Student Name Course	Vijayendra Rathod [Information Governance]
Student Number	W18034251
Tutors	Hamid
Word Count of Report	

Information governance policy

Information governance policy for the Aris pharmaceutical

1. Introduction

1.1 Aris pharmaceutical LTD established in 2007, and it is one of the quickest developing organizations inside the ongoing and intense classifications of the Branded Formulations market, for example, cardiovascular; against diabetes; nutrients; gastroenterology and gynaecology. The organization essential spotlight has been on creating, manufacturing, and marketing items which are connected to a way of life-related problems that are ongoing and are treated by the doctors

2. The intention of the Policy

2.1. This policy intends to process the information securely in every aspect, whether company dealing with the third party, child company, vendor, doctor, patient, medical council or an employee, Business require certain security framework or standard, that management can follow and achieve the primary goal preserve sensitive information leakage, and Company also want to enforce the role and responsibilities as well as define a boundary around the role to defend the critical information

3. Scope of the policy

3.1 The company adopts the hybrid approach while dealing with information hence some core system are developed by in house software development team while other systems are purchased by the well-established market leader vendor and some are placed in the cloud platform although some the system produce in-house there are numerous changes are done periodically to align the system according to the business requirement which might impact on the business continuity hence company also want to build the method around it which can improve the system availability

4. The Policy Objectives

To Prevent any unfavourable outcome associated with information, the company need to execute confidentiality integrity, and availability in their day to day practices, while dealing with a client, vendor, patients, child company or an employee

I. Define policy and procedure for reducing any risk pro-actively from internal and external threats

II. apply appropriate digital trust using a certain system in the various process which is executed by employee and client

III. Define accountability according to the various job function and distribute the responsibilities and decide the boundary related to that specific role

IV. Define the Policy structure by consulting and informing various compliance procedure among various department and enforce the responsibility, accountability around it

V. Build the security culture and strategy which will be adapted by the staff

VI. Securely store the previous year data for legal and compliance purpose and discard non-usable information after some year

VII. Assess the market pressure and priorities business expectation as well as provide timely support using the latest technological trends

VIII. Ensure the staff are periodically trained to maintain the security posture for the organization. And, cautious enough to prevent information leakage either from the vendor or from customer

IX. Restrict the change and execution of documented process without prior authoritative approval

X. Accept the Feedback from the executive team and adjust policy to create the advanced version of governance policy

5. Policy framework

5.4 Organize training and create awareness among the employees to create information security environment in the organization by exercising the security practices, assist the employees for the best practices by coordinating with HR process, and make them aware about employee termination procedure if they do not follow a suitable guideline

5.2 Roles and Responsibilities – The board has concluded that Roles and duties are to be allocated depending on the regions of work that staff are answerable for. Staff will be urged to raise Information Governance issues and concerns both according to our inhouse frameworks and frameworks possessed by customers, so it is reassuring a positive IG culture

5.3 SWOT Analysis: Determine the Organization internal and External factors and based on that assess organization strength, weakness, and upcoming opportunity and threats and decide the organization future goal and policy accordingly

5.4 Gap Analysis: Identifying the existing process and its outcome and decide the desired outcome that the organization want to achieve by fixing the gap in the current documentation procedure

6. Associated policies and practices

6.1 This policy is backed by a wide-ranging set of policies and processes including

Information Security policy and methods

- Entrance Control policy and practices
- Personnel Security policy and procedures
- Physical and Environmental Information Security policy and procedures
- Incident Management and response policy and procedures
- Business Continuity and Disaster Recovery policy and procedures
- Asset Managing policy and Equipment Clearance policy and procedures
- Code of Conduct and Accepted use policy and procedures
- Policy and Practices for the data at rest, data in transit
- maintaining digital assets and data handling method
- Remote access policy
- Email policy
- Data Secrecy policy
- Mobile Application Deployment Policies
- Mobile Device policy
- Application Security
- HR Policy

6.2 This arrangement must be executed as per the supporting approaches and strategies as they determine best methodology and guidelines, which are intended to limit risk, stay away from falls, and promote reliability

7. Monitoring, measurement, and review mechanisms

7.1 The organization will occasionally audit the propriety of all organization strategies. Any new threats which capable to disrupt the organization's strategies and methods will be modified to alleviate those risk

8. Compliance

8.1 Any Company Employee violates the rule and regulations, then the company may take disciplinary action on them,

9. Approval

Any emergency changes in information governance policy either from internal or external factors may require approval from the board of directors before it Applicable to Organization

Information Governance policy Report

Contents

1. Information about company in-terms of policy perspective

The company has been pro-actively working with doctors to improve the quality of drugs by considering the patient feedback. It has been noticed that multiple bodies such doctor, patient, employee, medical council, manufacturing and sales department, third party, and child company are dealing with critical information in their daily routine hence it is vital that company should implement information governance policy, which will channelize the flow of information from authorities towards the end customer so it can preserve the Confidentially, integrity and authenticity of the information. Hence. The company want governance policy which will build relationship and trust among the people and process in longer terms

The organization must work its business in a manner that mitigates hazard and guarantees administrative consistency with regulatory compliance. The association must establish an environment where critical information can be exchange securely to other entity, particularly governments, and merchants. As a significant part of the information is being exchanged using technology, hence gracefully monitoring strategies may need to develop or set up to track critical information leakage.

The biggest challenge and concerned for the pharma industry such as Intellectual Property related protection. This covers Protection (Prakash et al., 2018)of formulas, contracts and pricing, clinical research, third party contract and PII related information. Then there is risk & compliance, IoT and cloud usage, supply chain eco-system security and clinical trial data security.

2. Executive Summary

The Aris Pharmaceutical actively manufacturing medicine for different diseases and also build various mobile applications platform for doctor and patient engagement which will help them to assess the current demand of the drugs and as well as they can probably estimate, how drugs respond to patient disease by evaluating doctor feedback and based on that response company can improvise the Drugs

On an Average around, ten thousand IOS device and five thousand Android devices with eleven different application are deployed to build the patient engagement in various category. And Most of the Applications are Build by the In-house software development which is a third-party company hired by the organization to develop and customize the application according to companies and doctor’s requirement

Nearly About, eighty per cent of the Business process is run on the customize software especially finance and MIS System and that also has change management element due to business demands, and rest of the system such as email server, travelling and ticket booking system is run in the cloud platform. The Remote Desktop server and Active Directory setup are configured for the employee as well as for vendor to generate an order in the system. Hence the remote desktop functionality plays a major role in dealing with supply chain execution.

2.1. Introduction and structure of the report

The organization need to develop the information security strategy, based on practical idea and concepts of how security should look like for an organization and need to assess the external influencers that can affect governance function. The ideal security strategy is the establishment of the vision used to drive to develop the security program .the Policymaker will assess the organization with every policy method and back them up with supportive reference as well as regulatory guideline

Once, the organization decide the roadmaps to achieve the information security goal, then policymaker also provide the estimated timeframe and expense to achieve it

2.2. Why business should adapt and execute the policy

The Intellectual property such as trademark (India Code, 1999) , drug formula, brand name, slogan, research and analytics information and patent (IPIndia.gov.in, 1970) are needed to register under specific legislative authorities And need to follow the rule and regulation under (THE DRUGS AND COSMETICS ACT, 1940) the Organization want to Proactively assess the future threat that may affect under (ISO/IEC 27005, 2018) the realization of strategies such as timing, resource constraints, supply chain, and financial challenges. So, they can develop Information governances design which is a customizable, flexible, and consistent framework which can be re-align according to the business requirement without disrupting any other process

2.3 The Goal of Information Governance policy and its objective

The Company want to inherit information governance policy by bringing awareness into employee through various training program about information security (ISO/IEC 27000, 2018) however successful information governance cannot be done by exercising single control. the organization has to define the role and responsibilities (ISO/IEC 27000, 2018) for company top executive, who are actively dealing with critical information in their daily routine .moreover every opportunity in the organization has certain risk associated with it and that need to identify and assess the consequence and likelihood of it, if they triggered (ISO/IEC 27005, 2018) hence risk should be captured, monitor and conveyed to the top management to develop a risk mitigation plan

It is essential for the organization to (ISO 15489-1, 2016) keep the information record for the past year for compliance and legislative purpose .and if the information asked by the government or auditor they can provide it, however keeping record and providing it to authority is not enough they need to protect (ISO 15489-1, 2016) the record from unauthorized access, alteration, concealment or destruction from insider and outsider threats

The carrying and forwarding agent extensively using (ISO/IEC 27002, 2013) company remote server for invoice booking hence organization want to suggest secure and standardise a way to access those resource. The organization continuously monitoring and measuring current infrastructure want to embrace newer technology trend to stay ahead from their competitor (ISO/IEC 27003, 2017) so organization can reduce the business disruption and promote business continuity using redundancy plan (ISO/IEC 22301-2019, 2019) which maximize the business value in terms of profits and creditability

the top areas of IG are

1. Record and Information management
2. Application Security
3. Data Handling and Storage retention
4. Risk management
5. Cloud Security
6. Business Continuity
7. Remote Desktop
8. HR security
9. Access Control
10. Asset monitoring and Security

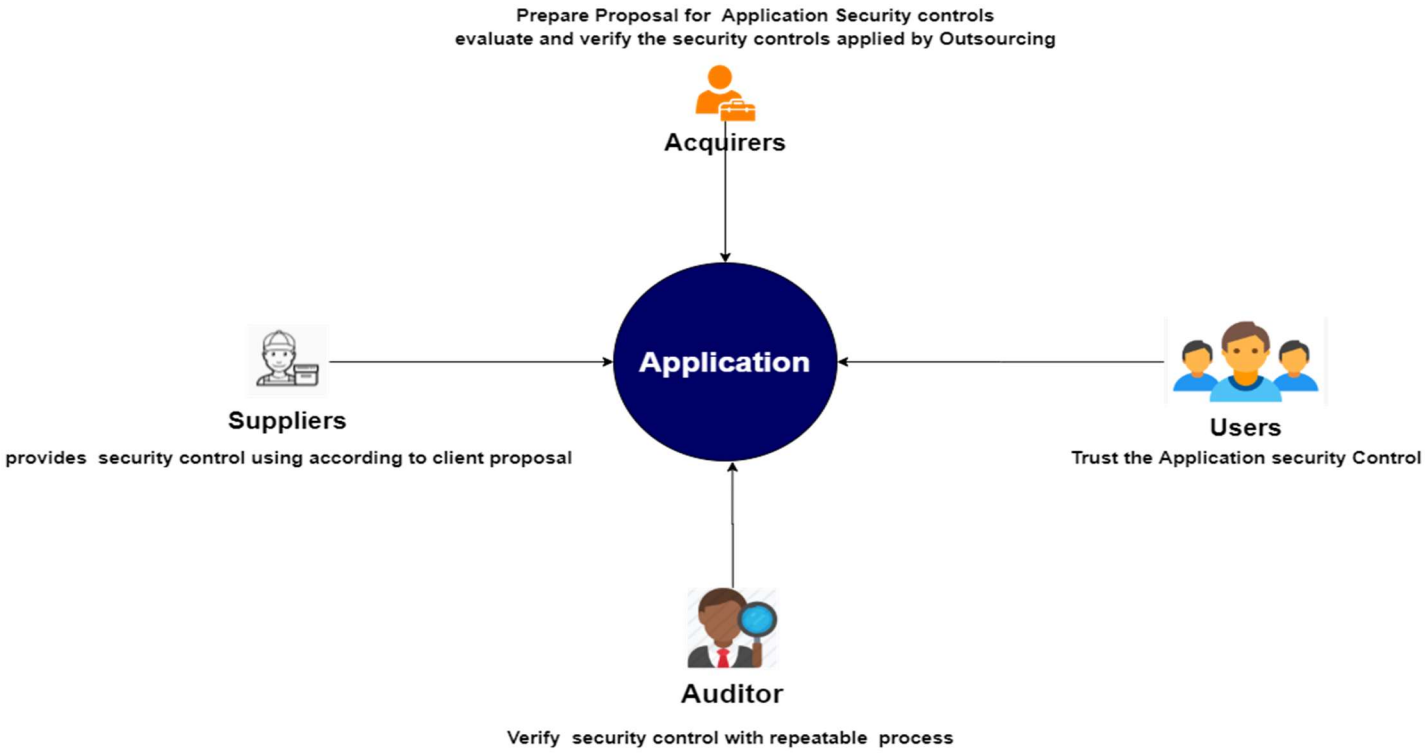
In the upcoming section, each policy is justified with appropriate ISO standards

3. Analysis of policy elements

Policy 1.1 The Company rely heavily on third party vendor for application development and deployment. Hence the information governance related to application security and deployment need to express using suitable document guideline .so the associate data and system are being protected from any unfavourable incident

Analysis of 1.1 Application security is based on the continuous process between acquirers, supplier, user, and auditor and that can be further understood by below mention figure

The Graphical Explanation inspired by the (ISO/IEC 27034-1, 2011)

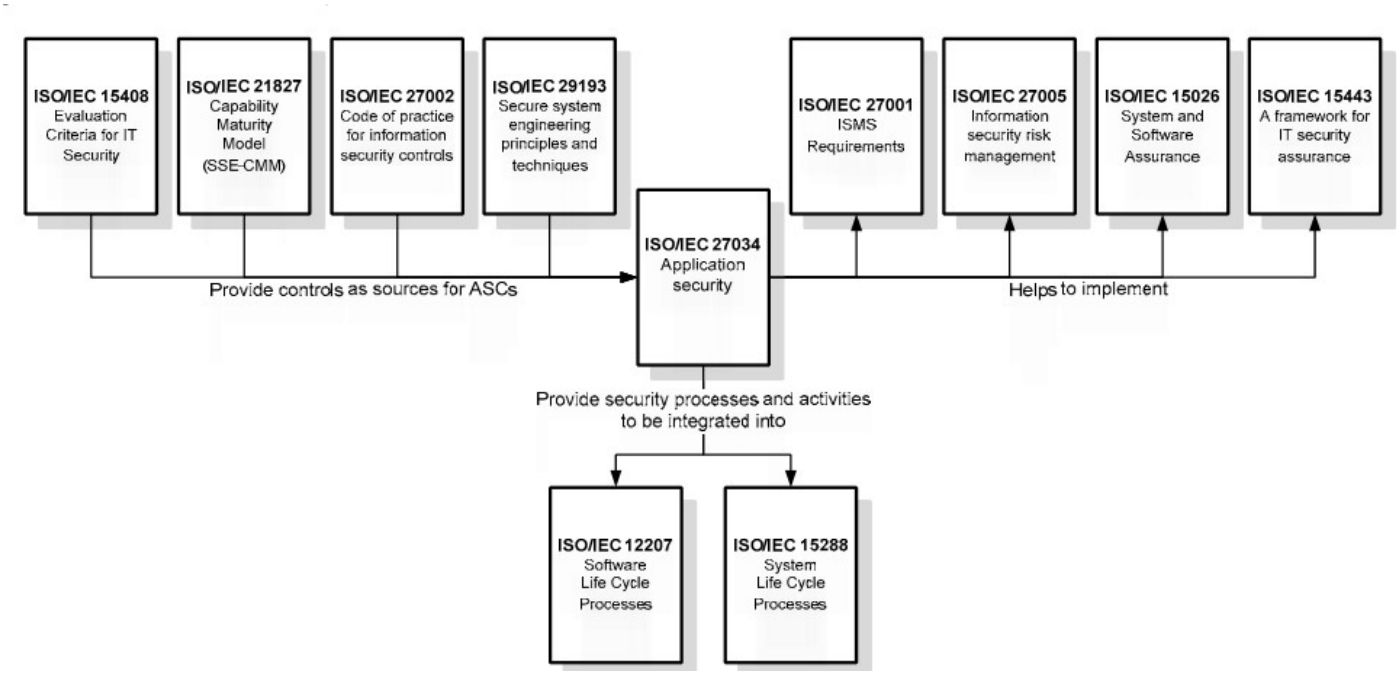


Application security Risk Domain

(ISO/IEC 27034-1, 2011)

1. **Business Risk**: the risk related to the Organization process and function
2. **Regulatory Risk**: specific risk arising from intellectual property rights, laws and regulation, rights and licensing, restriction on cryptographic protection
3. **Technological risk**: specific risk from the technology used by the organization such as reverse engineering, pen testing, code checking, operating system privilege, maintenance and secure distribution

Application security and its Relationship to other ISO standards



PDCA Cycle for Information Security

(ISO/IEC 27001, 2013)

Plan: prevent, reduce undesired effects, and achieve the continual improvement as well as evaluate the effectiveness of the actions

Do: Identify, analyse, evaluate Information security risk

Check: Compare the analysed risk with risk criteria

Act: Develop the Risk treatment Plan and communicate with risk owners

Application security using Code of practice under (ISO/IEC 27002, 2013)

ISO/IEC 27002 provides practices that an organization can implement as Application Security Controls as proposed by ISO/IEC 27034. Of utmost interest are controlled from the following clauses in ISO/IEC 27002:2013:

Clause 9 Access control:

The assets owners determine the appropriate access control rules, access rights and restriction for specific user roles towards their assets .the access (ISO/IEC 27002, 2013) control on physical and logical assets should be conveyed to the user and service providers to achieve the goal of it

Policy under Access control

- Segregation of access control roles, authorization, and administration
- Periodically review and remove the access control rights
- Network and network service authorization procedure and determine who allowed accessing what
- User registration, management, provisioning and determining the user responsibilities around it
- Secure the log-on procedure and implement a stronger password management system

Clause 12 Operational Security

The operation procedure should be documented, and change management should be executed to fine-tune the organization current resources or to (ISO/IEC 27002, 2013) predict the future requirement. The assets should be protected from the malware by scheduling information backup and appropriate log and event should be captured for incident management

Clause 13 Communication Security

- The network and network service should be segregated according to department
- Confidentiality or non-disclosure agreement for external vendor and employee to protect the confidential information

Clause 14 System Acquisition and Development

The application transaction should be protected from alteration, misrouting and disclosure by integrating digital certificate trust authority platform

- Secure the version control. repositories
- Security and guidance for software development life cycle
- Store the application development backup at an off-site location

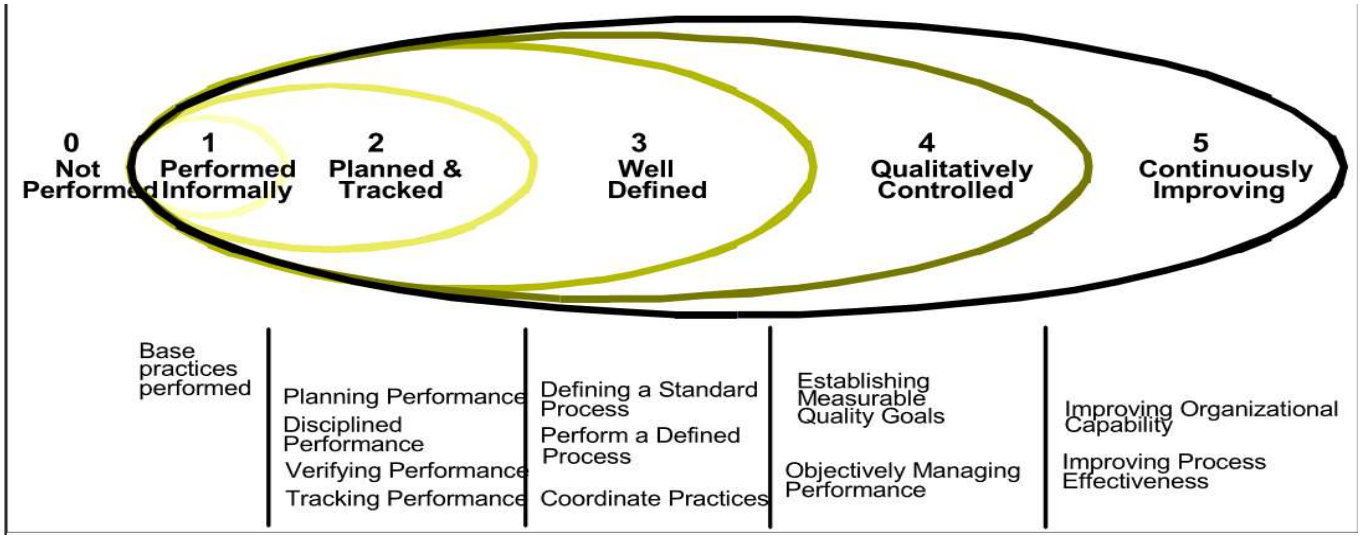
Application security risk Under ISO 27005 Annex C (ISO/IEC 27005, 2018)

- Theft of media, equipment, documents
- Remote spying, eavesdropping
- Retrieval of data form recycled or discarded media

System Security Engineering -Capabilities maturity model

ISO/IEC 21827 provides security engineering base practices that an organization can implement as Application Security Controls as proposed by ISO/IEC 27034. Also, processes from ISO/IEC 27034 help to attain several of the capabilities that define the capability levels in ISO/IEC 21827

Capability levels represent the maturity of security engineering organizations (ISO/IEC 21827, 2008)



The Systems Security Engineering Capability Maturity Model® (SSE-CMM®) capture best practice for Application Security under ISO Standards (ISO/IEC 21827, 2020) and provide characteristics for Application maturity. And according to standards the entire life cycle, including development, operation, maintenance, and decommissioning activities are need to assess as well as concurrent interactions with other disciplines, such as system, software, hardware, human factors, and test engineering; system management, operation, and maintenance need to consider to create a mature application security

5. Policy Framework

5.1 Role and responsibilities

The effective governance policy cannot be implemented without defining role and responsibilities across the organization, A role is assigned to an individual (iSACA CISM, n.d.) person who is performing the job function and who are accountable and Responsible enough to perform a critical function according to the access rights given to them

Cobit 2019 Role and Responsibilities According to Various business function phases

- **Program management** (outer ring)
- **Change enablement** (middle ring)
- **Continual improvement life cycle** (inner ring)

Phase 1 : RACI Chart

Key Activities	Board	I&T Governance Board	CIO	Business Executive	IT Managers	IT Process Owners	IT Audit	Risk and Compliance	Program Steering
	Responsibilities of Implementation Role Players								
Identify issues triggering need to act (CI1).	C/I	A	R	R	C	C	C	C	R
Identify business priorities and strategies affecting IT (CI3).	C	A	R	R	C	C	C	C	R
Gain management agreement to act and obtain executive sponsorship (CI7).	C	A/R	R	C	I	I	I	I	R
Instill the appropriate level of urgency to change (CE10).	I	A	R	R	C	C	C	C	R
Produce convincing outline business case (PM3).	I	A	R	C	C	C	C	C	R

A **RACI** chart identifies who is **R**esponsible, **A**ccountable, **C**onsulted and/or **I**nformed.

The **RACI** is an acronym stands for [**Responsible, accountable, Consulted, and Informed**]can be utilized to allocate the role and responsibilities to the individual however that can be better understand by assessing (ISACA Cobit, 2019) phase-wise RACI Model, as role and responsibilities are changed according to various phase. The role and responsibilities can also be segregated under (ISO/IEC 27001, 2013) however the Cobit 2019 Model brings more clarity in terms of role and responsibilities distribution

5.2 Code of Practice

The documentation procedure should be developed for the operational activities associated with information processing such as (ISO/IEC 27002:2013, n.d.)backup, media handling, installation and configuration of software settings hence the operational staff can relate these documentation norms in their daily activities. And improve overall information security process

5.3 Support

The resource, such as financial and infrastructure need to align for the better outcome of Information governance .however the only resource is not capable to deliver governance, the people with the correct mindset and adequate skillset also require (ISO /IEC 27013, n.d.) so the organization can achieve their intended goal. Although they are enough competence to deliver the performance still there is the scope of improvement hence their skills should be evaluated according to organization expectations, and the knowledge gap in the current skillset should be improvised through training and awareness

5.4 Compliance

The manager should periodically review the compliance information processing and procedure within the area of the responsibilities with appropriate security policies standards and any other security requirements

5.5 Performance Evaluation

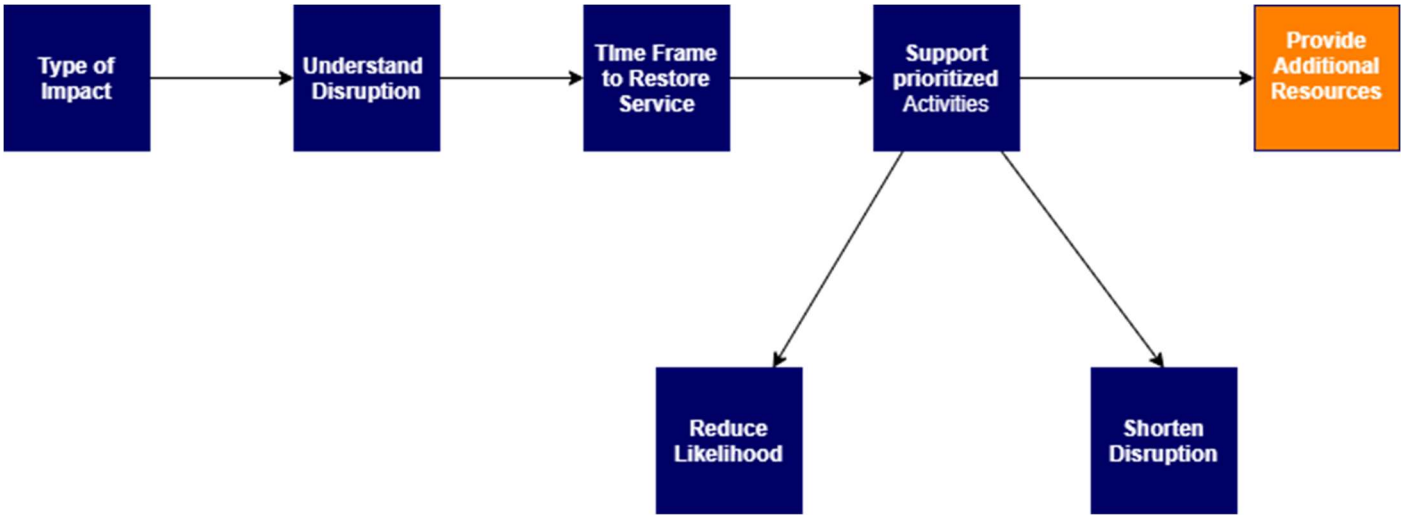
The Organization evaluates the information security performance and the effectiveness of policies by monitoring various system, process, or activity run by internal staff, and this information can use as a measurement parameter to determine the (ISO/IEC 27003 2017, n.d.)level of success that organization achieved during certain time frame however if there is knowledge gap identifies in the process then that process can be reviewed and analysed by the CISO then that process and norms are amended into governance policy for the better outcome of Information security

6. Summary

The Aris Pharmaceutical actively working in drug manufacturing segment and closely monitoring the doctor and patient engagement using the various digital platform since 2007. they also want to be competitive in the market in terms of drug supply chain and they strongly required the business continuity for their drug booking system. So, they can enhance their sales growth

The Company has tie-up with more than two thousand CFA [carry and forwarding Agent] to Distribute their drug in different geographical location of the country, hence, CFA required to access the company ERP system over the internet for Order booking.so Company also need to provide a secure, fast and reliable medium to access the company server .and they also need to make sure the all server has some redundancy, so in case of disruption faced by infrastructure, redundant set-up still serve the business process

The business continuity can be Established for various technological disruption Under ISO (ISO/IEC 22301-2019, 2019) by below mention activities



7. Recommendations

Human security :

The HR department should define the minimum level of verification checks to be applied to the future candidate before hiring, so people (ISO/IEC 27010:2015, n.d.) with the correct mindset and intention are taken part to achieve information governance goal

Asset management:

The various software, document, certificate, and hardware (ISO/IEC 27010:2015, n.d.) assets of the company need to record under asset inventory then afterwards ownership for these assets should be mapped to the person who possesses those assets .however the only accounting and mapping assets to a person does not solve the problem, the assets should be a monitor for acceptable use of it

Incident management

The unfavourable incident that may occur beyond the scope of Information security policy is somehow inevitable hence the incident management pl (ISO/IEC 27035-2:2016, n.d.)an need to develop which will mitigate with, virus, worms, ransomware, information theft and provide a properly documented guideline, which will improvise the process to handle such critical events

Network Security

The Networks are the entry gate for the hacker, from where they can exploit the various system vulnerabilities using malicious code hence there should IDS/I (ISO/IEC 27039:2015, n.d.)PS system need to configure in the hardware-based firewall for the central point filtration and endpoint IDS for the Client end so the organization IT Infrastructure can be prevented from such type of malicious attack

Storage Security

The data is the core element and heart in the information security, so whatever the data store in the form of a block, object,file-based form in a various appliance such as (ISO/IEC 27040:2015, n.d.)NAS and SAN need to protect using proper authentication, authorization, and accounting mechanism, additionally information confidentiality and retention can be preserved respectively using encryption and backup procedure

8. Conclusion

The Aris Pharmaceutical need to implement the relevant control and the procedure from ISO 27001;2013 and its family standards to achieve minimum baseline for the cyber secure infrastructure, additionally, they can refer to ISO 22301 for the business continuity and mitigate the security flaws and event with cybersecurity framework (NIST, 2018)

The procedure and the control defined under the policies need to convey through top management to the executive level, so the organization effectively monitor and measure policy condition, furthermore, they can distinguish between the desired and current state of information governance and re-align the norms and introduce the advance version of policies

References

India Code, 1999. *THE TRADE MARKS ACT, 1999.* [Online]
Available at: https://www.indiacode.nic.in/bitstream/123456789/1993/1/A1999_47.pdf
[Accessed 12 11 2020].

IPIndia.gov.in, 1970. *THE PATENTS ACT, 1970.* [Online]
Available at: http://www.ipindia.nic.in/writereaddata/Portal/IPOAct/1_31_1_patent-act-1970-11march2015.pdf
[Accessed 12 11 2020].

iSACA CISM, n.d. *CISM Review Manual.* fifteen ed. s.l.:s.n.

ISACA Cobit, 2019. *COBIT®2019 Implementation Guide: Implementing and Optimizing an Information.* s.l.:ISACA.

ISO /IEC 27013, n.d. *Information technology — Security techniques — Information security management systems — Guidance.* Second Edition ed. s.l.:s.n.

ISO 15489-1, 2016. *Information and documentation — Records management.* Second Edition ed. s.l.:ISO.

ISO/IEC 27003, 2017. Information technology — Security techniques. In: *Information technology — Security techniques.* s.l.:ISO.

ISO/IEC 21827, 2008. *Information technology — Security techniques — Systems Security Engineering — Capability Maturity Model® (SSE-CMM®).* Second Edition ed. s.l.:ISO.

ISO/IEC 21827, 2020. *Information technology — Security techniques — Systems Security Engineering — Capability Maturity Model® (SSE-CMM®).* Second ed. s.l.:ISO/IEC.

ISO/IEC 22301-2019, 2019. *Security and resilience — Business continuity management systems — Requirements.* Second ed. s.l.:ISO .

ISO/IEC 27000, 2018. *Information technology — Security.* Second Editon ed. s.l.:ISO.

ISO/IEC 27001, 2013. *Information technology — Security techniques — Information security management systems — Requirements.* 2nd ed. s.l.:ISO.

ISO/IEC 27002:2013, n.d. *Information technology — Security techniques — Code of practice for information security controls.* s.l.:s.n.

ISO/IEC 27002, 2013. *Information technology — Security techniques — Code of practice for information security controls.* third ed. s.l.:ISO.

ISO/IEC 27003 2017, n.d. *Information technology — Security techniques — Information security management systems — Guidance.* s.l.:s.n.

ISO/IEC 27005, 2018. *Information technology Information security risk management.* Third ed. s.l.:ISO.

ISO/IEC 27010:2015, n.d. *Security techniques — Information security management for inter-sector and inter-organizational communications.* s.l.:s.n.

ISO/IEC 27034-1, 2011. *Information technology — Security techniques — Application security.* First ed. s.l.:ISO.

ISO/IEC 27035-2:2016, n.d. *Information technology — Security techniques — Information security incident management — Part 2: Guidelines to plan and prepare for incident response.* s.l.:s.n.

ISO/IEC 27039:2015, n.d. *Information technology — Security techniques — Selection, deployment and operations of intrusion detection and prevention systems (IDPs).* s.l.:s.n.

ISO/IEC 27040:2015, n.d. *Information technology — Security techniques — Storage security.* s.l.:s.n.

ISO/IEC 27040, 2015. *Information technology — Security techniques — Storage security.* fist ed. s.l.:s.n.

NIST, 2018. *Framework for Improving Cybersecurity.* [Online].

THE DRUGS AND COSMETICS ACT, 1940. *THE DRUGS AND COSMETICS ACT*. [Online]
Available at: http://legislative.gov.in/sites/default/files/A1940-23.pdf
[Accessed 2020].