Project Title:
Design and implement DLP for financial institutions that protects customer financial information.

- Introduction
- Research Questions & Contribution
- Key literature related to the project
- Aims and Objectives
- Development strategy
- Ethical considerations and risk assessment
- Project Timeline

Introduction:

- Data loss prevention (DLP) is a set of technologies and processes that are used to protect sensitive data from unauthorized access, use, disclosure, modification, or destruction. DLP is particularly important for financial institutions, which collect and store large amounts of sensitive customer financial information. (Kaur, et al 2017)
- DLP framework can help financial institutions to: (Isaca, 2018)
  - Comply with industry regulations, such as the General Data Protection Regulation (GDPR)
  - Protect customer data from cyberattacks
  - Reduce the risk of data breaches and ransomware
  - Maintain their reputation and brand trust

Research Question

- How can a Data Loss Prevention (DLP) framework effectively protect customer financial information in financial institutions?

The research will investigate various strategies and technologies used in a Data Loss Prevention (DLP) framework to effectively protect customer financial information in financial institutions. It will explore the implementation of encryption techniques, access controls, and monitoring systems to detect and prevent unauthorized data leakage. (Isaca, 2018)

Additionally, the research will analyse the role of employee training and awareness programmes in ensuring the successful implementation of a DLP framework and reducing the risk of data breaches.

Project alignment to industry standards

Requirements	Artifacts
CYBOK knowledge Area based on the project title	5.1 Privacy & Online rights 5.2 Privacy as control
Protecting the confidentiality of personal identifiable information	NIST 800-122
GDPR	Data privacy
BCS	Data privacy and data protection

Description of artefact(s) that will be created

My research will explore policies to limit the operating system's ability to create, save, and open allowed file formats. By implementing restrictions on file formats, organizations can mitigate the risk of malware infection through malicious file attachments or unauthorized file execution. This is critical because not all files formats can be processed by the DLP tools.

These policies would be designed to enforce strict controls on file handling and promote the use of secure file formats, further enhancing the organization's security measures. (Kamalijeet, K. et. al., 2017)

Key literature related to the project - 1

- Explore the existing literature on various techniques used to secure data at rest and in transit, such as encryption, tokenisation, and data masking. Discuss their effectiveness in safeguarding sensitive information from unauthorized access or manipulation.
- Analyse different access control mechanisms and evaluate their efficiency in limiting unauthorized access to sensitive data. Consider discussing methods like role-based access control (RBAC).
- Examine the current technologies and techniques used in detecting and preventing data breaches, such as intrusion detection systems (IDS), security information and event management (SIEM) systems, and network segmentation. Assess their capabilities in identifying and mitigating potential security threats. Additionally, explore the importance of regularly updating and patching systems to ensure maximum protection against emerging vulnerabilities.

Aims and Objectives

The main aim of this research project is to evaluate the effectiveness of various security measures implemented in a DLP framework to safeguard customer financial information in financial institutions.

The specific objectives include assessing framework and techniques used to secure data at rest and in transit, evaluating the efficiency of access controls in limiting unauthorized access to sensitive information, and measuring the effectiveness of monitoring systems in identifying and preventing data leakage incidents.

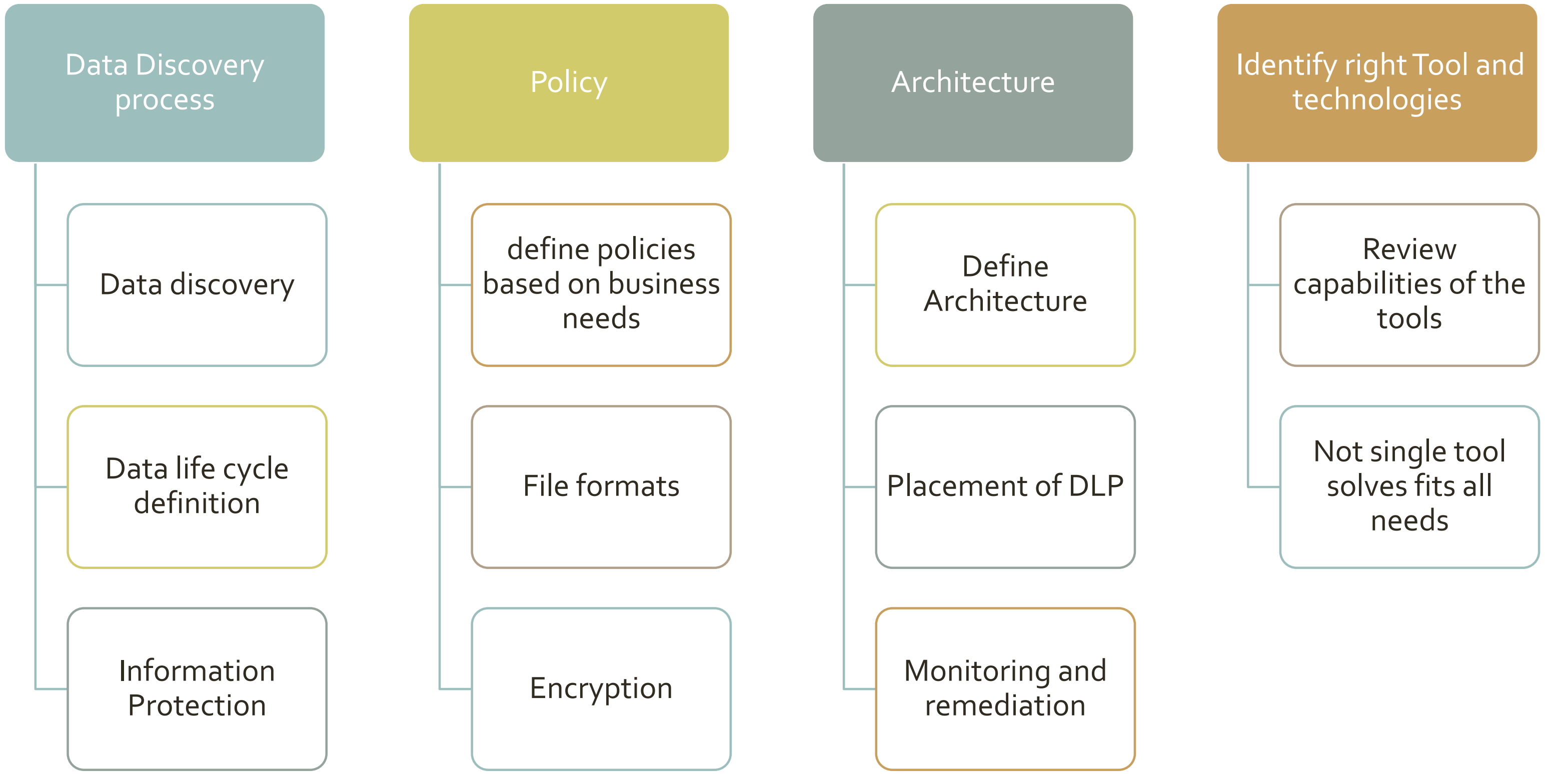
Furthermore, the research aims to determine the gaps in the implementing the operating system policy for the end user computing to protect data leakage.

Why its critical to deploy DLP solution?

UK and EU Government agencies has mandated the financial institute to implement Data Loss Prevention (DLP) solutions. These solutions help organizations prevent the unauthorized leakage of sensitive data, such as personally identifiable information (PII) or intellectual property. By deploying DLP solutions, financial institutions can ensure compliance with government regulations and protect their customers' confidential information from falling into the wrong hands. Additionally, DLP solutions can help organizations detect and respond to insider threats, such as employees intentionally or unintentionally leaking sensitive data.

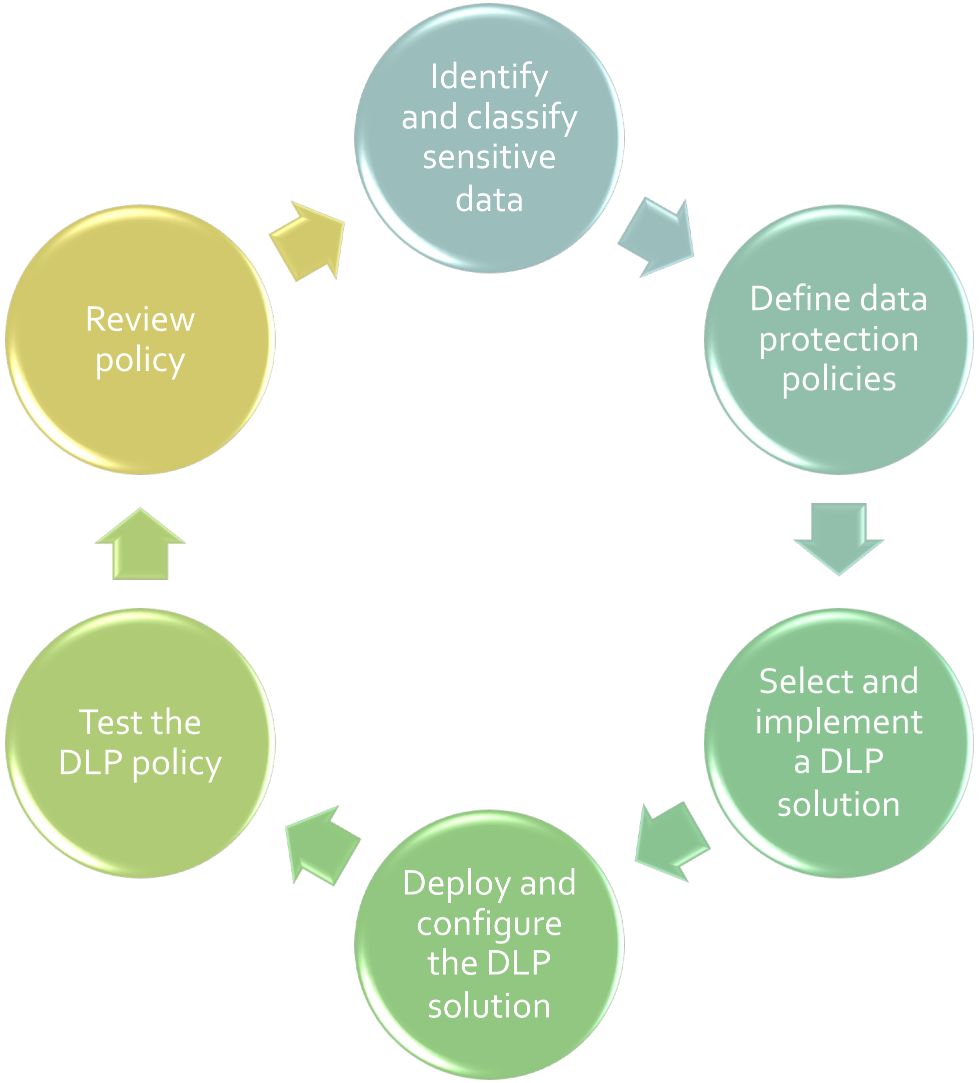
The General Data Protection Regulation (GDPR) is a privacy legislation that came into effect on May 25, 2018. The General Data Protection Regulation (GDPR) outlines guidelines for enterprises and institutions that are either based in Europe or cater to individuals within Europe. Other countries has their own data laws.

Overview – DLP process



- Data Discovery process
  - Data discovery
  - Data life cycle definition
  - Information Protection
- Policy
  - define policies based on business needs
  - File formats
  - Encryption
- Architecture
  - Define Architecture
  - Placement of DLP
  - Monitoring and remediation
- Identify right Tool and technologies
  - Review capabilities of the tools
  - Not single tool solves fits all needs

Development strategy



Identify and classify sensitive data

Define data protection policies

Select and implement a DLP solution

Deploy and configure the DLP solution

Test the DLP policy

Review policy

Steps to design and implement a DLP framework

1. Identify and classify sensitive data

   The first step in designing a DLP framework is to identify and classify all of the sensitive data that is stored and processed by the financial institution. This includes customer financial information, such as account numbers, Social Security numbers, and credit card numbers, as well as intellectual property and other confidential business data.

2. Define data protection policies.

   Once sensitive data has been identified and classified, the financial institution should define data protection policies. These policies should specify how sensitive data should be handled, used, and protected. For example, policies may restrict who can access sensitive data, how sensitive data can be transmitted, and where sensitive data can be stored.

3. Select and implement a DLP solution.

   There are a variety of DLP solutions available on the market. The financial institution should select a solution that meets its specific needs and budget. DLP solutions typically include features such as data encryption, data fingerprinting, and content monitoring.

Steps to design and implement a DLP framework

4. Deploy and configure the DLP solution.

   Once a DLP solution has been selected, it must be deployed and configured according to the financial institution's data protection policies. This may involve configuring the DLP solution to monitor specific data stores and networks, and to generate alerts when sensitive data is detected at risk.

5. Monitor and maintain the DLP framework.

   The financial institution should monitor the DLP framework on a regular basis to ensure that it is working properly and that it is being updated to reflect changes in the data environment and regulatory landscape.

Ethical considerations and risk assessment

- Ethical considerations play a vital role in implementing effective security measures. Organizations need to ensure they are not infringing on individual privacy rights while monitoring and gathering security information.
- Additionally, conducting a thorough risk assessment is essential to identify potential vulnerabilities and prioritize security measures accordingly. This includes evaluating the potential impact of security threats and determining the necessary steps to mitigate them.
- By considering both ethical implications and conducting comprehensive risk assessments, organizations can develop a robust security strategy that protects both their systems and the privacy of their users.

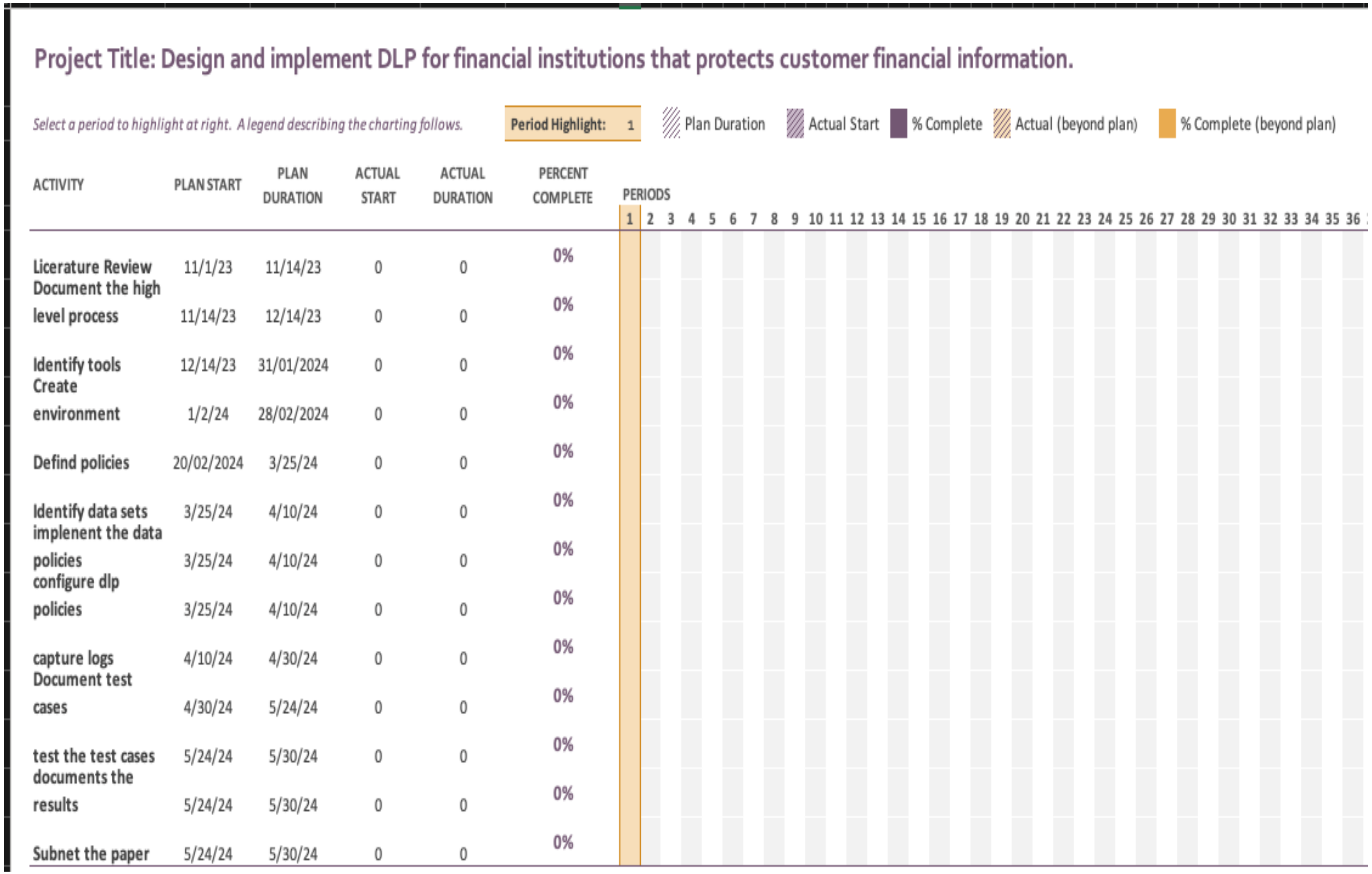
Description of artefact(s) that will be created

Define DLP Objectives	Identify critical data	
	Define protection goals	
	Set risk tolerance thresholds	
Data Discovery & Classification	Identify data repositories	
	Classify data based on sensitivity	Public Internal Confidential Restricted
Data Flow Mapping	Identify how data moves in and out of the organization	
	Map data transfer path and storge	
	Identify potential leakage points	
Implement DLP solution	Endpoint based	
	Network based	
	Storage based	
	cloud based	
Policy creation and management	Define acceptable use policies for data handling	
	Establish roles and permission for data access	
	Create automated response with Knowledge base article	
Monitor and alerting	Monitor and log each events and categories based on severity	
	Investigate alerts and verify incidents	
	Adjust the policy based on business needs	

Description of artefact(s) that will be created

Training & Awareness	Educate employees about the data categories
	Educate employees about data protection policies
	Conduct regular training sessions
	Simulate DLP incidents to assess preparedness
	Define protection goals
	Set risk tolerance thresholds
Review and Improvements	Audit DLP system performances
	Update data classification and flow maps
	Revise policies based on Organizational changes and feedback from employees and business
Compliance and reporting	ensure adherence to local and international data protection regulation
	conduct compliance assessments
	provide required reporting and stakeholders and regulators
Reporting Incidents to Government Agencies	Government agencies mandate companies to notified within certain timelines Agencies also fine the companies if they fail to comply

Timeline of proposed activities



Project Title: Design and implement DLP for financial institutions that protects customer financial information.

Select a period to highlight at right. A legend describing the charting follows.

Period Highlight: 1

▨ Plan Duration ▨ Actual Start ■ % Complete ▨ Actual (beyond plan) ■ % Complete (beyond plan)

ACTIVITY	PLAN START	PLAN DURATION	ACTUAL START	ACTUAL DURATION	PERCENT COMPLETE
Licerature Review	11/1/23	11/14/23	0	0	0%
Document the high level process	11/14/23	12/14/23	0	0	0%
Identify tools	12/14/23	31/01/2024	0	0	0%
Create environment	1/2/24	28/02/2024	0	0	0%
Defind policies	20/02/2024	3/25/24	0	0	0%
Identify data sets	3/25/24	4/10/24	0	0	0%
implement the data policies	3/25/24	4/10/24	0	0	0%
configure dlp policies	3/25/24	4/10/24	0	0	0%
capture logs	4/10/24	4/30/24	0	0	0%
Document test cases	4/30/24	5/24/24	0	0	0%
test the test cases	5/24/24	5/30/24	0	0	0%
documents the results	5/24/24	5/30/24	0	0	0%
Subnet the paper	5/24/24	5/30/24	0	0	0%

I have uploaded this document along with the presentation. I will detail this project plan as needed.

References:

Bcs, 2008 The Secret of effective data protection Available From: https://www.bcs.org/articles-opinion-and-research/the-secret-of-effective-data-protection/

Cybok, 2021 The Cyber security body of knowledge – Privacy and Online Rights knowledge tree Available from https://www.cybok.org/media/downloads/Privacy_Online_Rights_tree-1.0.2.pdf

Isaca, 2018, Data Loss Prevention—Next Steps Available from: https://www.isaca.org/-/media/files/isacadp/project/isaca/articles/journal/2018/volume-1/data-loss-prevention-next-steps_joa_eng_0218 [accessed on 05 Oct 2023]

Kamalijeet, K. et. al., 2017, A COMPARATIVE EVALUATION OF DATA LEAKAGE/LOSS PREVENTION SYSTEMS (DLPS) Available from: https://airccj.org/CSCP/vol7/csit77208.pdf [accessed on 05 Oct 2023]

Pleger, L.E., Guirguis, K. and Mertes, A., 2021. Making public concerns tangible: An empirical study of German and UK citizens' perception of data protection and data security. *Computers in Human Behavior*, *122*, p.106830.

R. Tahboub and Y. Saleh, 2014, Data Leakage/Loss Prevention Systems (DLP) Hammamet, Tunisia, 2014, pp. 1-6, doi: 10.1109/WCCAIS.2014.6916624.

Securosis, L.L.C., 2010. Understanding and selecting a data loss prevention solution. *Securosis, LLC*. https://securosis.com/assets/library/publications/DLP-Whitepaper.pdf

Stanikzai, A.Q. and Shah, M.A., 2021, December. Evaluation of cyber security threats in banking systems. In *2021 IEEE Symposium Series on Computational Intelligence (SSCI)* (pp. 1-4). IEEE.

Waziri, V.O., Ismaila, I., Alhassan, J.K. and Adedayo, B.O., 2016. Data loss prevention and challenges faced in their deployments. International Conference on Information and Communication Technology and its Applications Available from https://ceur-ws.org/Vol-1830/Paper17.pdf

Websense, N.D Financial regulations available from:
https://www.websense.com/content/support/library/data/v84/policy_classifier/financial%20regulations.aspx
[accessed on 05 Oct 2023]