



**TEVORA™**

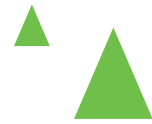
Whitepaper



# Data Loss Prevention (DLP) Implementation Strategy

Promoting successful implementation and execution  
of Data Governance

Data Loss Prevention (“DLP”) remains a challenging technology for most organizations to successfully implement and operate. Due to the nature of data and DLP operations, organizations frequently stumble with meeting timeline and effectiveness objectives. This often results in DLP being largely bypassed or relegated to disuse within the organizational technology stack in a short amount of time. The strategy outlined within this document explains processes Tevora has executed successfully within a variety of organizations to achieve these goals and ensure Organizational Data Governance is considered a successful initiative.



## DLP Implementation Strategy:

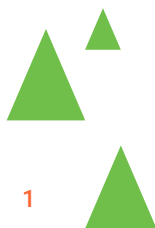
Additional details for each of these phases can be found in dedicated sections for each phase below.

- Data Identification/Tagging
- Data Control Vectors
- Review User Notification Policy
- Defining Response Processes
- Phased Policy implementation

Each phase within the strategy is intended to be iterative, with review and revision of each phase being conducted regularly to ensure organizational objectives are being effectively met. Additionally, each phase will have a component to address:



As we work with an organization to tune the plan, we include what risk factors each phase will address (detect, prevent, and respond), to show value capture and add throughout the organization. We also organize each phase to achieve quick wins that can be measured.





## 1. Data Identification/Tagging

Data identification centers around establishing the processes that will be used to identify sensitive data. This is frequently accomplished by conducting a data governance discovery campaign and identifying the data and sources that are considered sensitive to the business. Effectively, the goal is ensuring administrators can precisely qualify how sensitive will be identified or tagged for handling by DLP technologies. Specific activities include:

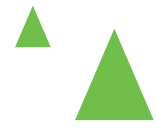
### (Process) Data Identification and Mapping Phase:

This project will focus on creating a Data Map against all systems that may collect, store or access sensitive data in-scope. The inventory will align to the global privacy laws applicable and data retention requirements of the organization. Activities will include:

- ▶ Identification of project stakeholders, key client programs and business units to be included in the impact assessment process.
- ▶ Interviews with key stakeholders and staff within Information Security, IT, Marketing, Customer Services, and other business areas, to identify any processes that may collect, store or access in-scope personal information.
- ▶ Identification of all locations and systems where personal information resides originating within identified business areas.
- ▶ Identification of the flow of IP and PII as it goes through the different data lifecycles phases include:



- ▶ Review the data architecture design and provide recommendations on data storage and location requirements based on applicable privacy laws.



Identification of all locations and systems where IP and PII data resides, through interviews and data dictionaries, including:

**Structured Databases (i.e. MySQL, Azure, AWS, Private Cloud, )365, OneDrive, SharePoint, backup storage)**

**Unstructured Data (i.e. PostgreSQL, Confluence, Share Drives, SharePoint, Private Cloud)**

**Local endpoint (i.e. laptop, workstation, tablet) storage by business process**

**Ensure a repeatable process is created to maintain the data storage locations, in accordance with the data governance program mentioned above**

- ▶ Document the data flow and storage of IP and PII
- ▶ Assess and research the applicable record series and retention requirements by working with the Client's stakeholders in the following areas:
  - Audit
  - Legal
  - Information Security
- ▶ Identification of applicable regulatory, legal, privacy and contractual requirements around data retention, destruction and sharing for both electronic and physical records including (not a comprehensive list at this stage):
  - FFIEC
  - NYDFS
  - GDPR
  - CCPA/CPRA
- ▶ Update existing data retention and destruction policy and procedure with information collected throughout the interviews and based on best practices.
- ▶ Provide best-practice recommendation for market solutions to maintain an accurate data map.



### (Program – Governance) Data Governance Program Development Phase:

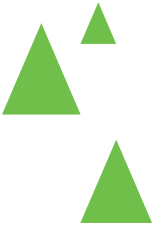
Interviews with key stakeholders and subject matter experts to capture any IT and relevant business requirements, as needed and understand existing data governance activities across Client systems (current and future state data modernization project).



Future-state is defined as all data sources throughout the organization for ingestion in the data modernization project

Development of a Data Governance Program Plan to detail future state data governance activities, which includes:

- Data Governance Objectives
  - Data Governance Challenges
  - Industry standard data governance frameworks (i.e. ISO 38505, NIST Privacy Framework)
  - Client-custom designed data governance framework
  - Data usefulness lifecycle
  - Roles and Responsibilities
  - Key Roles and Definitions
  - Data Discovery
  - Data Mapping
  - Governance Policy
  - Training
  - Data Minimization
  - Maturity Modeling and Measurement
  - KRIs and KPIs
  - Exceptions and Escalations Process
- Identification and documentation of the types of customer data currently collected and customer data required by Client in the future for product and business expansion including the review of any existing documentation for the ingestion and business use of customer data.

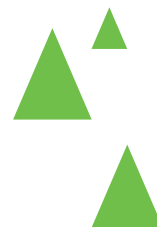


- ▶ Identification of the following related to usage and flow of customer data and other sensitive data throughout the organization including:

- ▶ **Review existing documentation from the Client for known data classification and privacy efforts**
- ▶ **Where is customer data and sensitive data stored?**
- ▶ **How is customer data and sensitive data ingested into the environment?**
- ▶ **Who accesses the customer data and sensitive data?**
- ▶ **Where does the customer data and sensitive data flow to outside parties?**

- ▶ (Technology Component) Identification of the baseline security standards for the protection of data at rest and usage within the organization (i.e., Data Usage Standard) to include:

- ▶ **Review of existing documentation: internal data protection and data treatment**
- ▶ **Define Data Governance practices**
- ▶ **Define Roles and Responsibilities for the Data Governance Program**
- ▶ **Define Security and compliance requirements for the storage and processing of data based on its classification**



- ▶ Provide expertise on industry trends and lessons learned for data modernization projects in regard to data governance.

### **(People) Data Governance Training Phase:**

This portion will focus on providing Client training to the organization on data governance.

Activities will include:

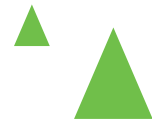
- ▶ Live (online) training session for Client's employees (will be recorded for future use by Client)
- ▶ Curriculum will be customized but may include topics such as:
  - Privacy
  - Data protection laws
  - Data governance
  - Data classification
  - Data transfer
  - Data usage
  - Data handling best practices
  - Data destruction

## **2. Data Control Vectors**

Once sensitive data sources are identified, the next objective should be to review use cases and requirements so the vectors for DLP can be identified. Common vectors generally include endpoints, network, email, or cloud. These vectors must be reviewed to ensure that technologies that will provide support for DLP operations are able to complete all required use cases.

### **Sample activities include:**

- ▶ (Technology Component) Assistance designing the policy engine, if applicable, (abstracted layer from the meta data) for enforcement of data classification including:
  - Architecture design
  - Identification and design of data classification categories for use in the data modernization environment
  - Definition of policy engine rules (i.e. smart logic that determines the data classification) and technologies to be used
  - Meta data tagging requirements for effective implementation of the policy



### 3. User Notification Policy

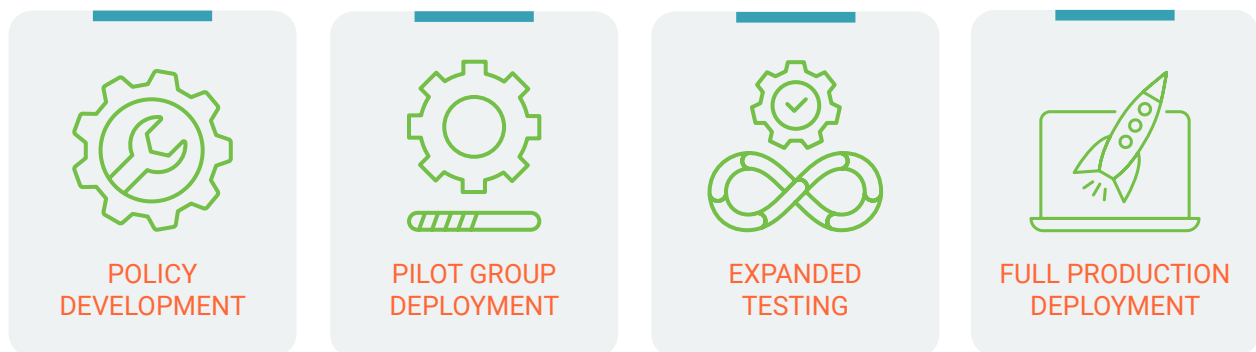
Defining user notification and feedback strategies are critical to successful execution of a DLP strategy and are primarily driven by the requirements of the organization. For instance, if the goal is to identify intentional bad actors, then a typical notification policy will include fewer notifications to users and significantly more to administrators and auditors; this allows for fewer opportunities for bad actors to discover how guard rails and controls are currently operation. Conversely, providing feedback to users can provide strong educational opportunities to users that are likely making only honest mistakes.

### 4. Defining Response Processes


Once the user experience is defined, the next phase should be establishing requirements for administration and operational support for the DLP solution. The organization must define use cases that will support self-service for users and the level of scrutiny and review that will be performed by personnel within trusted positions. For instance, defining who receives and responds to alerts, approves exceptions, and identifies opportunities for policy improvement will all occur within this phase.

### 5. Phased Policy Implementation

Once these underlying tasks are completed, the final phase is to begin implementation of the planned technology operations. This phase is centered around defining the policies previously defined into execution and generally has a recurring cycle that occurs something like this:





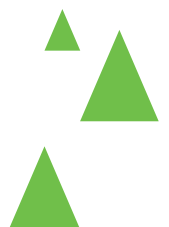


Initially, policies are developed by personnel as specific use cases are identified and defined. Following development, these policies are deployed to a small group of users that test these policies with both negative and positive testing scenarios; these users should be prepared for significant disruption due to poor DLP operation during these testing windows. If testing is completed successfully, testing expands to a large group of users that are less likely to experience disruption and will complete all normal business operations to identify any false positive results that might have been previously missed before policies are applied to all users.

Testing populations are typically contained in at least three groups. The pilot group is prepared for accepts almost any disruption and frequently special systems are designated for these purposes. The expanded testing group commonly comprises individuals across many different business units; this group is intended to represent a group that can effectively execute almost every business operational within the organization during the routine course of business.

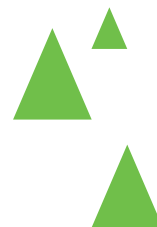
The expanded testing population is intended to identify issues with policies that might not be identified by the pilot group. Typically, the members of this group are more technical in nature than the average user and able to provide basic troubleshooting assistance to administrators are problems are identified and addressed.

Additional groups may be defined for large organizations. As the populations of these groups expand, users generally become less technically knowledgeable and represent more closely a standard user experience level. Technical knowledge and experience within test groups is less important than coverage around use cases; for instance, testing solely with members of IT would provide less value than testing with members from IT, accounting, human resources, etc.



## BEN DIMICK

### Director of Security Consulting Services



#### Primary Role

Ben leads the solution implementation practice at Tevora and is a specialist in the technology behind cyber security. He focuses on the daily operations of the solutions practice, as well as strategic alignment and partnerships. Ben is also responsible for partner and client relations within the sphere of solutions.

#### Notable Accomplishments

Ben is well versed in many technical areas given his extensive background in network architecture, application development, and systems administration. The depth and breadth of knowledge he brings to the table has been instrumental to Tevora's continued project success.

His expertise has allowed Tevora to continue to expand its strategic solution delivery reach and project success. His recent accomplishments include development of several successful architecture deployment strategies, focusing on SIEM, automation, and orchestration. He has functioned as primary architect for many solutions deployments for clients, with a special emphasis on development of cross-platform integration functionality.

Ben is responsible for providing the technical, engineering support for all Tevora security partner relationships. This enables him to learn intimately about the technologies used by Tevora's partners and provides him with a unique and well-rounded perspective on the information security landscape and what the future will hold for it.

#### Certification and Training

Ben holds a bachelor's degree in business management from Brigham Young University – Idaho. He is also certified as a Certified Information System Security Professional (CISSP), PCI QSA, and Okta Certified Consultant. Ben has received acknowledgment of expertise and achieved certifications from many of Tevora's technology partners, including Splunk, Palo Alto, Elastic, Cisco, and many others.

#### Tenure

Consultant has been with Tevora since 2012.

# CHRISTINA WHITING

## Principal | Privacy, Enterprise Risk & Compliance



**Primary Role** As Tevora's Principal over Privacy, Enterprise Risk and Compliance, Christina's primary role is to assist our clients in aligning their security and privacy programs with their business strategic objectives. With over 20 years of experience in the security and risk space, she helps organizations design, establish, and mature their privacy and security programs and capitalize on efficiency. Christina also mentors junior consultants, manages client relationships, assists with pre-sales and post sales activities, and oversees all projects from inception to the closeout presentation to ensure that every project exceeds our client expectations.

**Notable Accomplishments** With a diverse background in Education, Finance, Healthcare, Entertainment, Manufacturing, and Hospitality, Christina brings vast knowledge in both business and security to our clients. Her experience in privacy regulations (i.e., GDPR, CCPA, and LGDP), security assessments, security strategy, risk management, compliance, governance, data loss prevention and vendor management adds value to both our practice and to our client's engagements.

Christina holds a Bachelor's degree in Electronic Engineering and Information Technology, a Master's degree in Management Information Systems from NSU, a MBA from MIT and a PhD (ABD) in Information Security and Assurance from NSU. She has been inducted into all notable security and computer science honor societies including Alpha Beta Kappa National Honor Fraternity, Alpha Chi National Honor Fraternity, and Upsilon Pi Epsilon National Honor Fraternity. Christina presents on security, risk and privacy topics at conferences and regional events. Also an Information Security Instructor at University of California Irvine.

**Certification and Training** Christina holds the following certifications: PCI QSA, PA-DSS QSA, Certified Data Privacy Solutions Engineer (CDPSE), Certified Information Security Manager (CISM), Certified in Risk and Information Systems Control (CRISC), ISO 27001 Lead Auditor, Certificate of Cloud Security Knowledge (CCSK), Cobit, HITRUST Security Assessor (HSA), and a certification from the National Security Agency (NSA) Committee on National Security Systems (CNASS) in Information Security Management (ISO 17799).

**Tenure** Christina has been with Tevora since 2012



## About Us

Tevora is a leading management consulting firm specializing in enterprise risk, compliance, information security solutions, and threat research. We offer a comprehensive portfolio of information security solutions and services to clients in virtually all industries and also serve institutional and government clients.

Tevora's leaders are professionals with years of experience and records of accomplishments in technology as well as business. This dual background means that we understand the importance of growth and profitability and our solutions are designed to enhance both.

As a consulting firm that can fully implement whatever it recommends, Tevora works with all of the industry's top vendors, yet is beholden to none. We are completely vendor-independent and select best-of-breed products tailored exclusively to our clients' needs. Security is our only business and our single-minded focus on anticipating and solving client problems has been described as "obsessive." We consider this a fair assessment.

Our hard work and dedication have established us as a reliable partner CTOs, CIOs, and CISOs can depend on to help protect against threats, both internal and external. With Tevora as a partner, business leaders can devote their energies to enhancing the overall value of information technology to their enterprise.

Tevora is a Qualified Security Assessor (QSA) and Payment Application Qualified Security Assessor (PA-QSA) in good standing with the PCI Security Standards Council. Tevora is also a DVBE (Disabled Veteran Business Enterprise) certified by the California General Services Department (Cert REF# 32786).

For more information, please visit [www.tevora.com](http://www.tevora.com).