# Information Security Management Requirments Model Through Data Life Cycle

**Dr.Musbah Abobaker Musbah**
Computer science, Faculty of education
Aljufra University

*Abstract-* **information security management model through the data life cycle is a model that can help us to follow and understand the strategy life of the institution and determining all probabilities of threats and vulnerabilities of occurrence and outcomes through implementing it within the institution. The data life cycle has been chosen that the data life cycle management enables us to understand our data, which is an extremely valuable business asset and which must be managed properly, to ensure business success and regulatory compliance. Understanding data life cycle management means to classify and determine rules, responsibilities and IT needed and determine the requirement to business targets done in the best way, here we can say that it is the way to find out the weakness in the data process and helping us to determine security technical requirement and provide the security policy.**

*Index Terms:* **Software Development Life Cycle, Project management, Perform feasibility. Business Scenario, Threats, Audit, Plan, security policy, Authentication, Authorization, Access Control.**

## I. INTRODUCTION

At a time when there were many Data Breakthroughs in institutions, companies and organizations, the trend to secure and protect data and strategies grow to be large well. and since the process of protection and access to it was a very expensive and depend on the reliability of providers of technology protection and which they are mostly companies and people from outside the institution.

Technical and protection companies depended on international data protection standards such as ITIL, Britch Standard, and other international standards which are themselves Experiments of the companies for long periods and solutions that have been taken through it and which economic success.

There are still some gaps that can represent points of breach of protection such as the factor of confidence in the provider or contractor and employees in addition to the application of the global standard used on the status of the institution in terms of structure, strategy, and privacy. where each private institution distinguished from the rest of the institutions. where the result of The implementation differs from one institution to another, and we do not forget the high cost of applying for protection.

Received 30 Nov, 2019; revised 24 Nov, 2019; accepted 4 Dec, 2019.

Available online Dec 6, 2019.

Hence it was necessary to find a way to address these gaps and defects and reduce the cost.

To achieve this, we need to understand and know all about the organization's data processing strategies to determine the requirements.

From here exactly, I have been able to develop a management model depending on data life cycle to generate and define the protection policy and technical requirements needed to apply in the institution and within the institution "in detail by size", depending on the specificity of the institution and through the. Company's data life cycle DLC. This paper including a detailed explanation of the model.

## II. INFORMATION SECURITY MANAGEMENT MODEL

Each stage in the life cycle should be done by a human through technology follows the business strategy; avoiding risk occurs. [10]

The following figure 1 shows my model of security management which I will be displayed.

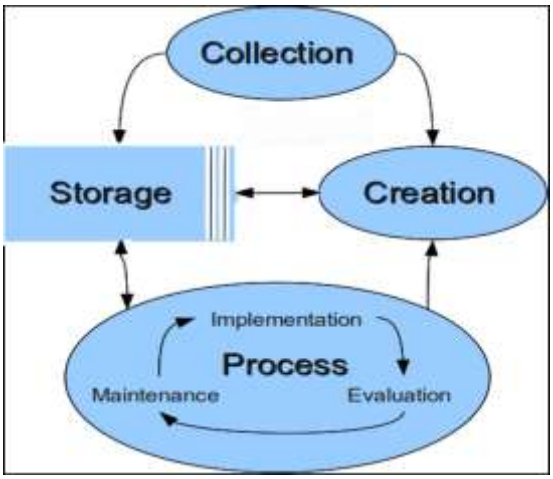


Figure 1. Security Management from DLC Perspective(author)

It is a collection of some activities which have to be followed to achieve the organization's security; also as we will see each activity has sub-process ends with reports collected in a storage unit to be used in other activities to build the organization security base. The following table1 includes the activity with simple identification and description

*a. Collection Process*

This activity includes subprocess in, Finding out specific data which are organization management structure, outline the scenario of business's process and find out probabilities of threats and vulnerabilities of occurrence and outcomes, these specific data can be done through constructing teamwork from three experts and their duty are to consulting the responsible people from the organization to discuss and collect displayed request, and this process ends with specific reports which have a value.

Table 1. Process Activities and Definitions(author)

| Activity | Description |
|---|---|
| collection | include sub-process to analyze and collect different information related to the goals and ends with reports |
| creation | include also sub-process to create a security plan and ends also with specific reports |
| process | also, subprocess to put the plan created in action and ends with specific reports |

*1. Organization Management*

In this process, the expert will meet and consult the top manager and the department's managers of the organization about the relation between the top manager and the department also the relation between the department's managers and their employees, then formulate the data in a graphical way. Either they have to prepare a Questionnaire related to security management that the managers have to answer. That to get information about security management situation, identity management, security policy, and change security management in the organization

*2. The scenario of Business Process*

In this process, the expert will flow the organization's data process of production from the beginning to ends and register each change on data and by what and who, in the end, he has to formulate the scenario diagram by using any case tools for example UML. That will give information about tools and rules used to create goods or services, from technical used hardware and software, also shows communication from inside and outside the organization. [11]

*3. . Threats and Probability Occurrence and Outcomes*

The expert should analyze through scenarios the probability of different threat agents causing damage. These scenarios should consider the organization's business strategy, quality of its control environment, and its own experience, or the experience of other institutions and entities, concerning information security failures. The assignment of probabilities by the organization should be appropriate for the size and complexity of the institution. Simple approaches (e.g., probable, highly possible, Possible, and unlikely) are generally sufficient for smaller, non-complex institutions.

The expert prepares two kinds of Questionnaires for employees and managers, one related to application security, network security, and system security. And the second to determine the level through the most four damages type can occur in Areas of vulnerability (Personnel, Facilities and equipment, Applications, Communications, Software, and operating systems):

- Unauthorized disclosure, modification, or destruction of information
- Inadvertent modification or destruction of information
- Non-delivery or miss-delivery of service
- Denial or degradation of service

*b. Creation Process*

As before this activity has a subprocess to outlines the specific requirements and rules that have to be met to implement security management and ends with a policy statement also determine the technical requirements from soft and hard and The general formulated goals are specified in operational level agreements. These agreements can be seen as security Plans for specific organizational units.

*c. Processes*

The processing activity has three sub-activities implementation, evaluation, and maintenance of the plan created in the last stage in the operating agreement. [12], Table 2 includes a description of the processing activity.

Table 2. description of the processing activity(author)

| Activities | Sub-activities | Descriptions |
|---|---|---|
| process | implementation | This process to put the operating agreement in action. |
| | evaluation | this process to audit and control the result of action to evaluate the security level |
| | maintenance | this point to reconstruct and create the operational plan |

*1. Implementation*

In this process, there is a subprocess summarized in classifying and managing applications, implement personal security, security management, access control, and reporting.

*1.1. Classifying and Managing Applications*

Process of formally grouping configuration items by type, software, hardware, documentation, environment, application Process of formally identifying changes by type e.g., project scope change request, validation change request, infrastructure change request this process leads to asset classification and control documents. [13]

*1.2. Implement Personal Security*

Here measures are adopted to give personnel safety and confidence and measures to prevent a crime/fraud. The process ends with personnel security.

*1.3. Security Management*

In this process, specific security requirements and/or security rules that must be met are outlined and documented. The process ends with security policies. [2]

*1.4. Access Control*

In this process, specific access security requirements and/or access security rules that must be met are outlined and documented. The process ends with access control. [2]

*2. Evaluation*

In this process starts with an examination of the implemented processes by a sub-process in:

*2.1. Self-Assessments.*

In this process, an examination of the implemented security agreements is done by the organization of the process itself. The result of this process is self-assessment documents.

*2.2. Internal Audit.*

In this process, an examination of the implemented security agreements is done by an internal Electronic Data Process EDP auditor. The result of this process is the Internal Audit statement.

*2.3. External Audit*

In this process, an examination of the implemented security agreements is done by an external Electronic Data Process EDP auditor. The result of this process is the External audit statement.

Evaluation Based on Security Incidents

In this process, an examination of the implemented security agreements is done based on security events which is not part of the standard operation of a service and which causes, or may cause, an interruption to, or a reduction in, the quality of that service. The result of this process is security incident reports. [1]

*3. Maintenance*

As before there are sub-processes to improve the implemented processes to cover any problem came out and these processes are:

*3.1. Maintenance of Service Level Agreements*

This process to keep the service level agreements in proper condition, and ends with Maintained Service level agreements

*3.2. Request For Change to OLA*

Request for a change to the OLA is formulated. This process ends with a request for change

*3.3. Reports*

In this process, the whole maintain implemented security policies process is documented in a specific way. This process ends with reports.

*4. Storage Unit*

The storage process is to create and maintain the basket work which will be the base of the security management data and security operational level change.

This process exists in all security management stages through collecting documents resulted from processes and redistribute again to maintain and improve the processes as figure 2 shows the management process and the documentary system in the storage process.

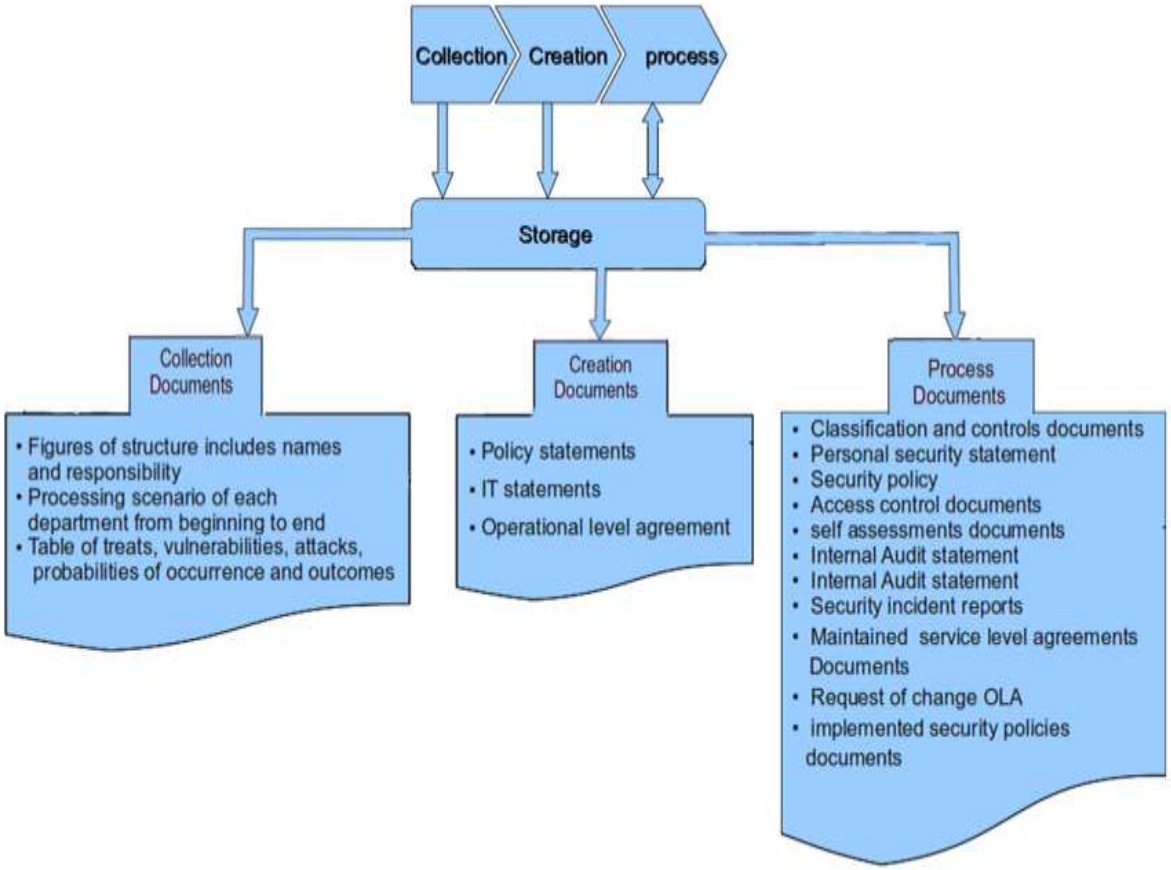


Figure 2. storage process and documentation(author)

## III. CONCLUSION

There are many practice models in the world of information technology like the British Standard and ITIL Information Technology Infrastructure Library, but they are not easy to implement. The security management requirements model can be understandable for any organization used technology and planned to implement security to secure their Data Resources and managed, also to be easy to implement and not to-much costly. The base of the model is the Data Life Cycle management from collecting, creating, processing and storage, where I was producing the model steps following DLC steps and formulating the security management as the main DLC process. And I can summarize my model in four steps: first collecting data required through analyzing the existing system's situation to find out three things (the management structure, the processing scenario in the organization and the threats vulnerabilities and probabilities of occurrences). The Second creating the security plan which includes (policy statement the determination of responsibility, IT statement the determination of IT required and the operational level agreement which considered the security policy) depend on data collected. The 3D is including three activates of an implement, evaluate and maintain the created plan. The 4th is the storage unit where all data has to be saved. That was my model of management security which can be implemented in any kind of organization. I plan to improve my model to be an intelligent security management provider application that can be used by any organization to create the security policy and determine the user's responsibility and requirements of IT and creating the implementation rolls and its reports.

## REFERENCES

[1] Timothy P.Layton, "*Information Security*". ISO/IEC17799 ISBN: 9780849370878, 2006.

[2] Aycock John, "*Spyware and Adware*" the University of Calgary. 2011 In the USA by Springer Science + Business Media. ISBN: 978-0-387-77740-5.

[3] Alison Cartlidge Xansa-Steria, Mark Lillycrop. "*an introductory overview of ITIL". v3 / auth. it SMF UK 2009.*" The UK Chapter of it SMF UK"- Vol. 3. ISBN 0-9551245-8-1.

[4] Jacques A. Cazemier, Paul L. Overbeek, Louk M.C. Peters. "*Best Practice for security management*". In the United Kingdom, 1999. ISBN: 0 11 330014X

[5] John .R.Vacca. "*Computer and Information Security*" .2009 in the USA. By Morgan Kaufmann Publishers is an imprint of Elsevier. ISBN: 978-0-12-374354-1.

[6] G. David Garson. 2003 "*Public information technology: policy and management issues*". In the US by Idea Group Publishing. ISBN: 1-59740-060-0.

[7] law American Bar Association .2008. "*Data of Security Handbook. Section of Antitrust"*. ABA. ISBN - 978-1-60442-047-0.
[8] Bart Van Ark, Simon K. Kuipers, Gerard H.Kuper.2000 "Productivity,
[9] in the Netherlands ISBN: 0-7923-7960-8.
[10] Nina Godbole. "*Information system security*". 2009.By Wiley India Pvt. Ltd. ISBN: 8126516925.
[11] Oracle. June 2007. "*Information life cycle management of business data*", An Oracle White Paper www.oracle.com/us/026964.pdf
[12] Information Technology Support Center. 2003. "*Best practices-security plus and policies*".[Online 2008] www.itsc.state.md.us/info/internetsecurity/bestpractices/secpolicy.htm.
[13] Danchev Dancho. Sept 24, 2003. "*Building and Implementing a Successful Information Security Policy*".SANSinstitute[Online] http://www.sans.org/rr/paper.pnp?id=418.
[14] Storage search. Feb 4, 2002. "*Developing a Disaster Recovery Procedure with Net Vault Backup Software*" Online. http://www.storgesearch.com/bakboneart.html