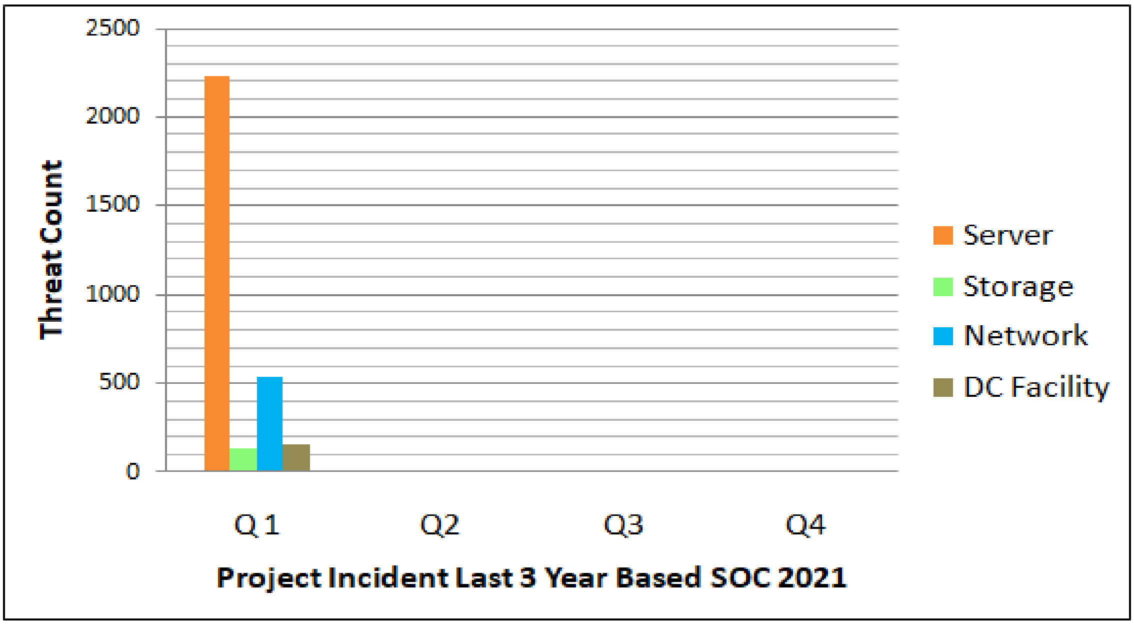
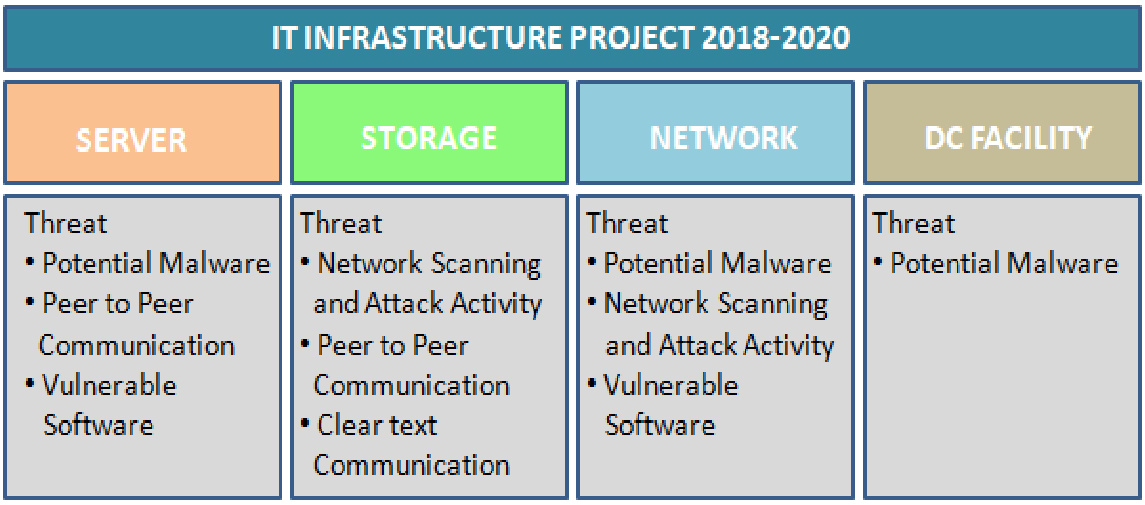


Fig.2. *Project and Threat Correlation*



IT INFRASTRUCTURE PROJECT 2018-2020			
SERVER	STORAGE	NETWORK	DC FACILITY
Threat • Potential Malware • Peer to Peer Communication • Vulnerable Software	Threat • Network Scanning and Attack Activity • Peer to Peer Communication • Clear text Communication	Threat • Potential Malware • Network Scanning and Attack Activity • Vulnerable Software	Threat • Potential Malware

Fig.3. *Threat Category in IT Infrastructure Project*

It is therefore imperative that project management planning be accompanied by information security controls that are expected to bring down incidents that occur. Taking the ISO 27001:2013 approach can serve as a recommendation and guide for IT Infrastructure project management in the industry, so it can prevent security threats that could affect future business processes.

Review and Related Literature

In this study discussed planning and control of information data security on IT Infrastructure technology implementation projects. The author will discuss related terms and understandings relating to such research.

2.1. Project Management

Project Management is an activity or activity related to project workmanship ranging from planning, execution, completion, and monitoring. As in the understanding that refers to references The Project Management Institute (PMI) (2013a, p. 8) defines project management as "the application of knowledge, skills, tools, and techniques to project activities to meet the project requirement" [3]. Project management is closely linked to the activities of an agency to achieve the objectives of its business. The aspects contained in it must have effective and efficient functions. In this case means it is effective in using resources and activities in accordance with its planning as well as its target covering security, quality, cost, time, and others. Whereas efficiently it is interpreted as using resources and selecting activities appropriately covering the number, type, time, etc. Project Management has five main phases: project initiation, project planning, project execution and control, project monitoring, and project closing[3].

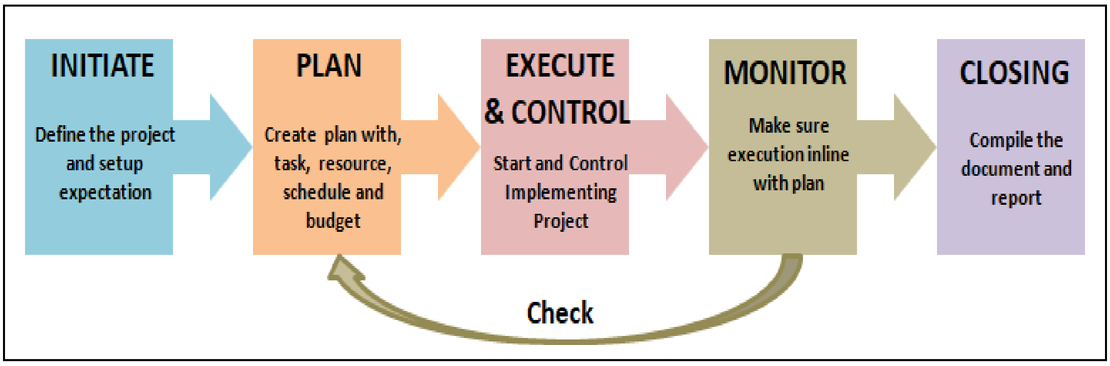

INITIATE
Define the project and setup expectation
PLAN
Create plan with, task, resource, schedule and budget
EXECUTE & CONTROL
Start and Control Implementing Project
MONITOR
Make sure execution inline with plan
CLOSING
Compile the document and report
Check

Fig.4. *The five phases of the project management lifecycle redesign*

2.2. IT Infrastructure

IT Infrastructure is the overall foundation underlying an application running its system. For its group, it covers its hardware, software, computer network, and support facilities. The main components of IT Infrastructure are server, storage, network, client, and data center facilities. Understanding IT Infrastructure includes network and middleware components that facilitate data delivery as well as a distribution [4]. Whereas understanding servers is a computer system that provides resources used as centralized data exchange as well as services for specific applications. For storage used as a primary data store either long-term or short-term. For networks constitute containers for hardware or software to communicate with each other efficiently and effectively. And the client constitutes a device that uses the services of all three components. Whereas for server centralization facilities, storage, network, and client are referred to by the data center

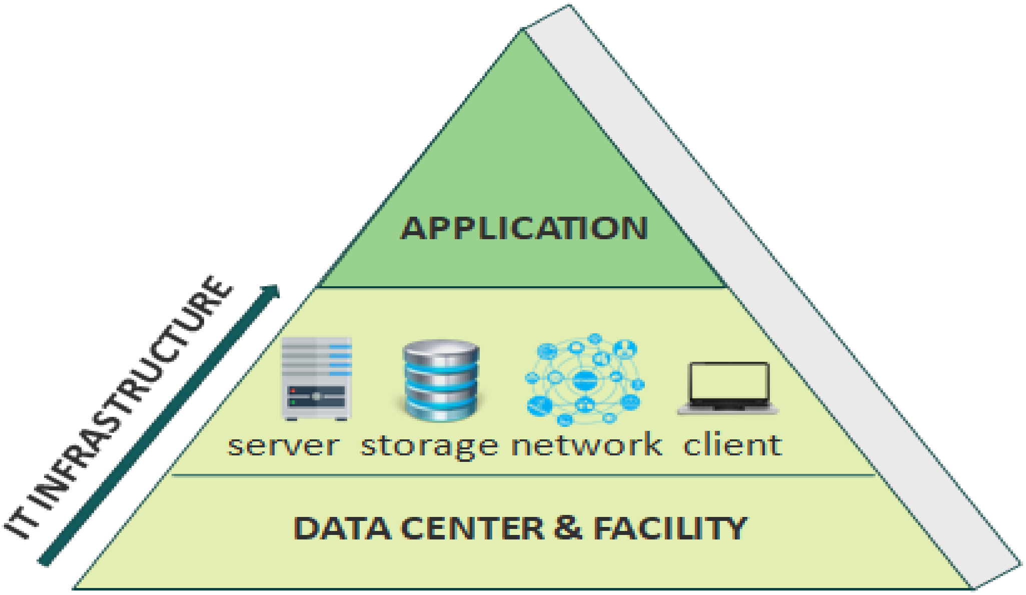


Fig.5. *IT Infrastructure component redesign*

2.3. Information Security

Information security can be interpreted as a strategy, rule, direction, and treatment to protect the confidentiality, integrity, and availability of data and prevent unauthorized access, use, modification, recording, and destruction of information. Not only can information security be applied to aspects of information technology only, but industries or agencies must also have a basis of understanding related to it so that in the event of an incident an industry or agency can make a quick recovery. Thus the need for information security can be met through thorough asset management in every aspect of the industry or agency.

On a good understanding basis related to information security, as well as the application of policies, strategies, rules, directives, and appropriate treatment according to applicable regulatory standards, then the industry or agency can minimize the presence of threat and vulnerability issues to emerging assets better. In the process of applying information security, industries or agencies should pay attention to 3 main aspects based on the core of the definition of information security i.e., confidentiality, integrity, and availability (convergence) often also referred to by the CIA. [5] Generally when attacks, problems, and risks threaten your information security, then there's at least one aspect of the CIA that will be the target of the attack.

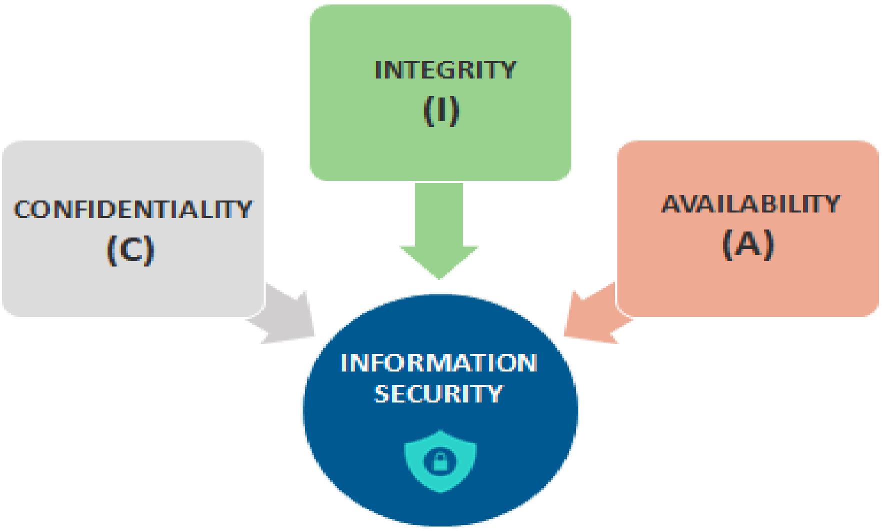


Fig.6. *Information security diagram redesign*

2.5. ISO 27001:2013

ISO 27001 represents an International standard in implementing better-known information security management systems with Information Security Management Systems (ISMS). ISO 27001 is an ISMS standard published by the International Organization for Standardization (ISO). The latest version was published in 2013 known as ISO 27001:2013. Applying the ISO 27001 standard will assist your organization or company in building and maintaining an information security management system (ISMS). ISMS represents a set of interrelated elements with an organization or company used to manage and control information security risks and to protect and maintain confidentiality (confidentiality), integrity (integrity), and availability (availability) of information. [1]

Research Method

The Research methodology that researchers conduct in conducting information data security planning and control on IT Infrastructure project management. The first step is to identify the problem and next look at solving the solution. The second step is to conduct a library review, at this stage intending to deepen the researcher's knowledge of the research plan to be carried out. The third step is the collection of data relating to the research process. The data collection technique performed is to conduct interviews with the implementation project operator side and data security-related policymakers of the pharmaceutical industry's corporate IT team. Once the data is collected then an analysis of the data will be conducted for conclusions to be drawn and serve as a basis as recommendation material for the management of implementation projects accompanied by security controls.

Result And Discussion

This section will discuss the results of the information security control plan for the IT Infrastructure technology implementation project. The safety management and control plan was prepared based on the existing project management stages in the pharmaceutical industry. The following is a framework proposed for delivering ISO27001:2013-based security control (ISMS) to project management processes with major phases initiate, plan, control, and execution, monitoring then closing.

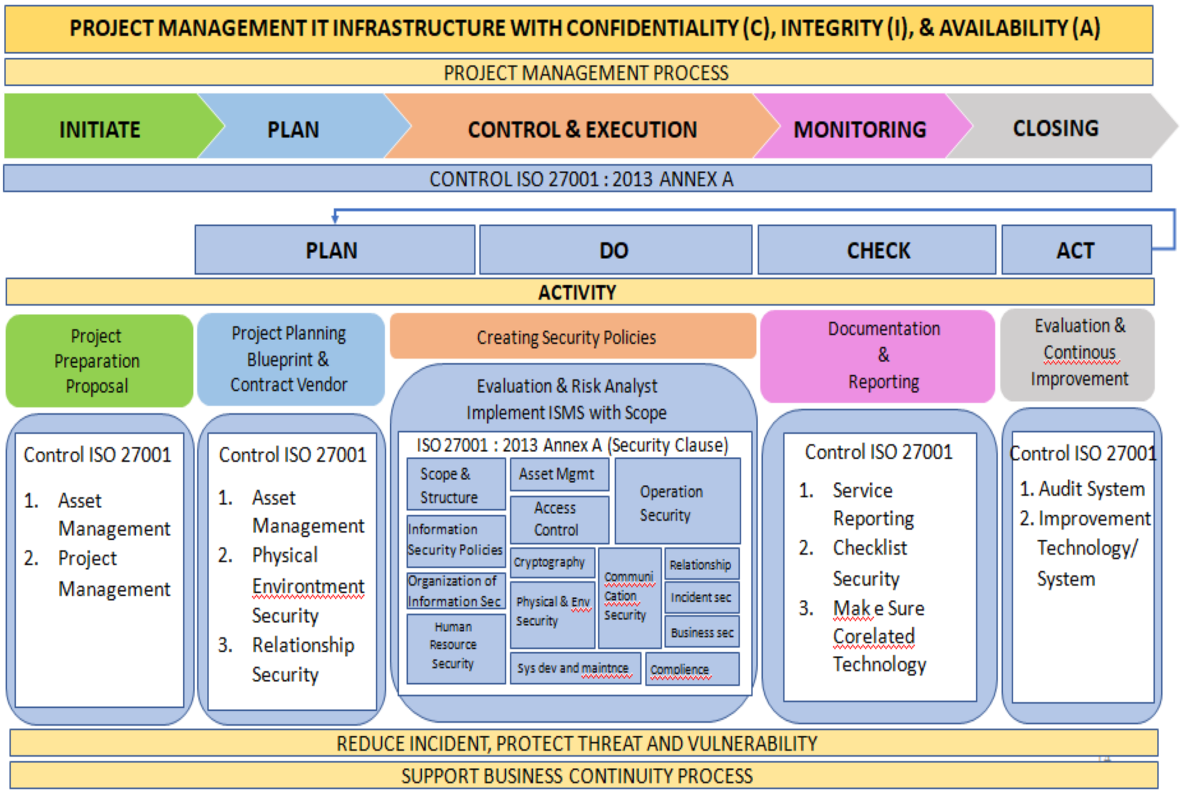

PROJECT MANAGEMENT IT INFRASTRUCTURE WITH CONFIDENTIALITY (C), INTEGRITY (I), & AVAILABILITY (A)
PROJECT MANAGEMENT PROCESS
INITIATE
PLAN
CONTROL & EXECUTION
MONITORING
CLOSING
CONTROL ISO 27001 : 2013 ANNEX A
PLAN
DO
CHECK
ACT
ACTIVITY
Project Preparation Proposal
Project Planning Blueprint & Contract Vendor
Creating Security Policies
Documentation & Reporting
Evaluation & Continous Improvement
Evaluation & Risk Analyst
Implement ISMS with Scope
Control ISO 27001
1. Asset Management
2. Project Management
Control ISO 27001
1. Asset Management
2. Physical Environtment Security
3. Relationship Security
ISO 27001 : 2013 Annex A (Security Clause)
Scope & Structure
Asset Mgmt
Operation Security
Access Control
Information Security Policies
Cryptography
Communi Cation Security
Relationship
Organization of Information Sec
Physical & Env Security
Incident sec
Business sec
Human Resource Security
Sys dev and maintnce
Complience
Control ISO 27001
1. Service Reporting
2. Checklist Security
3. Mak e Sure Corelated Technology
Control ISO 27001
1. Audit System
2. Improvement Technology/ System
REDUCE INCIDENT, PROTECT THREAT AND VULNERABILITY
SUPPORT BUSINESS CONTINUITY PROCESS

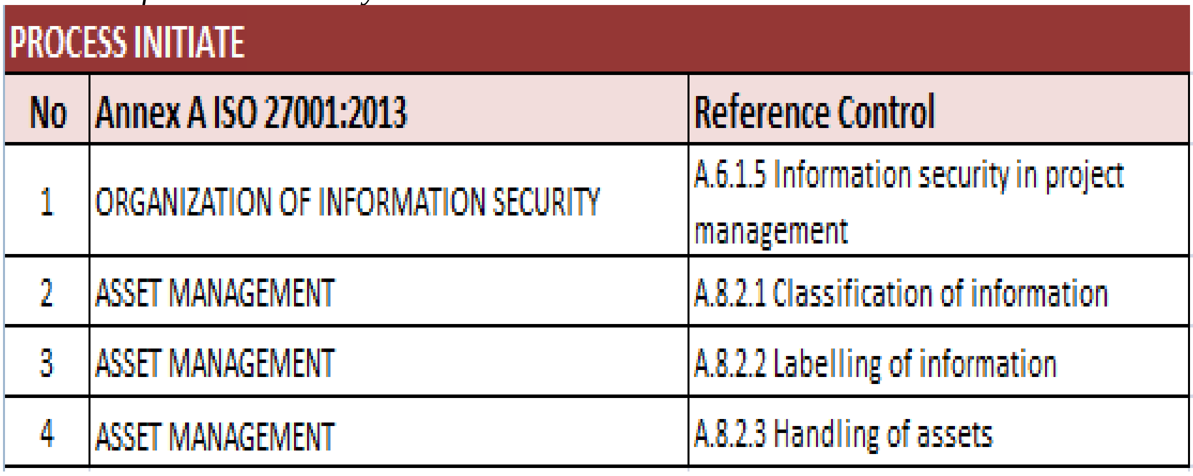
Fig.7. *Proposal of IT Infrastructure project management control framework*

The following are proposed security process controls on project management processes based on ISO27001:2013

Initiate

The initiation process represents the beginning of the project activity initiated. This stage contains sensitive information that guarded current his secrecy. The result of this process is a document containing the initiation of a project to be carried out involving the project operator and its users.

Table.1. *Information security control initiate*

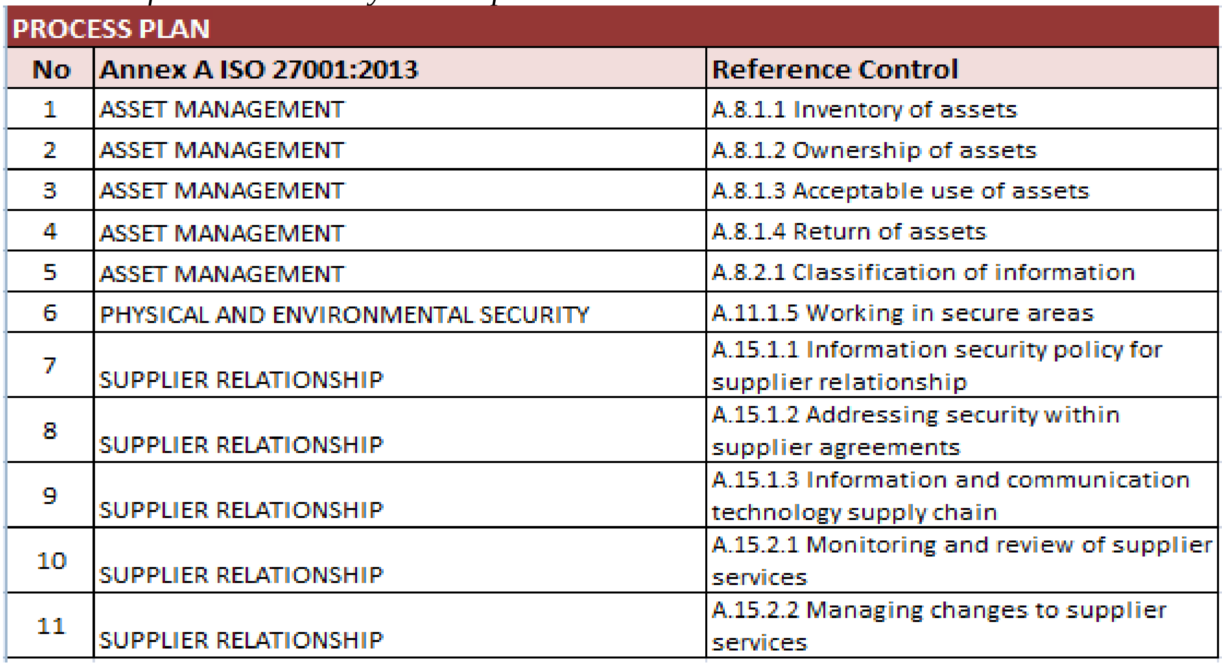


PROCESS INITIATE		
No	Annex A ISO 27001:2013	Reference Control
1	ORGANIZATION OF INFORMATION SECURITY	A.6.1.5 Information security in project management
2	ASSET MANAGEMENT	A.8.2.1 Classification of information
3	ASSET MANAGEMENT	A.8.2.2 Labelling of information
4	ASSET MANAGEMENT	A.8.2.3 Handling of assets

Plan

At this stage is a project planning process whose activities include collection of project requirements information, system/technology testing, conducting vendor and technology comparisons, and contracting processes as well as up to device delivery.

Table.2. *Information security control plan*



PROCESS PLAN

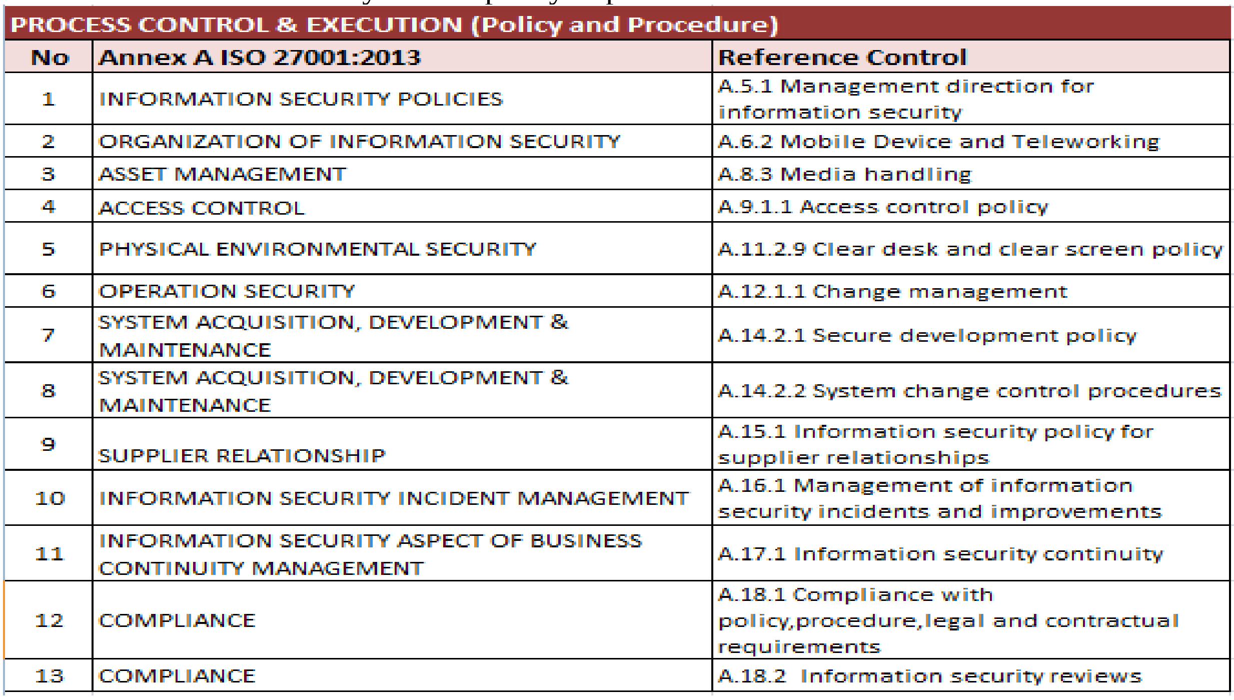
No	Annex A ISO 27001:2013	Reference Control
1	ASSET MANAGEMENT	A.8.1.1 Inventory of assets
2	ASSET MANAGEMENT	A.8.1.2 Ownership of assets
3	ASSET MANAGEMENT	A.8.1.3 Acceptable use of assets
4	ASSET MANAGEMENT	A.8.1.4 Return of assets
5	ASSET MANAGEMENT	A.8.2.1 Classification of information
6	PHYSICAL AND ENVIRONMENTAL SECURITY	A.11.1.5 Working in secure areas
7	SUPPLIER RELATIONSHIP	A.15.1.1 Information security policy for supplier relationship
8	SUPPLIER RELATIONSHIP	A.15.1.2 Addressing security within supplier agreements
9	SUPPLIER RELATIONSHIP	A.15.1.3 Information and communication technology supply chain
10	SUPPLIER RELATIONSHIP	A.15.2.1 Monitoring and review of supplier services
11	SUPPLIER RELATIONSHIP	A.15.2.2 Managing changes to supplier services

Control and Execution

Policy and Procedure

This stage constitutes planning controllers that govern related to instructions and procedures for protecting information security while performing the execution of infrastructure IT technology projects.

Table.3. Information security control policy & procedure



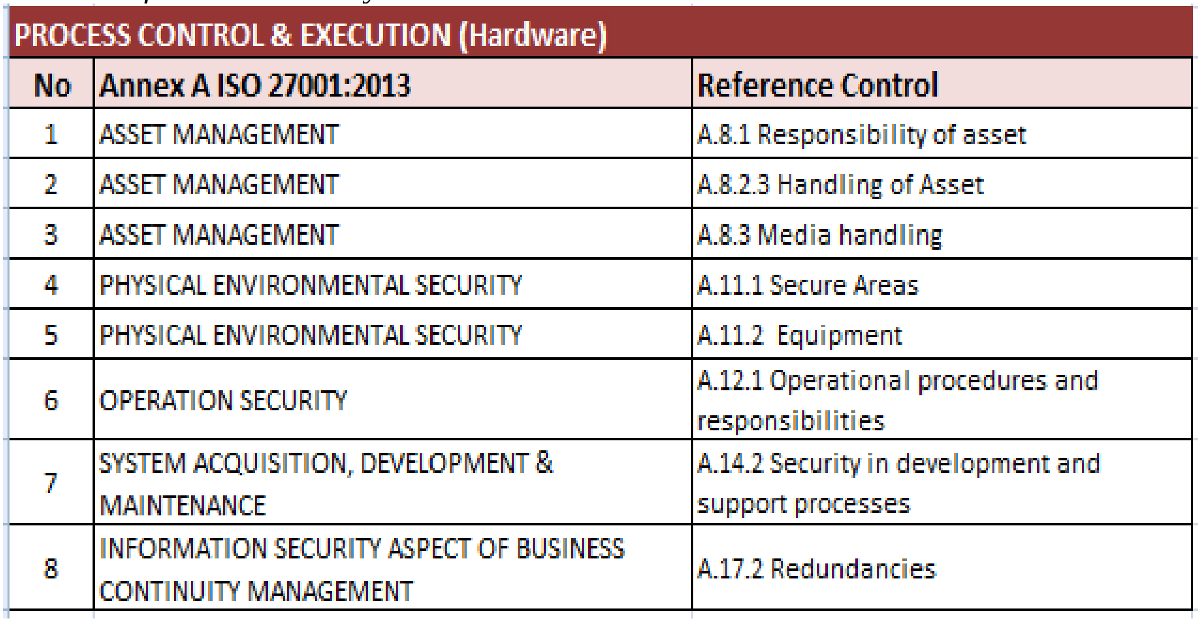
PROCESS CONTROL & EXECUTION (Policy and Procedure)

No	Annex A ISO 27001:2013	Reference Control
1	INFORMATION SECURITY POLICIES	A.5.1 Management direction for information security
2	ORGANIZATION OF INFORMATION SECURITY	A.6.2 Mobile Device and Teleworking
3	ASSET MANAGEMENT	A.8.3 Media handling
4	ACCESS CONTROL	A.9.1.1 Access control policy
5	PHYSICAL ENVIRONMENTAL SECURITY	A.11.2.9 Clear desk and clear screen policy
6	OPERATION SECURITY	A.12.1.1 Change management
7	SYSTEM ACQUISITION, DEVELOPMENT & MAINTENANCE	A.14.2.1 Secure development policy
8	SYSTEM ACQUISITION, DEVELOPMENT & MAINTENANCE	A.14.2.2 System change control procedures
9	SUPPLIER RELATIONSHIP	A.15.1 Information security policy for supplier relationships
10	INFORMATION SECURITY INCIDENT MANAGEMENT	A.16.1 Management of information security incidents and improvements
11	INFORMATION SECURITY ASPECT OF BUSINESS CONTINUITY MANAGEMENT	A.17.1 Information security continuity
12	COMPLIANCE	A.18.1 Compliance with policy,procedure,legal and contractual requirements
13	COMPLIANCE	A.18.2 Information security reviews

Hardware

This stage constitutes planning controllers that govern the information security of IT Infrastructure projects on hardware aspects.

Table.4. *Information security control hardware*

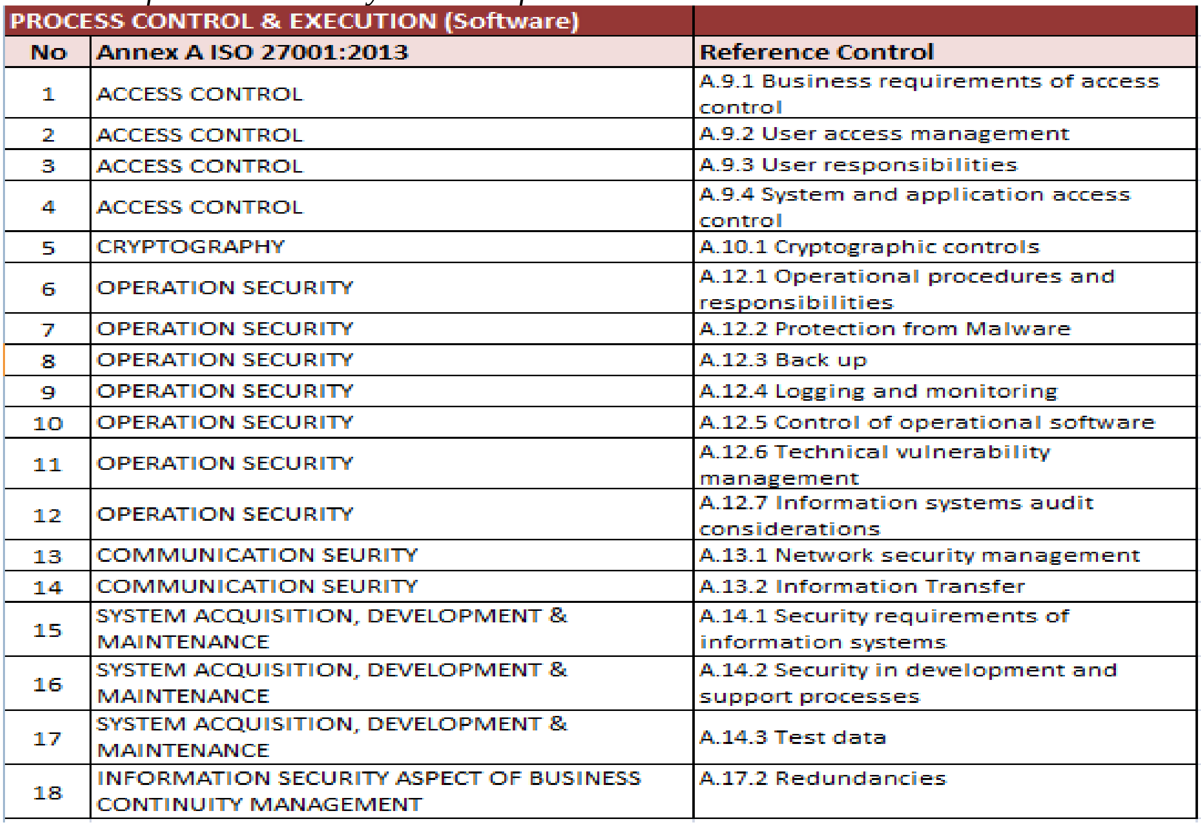


PROCESS CONTROL & EXECUTION (Hardware)		
No	Annex A ISO 27001:2013	Reference Control
1	ASSET MANAGEMENT	A.8.1 Responsibility of asset
2	ASSET MANAGEMENT	A.8.2.3 Handling of Asset
3	ASSET MANAGEMENT	A.8.3 Media handling
4	PHYSICAL ENVIRONMENTAL SECURITY	A.11.1 Secure Areas
5	PHYSICAL ENVIRONMENTAL SECURITY	A.11.2 Equipment
6	OPERATION SECURITY	A.12.1 Operational procedures and responsibilities
7	SYSTEM ACQUISITION, DEVELOPMENT & MAINTENANCE	A.14.2 Security in development and support processes
8	INFORMATION SECURITY ASPECT OF BUSINESS CONTINUITY MANAGEMENT	A.17.2 Redundancies

Software

This stage constitutes control planning that governs the information security of IT Infrastructure projects on software aspects.

Table.5. *Information security control software*

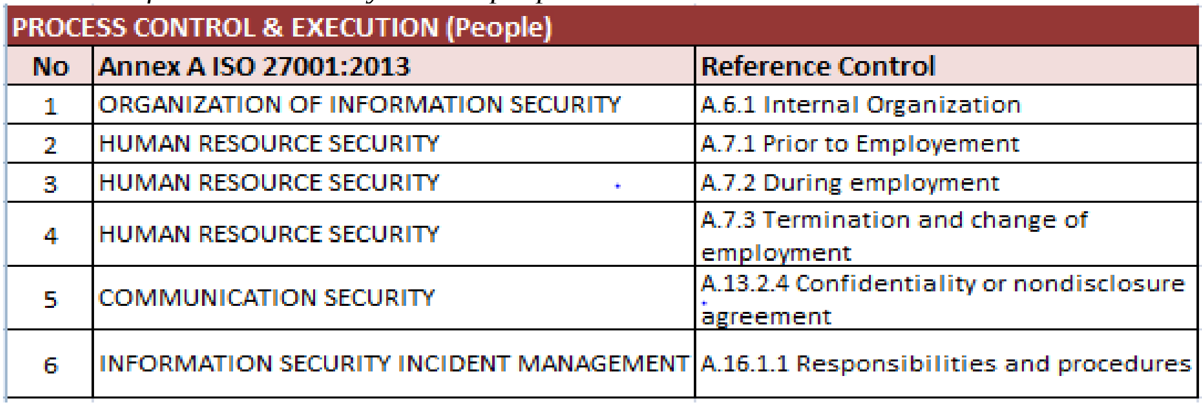


PROCESS CONTROL & EXECUTION (Software)		
No	Annex A ISO 27001:2013	Reference Control
1	ACCESS CONTROL	A.9.1 Business requirements of access control
2	ACCESS CONTROL	A.9.2 User access management
3	ACCESS CONTROL	A.9.3 User responsibilities
4	ACCESS CONTROL	A.9.4 System and application access control
5	CRYPTOGRAPHY	A.10.1 Cryptographic controls
6	OPERATION SECURITY	A.12.1 Operational procedures and responsibilities
7	OPERATION SECURITY	A.12.2 Protection from Malware
8	OPERATION SECURITY	A.12.3 Back up
9	OPERATION SECURITY	A.12.4 Logging and monitoring
10	OPERATION SECURITY	A.12.5 Control of operational software
11	OPERATION SECURITY	A.12.6 Technical vulnerability management
12	OPERATION SECURITY	A.12.7 Information systems audit considerations
13	COMMUNICATION SEURITY	A.13.1 Network security management
14	COMMUNICATION SEURITY	A.13.2 Information Transfer
15	SYSTEM ACQUISITION, DEVELOPMENT & MAINTENANCE	A.14.1 Security requirements of information systems
16	SYSTEM ACQUISITION, DEVELOPMENT & MAINTENANCE	A.14.2 Security in development and support processes
17	SYSTEM ACQUISITION, DEVELOPMENT & MAINTENANCE	A.14.3 Test data
18	INFORMATION SECURITY ASPECT OF BUSINESS CONTINUITY MANAGEMENT	A.17.2 Redundancies

Human Resources

This stage constitutes planning controllers that governs the information security of IT Infrastructure projects on aspects of IT project implementation infrastructure.

Table.6. *Information security control people*

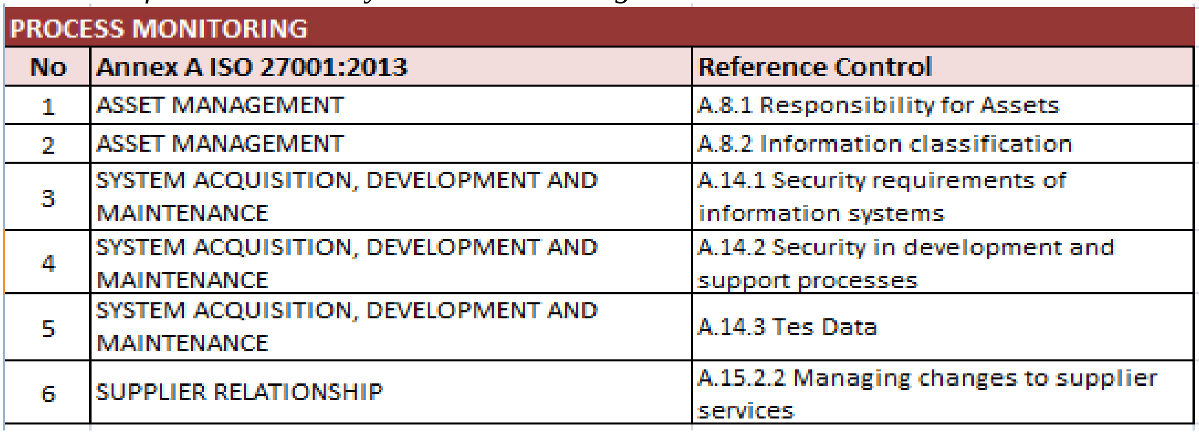


PROCESS CONTROL & EXECUTION (People)		
No	**Annex A ISO 27001:2013**	**Reference Control**
1	ORGANIZATION OF INFORMATION SECURITY	A.6.1 Internal Organization
2	HUMAN RESOURCE SECURITY	A.7.1 Prior to Employement
3	HUMAN RESOURCE SECURITY	A.7.2 During employment
4	HUMAN RESOURCE SECURITY	A.7.3 Termination and change of employment
5	COMMUNICATION SECURITY	A.13.2.4 Confidentiality or nondisclosure agreement
6	INFORMATION SECURITY INCIDENT MANAGEMENT	A.16.1.1 Responsibilities and procedures

Monitoring

At this stage, this represents a project monitoring process that includes preparation of project workmanship reporting documents, conducting a security checklist, and also verification against users and systems of those technologies.

Table.7. *Information security control monitoring*

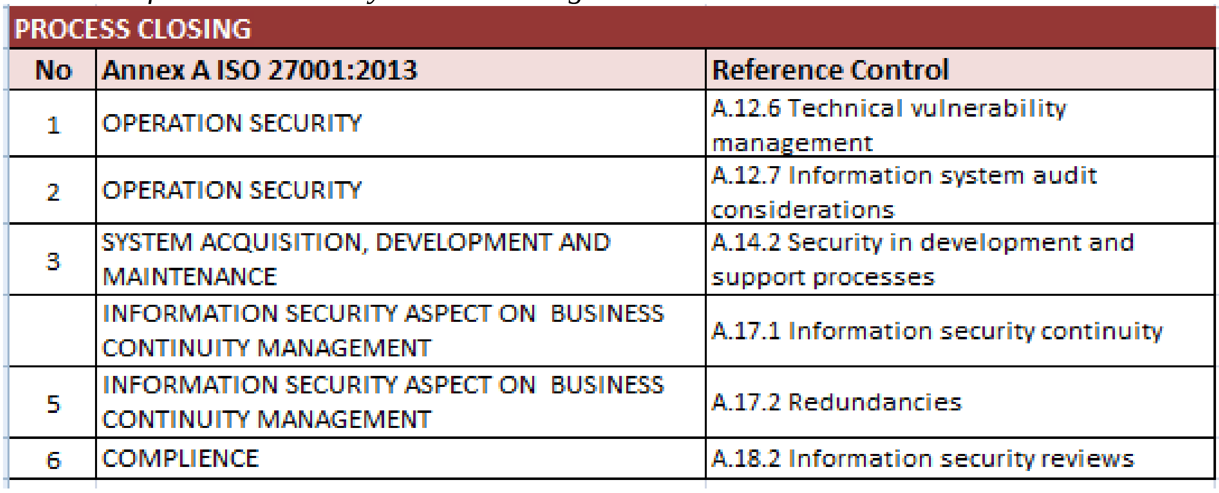


PROCESS MONITORING		
No	**Annex A ISO 27001:2013**	**Reference Control**
1	ASSET MANAGEMENT	A.8.1 Responsibility for Assets
2	ASSET MANAGEMENT	A.8.2 Information classification
3	SYSTEM ACQUISITION, DEVELOPMENT AND MAINTENANCE	A.14.1 Security requirements of information systems
4	SYSTEM ACQUISITION, DEVELOPMENT AND MAINTENANCE	A.14.2 Security in development and support processes
5	SYSTEM ACQUISITION, DEVELOPMENT AND MAINTENANCE	A.14.3 Tes Data
6	SUPPLIER RELATIONSHIP	A.15.2.2 Managing changes to supplier services

Closing

At this stage, this represents the process of closing and developing the project. For activities undertaken is to conduct regular evaluations interface projects already undertaken and then develop systems to sustain the pharmaceutical industry's business processes.

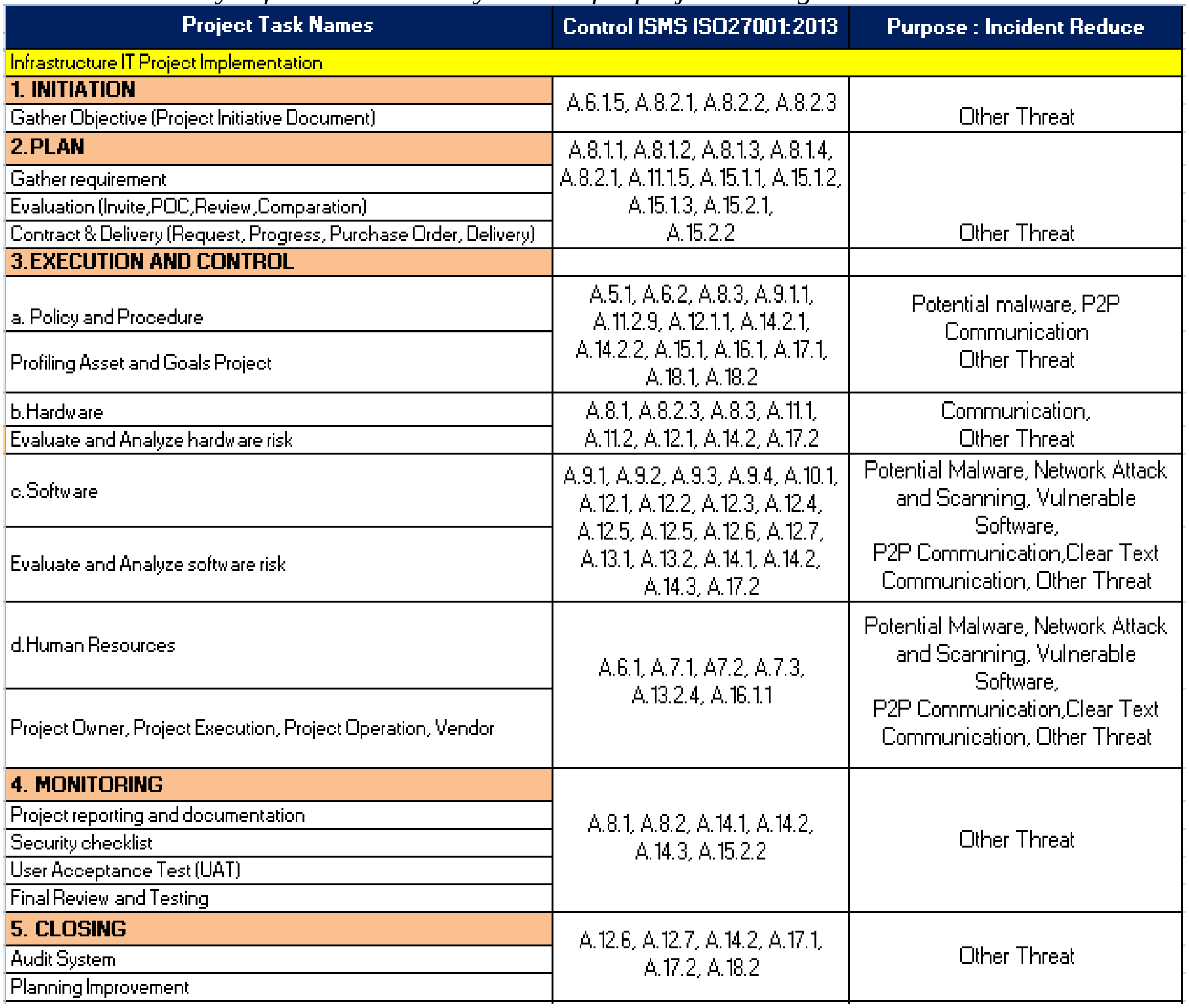
Table.8. *Information security control closing*



PROCESS CLOSING		
No	**Annex A ISO 27001:2013**	**Reference Control**
1	OPERATION SECURITY	A.12.6 Technical vulnerability management
2	OPERATION SECURITY	A.12.7 Information system audit considerations
3	SYSTEM ACQUISITION, DEVELOPMENT AND MAINTENANCE	A.14.2 Security in development and support processes
	INFORMATION SECURITY ASPECT ON BUSINESS CONTINUITY MANAGEMENT	A.17.1 Information security continuity
5	INFORMATION SECURITY ASPECT ON BUSINESS CONTINUITY MANAGEMENT	A.17.2 Redundancies
6	COMPLIENCE	A.18.2 Information security reviews

The following are control recommendations used in the IT Infrastructure project management process in the ISO27001:2013 based pharmaceutical industry in order to reduce incidents that have occurred and protect agains other threats in the future.

Table.9. *Summary Information security control for project management*



Project Task Names	Control ISMS ISO27001:2013	Purpose : Incident Reduce
Infrastructure IT Project Implementation		
1. INITIATION	A.6.1.5, A.8.2.1, A.8.2.2, A.8.2.3	Other Threat
Gather Objective (Project Initiative Document)		
2.PLAN	A.8.1.1, A.8.1.2, A.8.1.3, A.8.1.4, A.8.2.1, A.11.1.5, A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2	Other Threat
Gather requirement		
Evaluation (Invite,POC,Review,Comparation)		
Contract & Delivery (Request, Progress, Purchase Order, Delivery)		
3.EXECUTION AND CONTROL		
a. Policy and Procedure	A.5.1, A.6.2, A.8.3, A.9.1.1, A.11.2.9, A.12.1.1, A.14.2.1, A.14.2.2, A.15.1, A.16.1, A.17.1, A.18.1, A.18.2	Potential malware, P2P Communication Other Threat
Profiling Asset and Goals Project		
b.Hardware	A.8.1, A.8.2.3, A.8.3, A.11.1, A.11.2, A.12.1, A.14.2, A.17.2	Communication, Other Threat
Evaluate and Analyze hardware risk		
c.Software	A.9.1, A.9.2, A.9.3, A.9.4, A.10.1, A.12.1, A.12.2, A.12.3, A.12.4, A.12.5, A.12.5, A.12.6, A.12.7, A.13.1, A.13.2, A.14.1, A.14.2, A.14.3, A.17.2	Potential Malware, Network Attack and Scanning, Vulnerable Software, P2P Communication,Clear Text Communication, Other Threat
Evaluate and Analyze software risk		
d.Human Resources	A.6.1, A.7.1, A7.2, A.7.3, A.13.2.4, A.16.1.1	Potential Malware, Network Attack and Scanning, Vulnerable Software, P2P Communication,Clear Text Communication, Other Threat
Project Owner, Project Execution, Project Operation, Vendor		
4. MONITORING	A.8.1, A.8.2, A.14.1, A.14.2, A.14.3, A.15.2.2	Other Threat
Project reporting and documentation		
Security checklist		
User Acceptance Test (UAT)		
Final Review and Testing		
5. CLOSING	A.12.6, A.12.7, A.14.2, A.17.1, A.17.2, A.18.2	Other Threat
Audit System		
Planning Improvement		

Conclusion

Based on the hypothesis and planning on researching IT Infrastructure technology implementation projects in pharmaceutical industry areas using the ISO 27001:2013 approach, some conclusions can be drawn that could be interpreted as follows

1. Management of IT Infrastructure project management by applying security controls at process stages initiate, plan, control & Execution, Monitoring, and Closing is predicted to improve project management readiness to reduce incident future threats.
2. Utilization of ISO27001:2013 Annex A security controls on IT Infrastructure project management is predicted to sustain development to sustain business process continuity.
3. The application of information security controls to IT Infrastructure project management encourages the emergence of new policies related to project management.
4. Application of information security controls to IT Infrastructure project management can be references and guidelines for project workmanship as well as can be developed for subsequent research.

Reference

Achmadi,Dedy, Suryanto,Yohan, Ramli,Kalamullah "On Developing Information Security Management System (ISMS) Framework for ISO 27001-based Data Center"International Workshop on Big Data and Information Security (IWBIS) IEEE 2018

[Nurfitriani,Anita, Raharjo,Teguh, Hardian,Bob, Prasetyo,Adi "IT Infrastructure Agile Adoption for SD-WAN Project Implementation in Pharmaceutical Industry : Case Study of an Indonesian Company" International Conference IEMTRONICS 2021.

Alberch t, Jochen "GIS Project Management" Reference Module In Earth System and Environmental Sciences 2017.

Kordha,Ermelinda, Gorica,Klodiana, Ahmetaj,Lavdosh "Managing IT Infrastructure for Information Society Development. the Albanian Case"

Lundgre,Bjorn, Moller,Niklas "Defining Information Security" Science and Engineering Ethics 2019.

Al-Dhahri,Sahar, Al-Sarti,Manar, Abdaziz,Azrilah " Information Security Management System" International Journal of Computer Applications 2017.

Pretesh Biswas ISO 27001:2013 A.6.1.5 Information Security in Project Management, December 25, 2019.

C. Pelnekar, "Planning for and Implementing ISO 27001," ISACA Journal, vol. 4, no. 2011, pp. 1-8, 2011.

Iset.com, "www.iso27001security.com," Iset.com, 17 January 2017.

M. K. Harold F Tithon, Information Security Management Handbook, FL: Auerbach, 2006.