Cardiff Metropolitan University | Prifysgol Metropolitan Caerdydd

Student Details (Student should fill the content)				
Name				
Student ID (UWIC ID and ICBT ID)	Cardiff Met ID :		ICBT ID :	
Scheduled unit details				
Unit code	CIS 7028			
Unit title	**Information Security and Document Management**			
Assignment Details				
Nature of the Assessment	REPORT			
Topic of the Case Study	GIVEN			
Learning Outcomes covered	YES			
Word count	4000 Words			
Due date / Time	21st March 2021			
Extension granted? (For Office use only)	Yes	No		
Declaration				
I certify that the attached material is my original work. No other person's work or ideas have been used without acknowledgement. Except where I have clearly stated that I have used some of this material elsewhere, I have not presented it for examination / assessment in any other course or unit at this or any other institution				
Signature			Date	

Result (Assessor use only)				
Marks by 1st Assessor		Name & Signature of the 1st Assessor		**Agreed Mark**
Marks by IV:		Name & Signature of the IV		
For Office use only (hard copy assignments)				
Receipt date		Received by		

Assignment Type & Title:			
For student use: *Critical feedback on the individual progression towards achieving the assignment outcomes*			
For 1st Assessor use: Assessment feedback			
Strengths **Weaknesses**			
Name & Signature of the Assessor :		**Date :**	
Comments by the IV			

EVALUATE THE PROFESSIONAL STRATEGIES ASSOCIATED WITH DATA MANAGEMENT IN THE INFORMATION SYSTEMS ENVIRONMENT.

Content

Introduction

Any business generates heaps of data every day. Generated from external or internal sources these data provide a broad understanding of the business and its market when managed properly. As information is not static, there is a life cycle for information. Information capture, data storage, utilization, archiving, and purging are significant steps in the information lifecycle. Governments and organizations use data generated by processes to gain deep insights into market and customer behaviors. Hence managing data has become a crucial element of information systems environments (ISM). Information systems (IS) professionals work on merging the two areas of information technology (IT) and business processes. An ISM is an area where IS professionals view the business as a whole, understand the interactions of the parts of the system, and manipulate the variables with technical skills to develop IT solutions for the organization (Yaverbaum & Feinstein, 2004). Professional strategies help to standardize the data management process and ensure that the right data is acquired, managed, and retained for the best usage inside a business. Data is one of the most valuable assets a business produces. Managing the data right can bring valuable benefits in an information systems environment. There are many data management strategies in practice. Overall, an information management strategy is how a company is going to handle information created or acquired within business functions to achieve its goals and objectives in the most successful manner. There are several models developed on the information life cycle such as POSMAD and the CSRUD model. These models are built around the acquisition, maintenance, usage, and disposal of information in general. As there are multiple ways to design the right data management strategy for a company, evaluating them should be based on how efficient the strategy with regards to the goals that need to be achieved.

Justification for selecting the topic and feasibility

To research the chosen topic, the availability of resources is very important. Data management concepts first began to form in the 1960s. Since then, many types of researches and studies have been conducted on the subject area. With the advancements of technology, sophisticated tools have developed in aid of the processes as well. Hence there is positive feasibility in conducting this research successfully. By choosing the topic of “Evaluate the professional strategies associated with data management in the Information Systems environment” it is possible to gain in-depth knowledge about the data management process and widen the knowledge of different strategies too. It is convinced that the knowledge obtained by research on the chosen topic can be a great asset in the future as a professional in the field.

Literature Review and Analysis

Any data or information that has been produced are not static. The value of information changes over time and goes through a variety of stages of a cycle. Starting from the data entering to the storage system, to the time it is permanently retained or destructed, it must be managed through the life cycle to obtain the true value of the information. Information lifecycle makes it possible to understand and categorize the information within an entity and helps to decide what security mechanisms should be used to keep the information safe. It also helps to identify the most relevant information and store

them properly according to the priorities. Since information is needed in every stage of a process whether it's a business or a service, it is essential to understand the lifecycle of information precisely. At every stage, there should be decided and defined software, storage mechanisms, and hardware in the management of information.

There have been researches and discussions conducted on the information life cycle since the early 1980s. In 1999 the five-phased model (plan, acquire, maintain, dispose, and apply) was proposed, (Larry P. English, 1999) that can be used on any resource including information, money, people, material, product, and facilities. In 2008, (McGilvray, 2008) extended it to a six-phase model with an additional "store and share" phase. The phases of this model are, Plan, Obtain, Store and share, Maintain, Apply and Dispose. This model is similar to the CRUD model databases use; the Create, Read, Update and Delete model(Talburt & Zhou, 2015). It has also presented as a recursive process where the Apply, Store and share, and Maintain phases are recursively connected. It is identified as POSMAD with the starting letters of each phase's name. Below is a short description of the POSMAD phases.
Plan: This is the first step and it is allocated for preparing for the information. In this step, it is needed to identify objectives, plan information architecture, develop standards and definitions. In an organization, before designing and developing information management applications, databases and processes, this phase can be used to plan for the incoming data.
Obtain: In this step, the acquisition of the resources happens. Creating, loading, exporting, or purchasing records belong to this step.
Store and share: Holding the information in databases or as physical storage like documents, and distributing through electronic media (emails, networks) or physical media (documents).
Maintain: Maintaining the resources without unnecessary or unauthorized changes to content. Updating, validating, standardizing, and verifying existing information are the main activities in this step.
Apply: Using the information as it is needed to perform the jobs.
Dispose: Discarding the information when it is not useful. As the last step, the information can be archived or deleted depending on the value and the retention period of the data.

Apart from the models proposed in academia, there is a commonly used information life cycle model with five steps as, Creation and Receipt, Storage and Distribution, Use, Maintenance, and Disposition. This is much similar to the POSMAD model apart from the planning stage which is missing in the practicality.
Following is a detailed explanation of this information life cycle with some best practices that can be adhered to.
Creation and Receipt: This includes the creation of information internally or externally by processes and people of varying levels for an organization. The main sources could be computer input/outputs, reports, forms, receipts, and other similar resources. It is not only about the acquisition of already existing data, but also about capturing and performing data entry operations on the data generated by processes. The data entered could be of any form, from images to text files. Data that are in the system should be

stored in a way that, only the roles with proper access privileges can access and modify them. The accuracy of the data entered into the system should be managed and looked after by data entry professionals. To ensure that the data entered is in line with the final objective of the data usage, one common best practice is to classify data. By categorizing data as internal, external, public, private, confidential, or restricted it can define the guidelines for categorizations and establish the understanding of the criticality and sensitivity of information inside the organization. Along with the classification of data, to ensure the privacy and safety of the data creation stage, it is better to minimize the collection of restricted data.

Storage and Distribution: The storage and distribution of information are taken care of in this phase. After the information is created or received, it is needed to be stored, protected, and distributed to relevant parties for usage with an appropriate level of security and safety. The distribution could be internal or external. If some data is not frequently used, they can be archived for later usage. The best practice for storage is to implement a robust disaster recovery plan. It is best to keep a redundant, archived copy for a faster disaster recovery process. When storing information, using storage with authorized access, encryption of digital information, keeping physical media locked and safe is important to keep the data out of security breaches.

Use: After distributing information it can be used to generate business decisions to generate reports. Granting access rights only for the required roles can keep the information safe in usage. Mainly the information supports the activities of an organization. Information can be modified and saved. The best practice is to maintain an audit trail for critical data in the order for it to be traceable. At this stage, it should already be ensured that the information meets certain validations and is qualified for being used.

Maintenance: Management of information is called maintenance. Here, the information is stored according to a predefined schema and make available through a system. A proper filing method makes the usage and retrieval easy and efficient. Maintenance is also about timely responding to requests. Performing data synthesis combining different information from multiple sources to make conclusions is also an activity in maintenance. When transmitting data, using encryption and avoiding the use of printed material is encouraged to keep the data safe.

Disposition: Information retention or destruction is called disposition. Information that has met the end of its retention period is either retained or deleted. Only a small percentage of information remains valuable for a long period. Most of the information tends to decline its value over a short period. The challenge of this phase is to ensure that the data has been properly destroyed so that it will not cause any privacy or security breach in the future. As a best practice, a compliance policy can be created to ensure all the policies, regulations and standards have been followed before destructing information. Physical data should be discarded properly using a cross-cut shredder or similar means while data in electronic media should be erased properly.

With the introduction to the information lifecycle, the next term that comes into life is information lifecycle management (ILM). ILM is a standard approach to manage data center operations based on compliance and business protocols. For any business or service that is data-dependent, ILM is imperative. Due to the large volume of data produced each day by organizations, it is near impossible to manage data centers without a proper ILM system. (Reiner et al., 2004) has stated that Information Lifecycle Management (ILM) is a business-centric strategy for proactive management of information according to its value.

Considering the broad aspects considered in an ILM process, some commercial tools and services support the implementation of ILMs. Following are some of such tools.

- Data Management and Landscape Transformation (DMLT) group/SAP Consulting (Data Management and IT Landscape Transformation Services | DMLT, n.d.) - provide compliant data archiving and destruction, system decommissioning services, data migration, data privacy services.
- Oracle - has in-built support in the Oracle database to build an ILM on top of the database.
- Alfresco Governance Services - the Alfresco Content Connector for Amazon S3 Glacier's archiving services with ensured security.
- Informatica's Data Lifecycle Management Tool (Hub, 2020) - an all-in-one ILM tool compatible with many cloud platforms.
- IBM (Hub, 2020) and Tech Mahindra (Hub, 2020) also have all-in-one ILM tools of their own.

These solutions can broadly be categorized into hardware (IBM) and software tools (Oracle ILM Assistant and SAP ILM).

With ILM in action, the next concern should be information security management (ISM). This system requires some preparation beforehand. The chief information officer (CIO) and the chief information security officer (CISO) play a role in deciding the most optimal strategy overall for an organization. They are responsible for creating a strategic (long-term) information security (IS) plan. Planning should consider employees, management, and stakeholders and also the physical, political, legal, competitive, and technological environment alike. Strategic planning involves creating a long-term plan taking into consideration the allocation and acquisition of resources needed to pursue the organizational goals. Strategic flow usually starts from the top of the organizational hierarchy and to the bottom. A framework plan is provided by the management initially and it is passed down the hierarchy through managers and employees who oversee the nuances in the execution. Once the planning is completed it is converted to goals. Goals are further defined as tasks. This procedure of IS strategic planning is seen with three specific stages as mentioned below.

Strategic Planning →	Tactical Planning →	Operational Planning
Long term focus Performed by senior managers Supports overall vision and mission of the organization	Short term focus than strategic planning Usually one to three years Breaks strategic goals into incremental objectives	Used in the day-to-day performance of tasks Identified activities Involves weekly meetings, summaries, progress reports.

Typical elements which help define the strategic plan of an organization are as below.

- Executive summary.
- Mission, vision, and values statements.
- Organizational profile and history.
- Strategic issues and core values.
- Corporate goals and objectives.
- Major business units' goals and objectives.
- Market analyses, surveys, budgets, R&D projections.

With a description of strategic planning, it is important to mention some tips for effective planning as well. Below are some points that can be of help.

- Clearly define the vision statement.
- Logically analyze prior plans to identify effects against previous actions.
- Consider inputs from stakeholders comprehensively.
- Make the planning transparent so the stakeholders understand the process.
- Involve everyone in the organization in the planning process.
- Stick with the prose despite positive results as development takes time.
- Make the planning execution a part of the company culture.
- The processes should go in line with company culture.

When implementing an IS plan, information security governance (ISG) also becomes a major concern. ISG is, determining the authority and responsibility for making security-related decisions. It is not the execution of the plan but capturing the business objectives and strategies and creating a framework that directs IS strategy along with the company goals. ISO standard for governance of IS is, ISO 27014:2013 which specifies six high-level action-oriented IS governance principles. An organization that adheres to standards can follow those guidelines to implement an ISO-certified IS governance strategy in a company.

Once the planning for IS is completed, it can be executed in a top-down or bottom-up manner. The Security Systems Development Life Cycle (SecSDLC) is a methodology that can be used in the implementation. SecSLDC may differ in several specifics, but the overall methodology is similar to the SDLC. To work on all the major jobs related to IS of a company it must define various roles as, the champion (one who leads the identification and fixing bugs), team leader, security policy developers, risk assessment specialists, security professionals, systems administrators, and end-users. The process

should also take support from professionals like CISO, CIO, Chief Security Officer (CSO), Security Managers, Security Technicians, Data Owners, Data Custodians, and Data Users. Once the IS plan is implemented, it should be maintained adjusting to the changes in external and internal changes.

Tools and technologies make it easier to implement ILM systems yet meeting the privacy compliances require dedicated attention. Implementing an ILM should meet the needs of an organization while complying with mandates regarding data accessibility and retention such as the Sarbanes-Oxley Act (*The Sarbanes-Oxley Act 2002*, 2002), Health Insurance Portability and Accountability Act (HIPAA) (*Health Insurance Portability and Accountability Act of 1996 (HIPAA) | CDC*, 2019)), Children's Online Privacy Protection Act (COPPA) (*Children'S Online Privacy Protection Act (COPPA) - Encyclopedia - Business Terms*, n.d.), EU Data Protection Directives and privacy guidelines (*Data Protection in the EU*, n.d.) and OECD (*OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data - OECD*, n.d.) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (OECD).

As companies maintain confidential and sensitive data, they must be managed according to privacy laws and policy guidelines. HIPPA is a lawsuit to protect sensitive patient health information from being disclosed without the patient's consent or knowledge (*Health Insurance Portability and Accountability Act of 1996 (HIPAA) | CDC*, 2019). COPPA is a U.S. federal law designed to limit the collection and use of personal information about children by the operators of internet services and websites (*Children'S Online Privacy Protection Act (COPPA) - Encyclopedia - Business Terms*, n.d.). OECD and EU data protection laws are also guidelines to protect from violations of fundamental human rights, such as the unlawful storage of personal data, the storage of inaccurate personal data, or the abuse or unauthorized disclosure of such data.

Information as a resource is a huge asset to an organization if managed properly according to policies and guidelines. With the huge amount of data being produced every day, without a proper ILM system it is impossible to handle these data. Analyzing all the facts presented so far in this research it is evident that implementing an ILM system should be conducted with the knowledge of experts as the aspects that needed to be considered span over several subject areas. It is a combination of methodologies, tools, techniques, policies, regulations, guidelines, and budgetary constraints as well.

Discussion and Conclusion

This research is a study about professional strategies in information management in the information systems environment. The findings of the literature review have established that the professional strategies of information management are a cumulative effort that involves multiple subject areas and several professional practices. To keep up the good name, enterprises usually try to keep the information as easily accessible as possible. But considering the increasing number of incidents including identity

thefts, misuses of personal data, data leakages, etc. shows how complex and hard is to manage confidential documents and personal information in a privacy-compliant way (Mont, 2006). Therefore, it is evident that information management professionals must keep learning and stay updated about all the aspects discussed above to maintain the quality of the information management strategies they practice.

Information lifecycle management is a significant business process as important as customer relationship management (CRM) and enterprise resource planning (ERP). An effective ILM implementation can organize costs and management efficiencies well. It also helps organizations implement CRMs, ERPs, and disaster recovery solutions effectively as the information is prioritized and available. ILM systems and implementation of ILM systems is an ever-growing process. The nature of information, ILM tools, related technologies, policies, regulations, and even the nature of requirements of organizations changes over time. Therefore, to realize the benefits of ILM processes and maintain the validity of the ILM process organizations as well as researchers of the subject areas must continually review the usage patterns and quality of the outputs of ILM systems. With new tools like storage resource management (SRM) / Automated Data Migration (ADM), process monitoring has become easier. Also, new advancements in Advanced Technology Attachment (ATA) and Serial Advanced Technology Attachment (SATA) disks can help administrators to stage backups and snapshots inexpensively. Software innovations around SRM and ADM have also increased the ability to identify data, classify data and move data to the proper location over time. Privacy-aware information lifecycle management (Mont, 2006) is another area where researches are being conducted to develop approaches and technologies to automate aspects of privacy-aware information lifecycle management.

ILM needs to be a part of the overall information technology strategy of an organization as it has a direct impact on disaster recovery and business continuity. The initial steps of ILM are to classify the information based on its value. Information value is directly related to the value of the application that uses it. However, policy requirements also have an impact on the value of data. In the United States alone, there are around ten thousand state and federal regulations, such as HIPPA, COPPA, and Sarbanes-Oxley Act. Adhering to all these policy compliances has a real challenge in ILM implantations.

Various services related to ILM systems such as archiving, provisioning, backup, replication, and clustering are readily available from a variety of vendors. But the challenge is they do not integrate well with each other. The protocols, terminologies, tech stacks are different from each other making the integration of such services a true challenge. In response to this, integrated and automated ILM systems have been developed which can be considered as a positive trend related to ILM. With the new inventions in artificial intelligence/machine learning, big data handling, cloud platforms and parallel computing, the areas where the ILM can improve and evolve are seamless. Considering the ILM strategies being practiced as reported in the literature review section, different stages of ILM system implementation can be studied to find novel research ideas for academics. This report has discussed many areas related to

professional strategies in ILM thus has paved a way for enthusiastic individuals to conduct more researches on the different subject areas and make an effort to accumulate all the knowledge to bring up more advances to existing strategies and methodologies in information management.

References

Al-Fedaghi, S. (2008). On Information Lifecycle Management. *2008 IEEE Asia-Pacific Services Computing Conference*, 335–342. https://doi.org/10.1109/APSCC.2008.81

Avril, P., Baer, H., Baskan, Y., Christman, G., Dijcks, J.-P., Doraiswamy, S., Ganesh, A., Hobbs, L., Jernigan, K., Jeunot, D., Lakshmanan, H., Lane, P., Lee, S. K., Lorentz, D., Marwah, V., Moore, V., Muthulingam, S., Mylavarapu, A., Morales, T., … Belden, E. (n.d.). *Managing Data in Oracle Database With ILM* [Concept]. Oracle Help Center; December2020. Retrieved March 17, 2021, from https://docs.oracle.com/en/database/oracle/oracle-database/19/vldbg/manage-data-db-ilm.html#GUID-AC2B567F-14EF-4E7A-9992-076A2A820305

Children'S Online Privacy Protection Act (COPPA)—Encyclopedia—Business Terms. (n.d.). Inc.Com. Retrieved March 17, 2021, from https://www.inc.com/encyclopedia/childrens-online-privacy-protection-act-coppa.html

Data Management and IT Landscape Transformation Services | DMLT. (n.d.). Fast-Track Your Transition to SAP with Data Management. Retrieved March 17, 2021, from https://www.sap.com/services/implementation/data-mgmt-landscape-transformation.html

Data protection in the EU. (n.d.). [Text]. European Commission - European Commission. Retrieved March 17, 2021, from https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en

Health Insurance Portability and Accountability Act of 1996 (HIPAA) | CDC. (2019, February 21). https://www.cdc.gov/phlp/publications/topic/hipaa.html

Hub, D. S. X. (2020, October 14). Data lifecycle management: Top of the main tools. *DSX Hub*. https://www.dsxhub.org/data-lifecycle-management-top-of-the-main-tools/

McGilvray, D. (2021). *Executing Data Quality Projects: Ten Steps to Quality Data and Trusted Information* (2nd edition). Academic Press.

Mont, M. C. (2006). On Privacy-aware Information Lifecycle Management in Enterprises: Setting the Context. In S. Paulus, N. Pohlmann, & H. Reimer (Eds.), *ISSE 2006—Securing Electronic Busines Processes: Highlights of the Information Security Solutions Europe 2006 Conference* (pp. 405–414). Vieweg. https://doi.org/10.1007/978-3-8348-9195-2_43

OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data—OECD. (n.d.). Retrieved March 17, 2021, from https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

Reiner, D., Press, G., Lenaghan, M., Barta, D., & Urmston, R. (2004). Information lifecycle management: The EMC perspective. *Proceedings. 20th International Conference on Data Engineering*, 804–807. https://doi.org/10.1109/ICDE.2004.1320052

Secure Content Management Solutions for a Distributed Workforce. (n.d.). Alfresco. Retrieved March 17, 2021, from https://www.alfresco.com

Shorten, A. (2016). *ILM Clarification*. https://blogs.oracle.com/utilities/post/ilm-clarification

Talburt, J. R., & Zhou, Y. (2015). *Entity Identity Information and the CSRUD Life Cycle Model*. https://doi.org/10.1016/B978-0-12-800537-8.00002-8

The Sarbanes-Oxley Act 2002. (2002). https://www.soxlaw.com/

Yaverbaum, G. J., & Feinstein, D. (2004). *THE INFORMATION SYSTEMS ENVIRONMENT*. 7.