



# Information Lifecycle Management Playbook

9/16/2022



Revision	Description of Change	Date	Initials
1.0	Initial version	3/18/2022	ILM Team
2.0	Updated template and edits to ILM Vision	9/16/2022	ILM Team



## Table of Contents

Introduction.....	6
What is a Playbook? .....	6
The Plays.....	6
Information Lifecycle Management (ILM).....	6
The ILM Mission at Discount Tire .....	7
Discount Tire's ILM Vision.....	7
ILM Roles & Responsibilities .....	10
Business Segment Leadership .....	10
The ILM Core Team.....	10
ILM Senior Manager .....	11
ILM Plays.....	12
Sustain Data Map (IGMM-2) .....	12
Develop and Run Information Landscape Reports (IGMM-21) .....	13
Review ILM-Related Components of New Technology Solutions (IGMM-30) .....	13
Conduct Annual ILM Maturity Assessment (IGMM-19, 35, 38) .....	14
Conduct a Digital Records and Information Inventory .....	15
Privacy.....	16
Privacy Roles and Responsibilities.....	17
ILM Core Team.....	17
ILM Senior Manager .....	17
Legal .....	17
Meru Data .....	17
Privacy Plays .....	18
Conduct Awareness Activities.....	18
Conduct Training Activities .....	18
Identify, Collect, and Analyze Privacy-Related Metrics .....	19
Leverage the Data Map .....	20
Conduct Privacy Risk Reviews for Information Systems.....	21
Receive and Respond to Data Subject Access Requests (DSARs) .....	22
Review and Maintain Privacy Disclosures .....	24

Report Privacy Program Status .....	24
Records and Information Management (RIM) .....	25
RIM Roles and Responsibilities .....	25
Records Manager .....	25
Records Analyst .....	26
Records Coordinator .....	27
RIM Plays .....	27
Conduct Awareness Activities .....	28
Identify, Collect, and Analyze RIM-Related Metrics .....	29
Capture and File Physical Records .....	29
Respond to Requests for Records .....	30
Conduct a Physical Records Inventory .....	31
Recommend Appropriate Retention and Disposition (IGMM-20, 22, 23, 24) .....	31
Apply Legal Holds to TRIM .....	32
Administer the Recordkeeping System .....	33
Support PCI Compliance – Cardholder Data Storage & Retention .....	34
Information Security .....	35
Information Security Roles and Responsibilities .....	35
Information Security Plays .....	35
Identify, Collect, and Analyze Metrics .....	35
Ensure PCI Compliance .....	36
Review and Update the Acceptable Use Policy (AUP) .....	38
Conduct Technical Security Assessments .....	38
Sustain Security Incident Response Plan .....	39
Support and Sustain SAP Security .....	40
Provide Identity & Access Management .....	41
Litigation .....	42
Litigation Roles and Responsibilities .....	42
Litigation Team .....	42
OpenAxes Team (managed service) .....	42
Litigation Plays .....	42
Apply Legal Holds for Region/Store (Paper) Records .....	43



Apply Legal Holds to Information Management Systems for Regular (non-complex) Cases .....	43
Apply Legal Holds to Information Management Systems for Complex Cases .....	44

## Introduction

### What is a Playbook?

The playbook's objective is to provide best practices for major areas, not to substitute for management and leadership. It is critical to balance the importance of standards and guidelines with the value of local management discretion and individual employee creativity<sup>1</sup>.

Another way to look at a playbook is that it contains what someone would need to know in order to do a particular job for 30-60-90 days, perhaps even up to a year. What are the things you do, create, monitor, or report regularly? What are the questions you answer every day or every week?

The ILM Playbook is a living document. As new ILM processes are developed, they should be added to the Playbook. As ILM processes are updated to reflect changes in work processes, technology, or legal or regulatory requirements, they should be updated in the Playbook. The ILM Playbook thus becomes the single source of truth for all things ILM-related.

## The Plays

At Discount Tire, the overarching ILM initiative is broken into four workstreams:

- Privacy
- Records and information management (RIM)
- Security
- Litigation

Each workstream has its own “plays” based on the nature of the work being done. These plays are generally specific to a particular workstream, though some of them have a tangential effect on other workstreams.

There are also a number of ILM-related plays that cross most or all of the workstreams. For example, the data map directly supports plays in all four workstreams. And there are other ILM plays that are common to all four workstreams – for example, developing and sustaining awareness, or reviewing and evaluating processes. These two types of plays are grouped into a fifth workstream called ILM. We present these plays first, followed by the other four individual workstreams.

## Information Lifecycle Management (ILM)

Information Lifecycle Management (ILM) is a framework for managing corporate information and data in support of immediate and future regulatory, legal, risk, and operational

---

<sup>1</sup> <https://www.indeed.com/career-advice/career-development/what-is-a-playbook-in-business>



requirements. A solid ILM framework supports Discount Tire's strategy, operations, legal and risk landscape to create and operationalize controls and procedures related to the creation, management, preservation, retention and disposition of business records and information.

ILM requires ongoing, programmatic support and is key to the success of many critical corporate initiatives. ILM also facilitates the sharing of information and knowledge across organizational boundaries to eliminate silos of data management while controlling access and protecting our corporate information assets.

### The ILM Mission at Discount Tire

The purpose of the ILM program at Discount Tire is to provide oversight (guard rails), ensuring that policies and practices align with today's regulatory demands while still adhering to Discount Tire's culture. New regulations require a mechanism for establishing and maintaining policies and procedures that can be measured and validated.

Organizations are expected to manage information assets as deliberate as financial management practices. The expectation is to be good citizens and be diligent when collecting, creating, storing, using, and sharing information.

The ILM vision includes data minimization. Data minimization can be thought of in two separate but related and complementary senses: collection and disposition. Privacy best practices recommend that organizations collect only the minimum amount of information required to satisfy a particular task or process requirement. Information that is not collected cannot be breached, unlawfully disclosed, or altered.

Data minimization also includes getting rid of information assets that have no further business value – or indeed never had any. Information assets that are determined to be redundant, obsolete, or trivial should be disposed of on an ongoing basis. This will make it easier to find, and trust, information assets that retain business value. It will also support compliance-related activities and reporting and assessment efforts. Minimizing data by disposing of it at the end of its business lifecycle reduces costs and can further reduce the risks of a breach or unlawful disclosure.

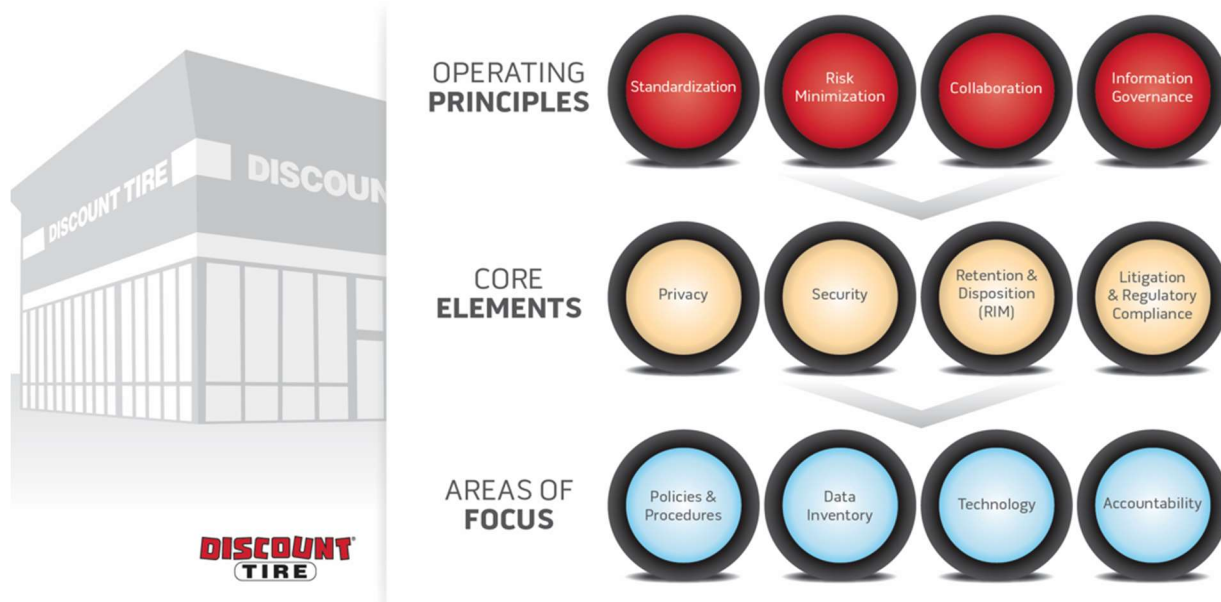
Data minimization supports the end-to-end management of enterprise information throughout its entire lifecycle, development of effective collaboration across every business segment, appropriate governance and controls on all information created across the enterprise, risk optimization, enforcement of data minimization principles, and consolidation of enterprise storage within fully integrated technology platforms.

### Discount Tire's ILM Vision

# ILM

## INFORMATION LIFECYCLE MANAGEMENT PROGRAM

A Unified Strategy for Managing Enterprise Information for Discount Tire



The vision for ILM at Discount Tire is that ILM serves as a unified approach for managing its enterprise information. The ILM Vision focuses on the development and refinement of enterprise policies, mapping of enterprise data, consolidation of storage platforms where feasible, creation of workflows that ensure information governance is implemented globally, and training of the workforce to understand the functionality and governance elements of enterprise technology platforms.

This means that the ILM team should be consulted on any projects, programs, processes, or systems that are created, procured, or updated, and that involve the creation, use, storage, and management of information. The ILM team will work with business units and implementation teams to ensure that information assets are managed appropriately to meet Discount Tire's business and regulatory requirements.

The program's mission statement is:

To ensure that information is effectively and efficiently managed throughout the lifecycle. This will be accomplished by working with each Business Segment to support Discount Tire's immediate and future operational, environmental, risk, legal, and regulatory requirements.

The ILM Program is based on four operating principles:



- **Standardization.** Policies, processes, procedures, and activities and outputs should be standardized where it makes sense to do so, taking into account individual business segments' particular business, operational, or legal needs.
- **Risk Minimization.** Better information management can help to minimize risks, whether the legal risks associated with inefficient eDiscovery, reputational risks associated with outdated information, the risks associated with ineffective safeguarding of customer information, and so forth.
- **Collaboration.** Effective ILM requires collaboration between the specialized roles executing the ILM processes and procedures, and Discount Tire's business segments and leadership in order to balance governance and compliance needs with business requirements and realities.
- **Information Governance.** In its definition of information governance, Gartner notes that [it] ensures the effective and efficient use of information in enabling an organization to achieve its goals<sup>2</sup>.

The overall ILM Program has been broken into four key elements:

- **Privacy.** This element focuses on policies and processes to safeguard customer and employee personal data and other sensitive information.
- **Retention & Disposition (RIM).** This element focuses on ensuring that Discount Tire retains information for as long as it has business value and manages it appropriately throughout the information lifecycle.
- **Security.** This element works to ensure the overall security of all Discount Tire information assets.
- **Litigation & Regulatory Compliance.** This element works to ensure that Discount Tire is meeting its legal and regulatory obligations and steers any litigation or other similar processes.

Each of the elements in turn is supported by and through the following areas of focus:

- **Policies & Procedures.** Policies and procedures should be clear, correct, current, and consistently followed, and compliance with them should be routinely measured and remediated where necessary.
- **Data Inventory.** Many organizations and analysts have asserted that information is an asset; the Association for Intelligent Information Management (AIIM) has said that information is an organization's most important asset. Discount Tire needs to know what information it has, where it is, and what its business value is, to manage it effectively.

---

<sup>2</sup> <https://www.gartner.com/en/information-technology/glossary/information-governance>



- **Technology.** The efficiency and effectiveness of an ILM program can be significantly enhanced by technology. The more mundane tasks that can be streamlined or automated using technology tools, the more time is freed up for tasks that need human interaction or decisions.
- **Accountability.** Ultimately, the best policies and procedures, the best tools, and the best of intents require that decisions be made, and owners be held accountable for their decisions and actions – or lack thereof.

### ILM Roles & Responsibilities

The ILM structure at Discount Tire operates across organizational boundaries and consists of a number of different roles, each with their own focus, responsibilities, and accountability. This section reviews the teams and structures responsible for developing and executing Discount Tire's ILM vision.

#### Business Segment Leadership

The Business Segment Leadership (BSL) consists of representatives from each major business segment. In this role, the BSL supports the ILM Core Team's efforts to improve efficiency, reduce risks, and lower costs.

The cross-functional nature of the BSL provides a forum for the entire organization to have input into the development of the ILM program to ensure it not only meets legal and regulatory requirements but meets Discount Tire's business needs and fits its corporate culture.

Specific ILM activities and responsibilities of the BSL include:

- Support the move from siloed to holistic data management
- Champion efforts to reduce potential risk and expenses associated with Discount Tire's information assets and processes

#### The ILM Core Team

The ILM Core Team is a cross functional group of Discount Tire employees in Risk, Legal, HR, and IT along with technology partners and external advisors who meet regularly to discuss strategic and tactical issues associated with ILM.

The ILM Core Team supports the development and execution of ILM-focused processes to improve efficiency, reduce risks, and lower costs, by ensuring that corporate records and data are created, received, appropriately shared, maintained, and disposed of in accordance with Discount Tire's legal obligations, regulatory compliance, and data governance policies, with minimal disruption to day-to-day workflows. These processes are also designed to help Discount Tire be a good steward of the data that has been provided to us, and ensure protection of Discount Tire's data, as well as our customers' and employees' data.



Specific ILM activities and responsibilities of the ILM Core Team include:

- Drive ILM-related efforts that require cross-functional cooperation, buy-in, and decision making
- Contribute to and approve information governance policies, standards, and procedures
- Review & update strategies
- Advise individual work streams
- Coordinate meetings with business teams
- Provide recommendations to the BSL as necessary

While the ILM Core Team provides guidance and support, it is sometimes necessary to work more directly with key individual stakeholders in order to make decisions and implement them. When necessary, these are initiated by the ILM Senior Manager who will reach out directly to those stakeholders.

#### ILM Senior Manager

The Information Lifecycle Management (ILM) Senior Manager plays a critical role in coordinating strategy, sustaining excellence, and nurturing culture, growth, and stewardship. The ILM Senior Manager is responsible for overall enterprise-wide program development, implementation, and compliance program standards to include compliance with laws, rules, regulations, and internal policies and procedures throughout the information life cycle.

In other words, the ILM Senior Manager leads, and is the focal point for, Discount Tire's ILM efforts across the organization.

The ILM Senior Manager recognizes that ILM is interdisciplinary and affects every employee and every work process at Discount Tire. The ILM Senior Manager is a partner with IT, Compliance, Risk Management, and the business segment leadership and works closely with each to ensure they are able to leverage their records and information to meet their individual goals and the overarching goals of Discount Tire. The ILM Senior Manager also meets regularly with individual stakeholders, including but not limited to the CIO and CISO to make decisions that impact the ILM program.

The ILM Senior Manager's responsibilities include:

- Providing leadership for a multi-disciplinary delivery team to ensure successful implementation of key initiatives
- Providing project/program facilitation and oversight by facilitating agreement objectives, identifying success measures, and resolving issues and removing roadblocks

- Collaborating with key stakeholders including the CIO and CISO to raise awareness and develop consensus
- Partnering with Information Security, IT and Business Leadership in the creation and execution of a roadmap that aligns with the Discount Tire Business Strategy
- Effectively engaging and collaborating with leadership across the organization to develop, define and build on innovative ideas and business priorities
- Partnering with stakeholders to understand their needs, and use that knowledge and those relationships to drive effective prioritization and roadmaps for delivery
- Evolving current ILM and governance, risk, and compliance (GRC) practices to better align with recent growth and ensure future scalability

A complete job description can be found on the Knowledge Center.

### ILM Plays

These are Plays that impact most, if not all, of the individual workstreams.

#### Sustain Data Map (IGMM-2)

The Data Map provides a comprehensive footprint of data and data related processes across Discount Tire. It is a catalogue of what data is created, how it is classified, where it is stored and how it travels within and outside the Discount Tire organization.

The Data Map views each unique source of data as a System. Some examples of systems include file shares, document management applications, email, messaging, laptops, databases, mobile devices, cloud repositories, archives, backups and hard copy archives.

The Data Mapping tool automatically captures a number of details about each system, including but not limited to:

- System details, such as the name, description, and owner
- Privacy-related details, such as whether the system contains personal or confidential information
- Security details, such as whether the data is encrypted at rest or in transit
- Backup and disaster recovery details
- Records retention fields, such as record type and legal retention period
- Commercial fields, such as contract type and start and end dates
- Data flows, such as whether the system is a source for, or a target of, data from another system

This process is operated as a managed service by Meru Data. The Data Map is regularly updated based on quarterly interactions with system owners. Some systems are also updated automatically via an API.



As new systems are added to Discount Tire's environment, they will be submitted through the New Technology Review process described below.

Responsible	Accountable	Consult	Inform
Meru Data Managed Service	RMoq	ILM Core Team	RIM Team

Relevant policies and procedures:

- Data Map Privacy Fields [location]
- DT Data Map v2 [location]

Metrics:

- # systems mapped in data map (trend)
- # systems with retention applied (trend)
- Amount of data in mapped systems (trend)

Cadence: Quarterly or as systems are updated

#### Develop and Run Information Landscape Reports (IGMM-21)

These are reports that focus on providing a general view of Discount Tire's information holdings, e.g., volume, types/formats, date created, date last accessed, and other metrics of interest. These reports are generated monthly and reviewed by the ILM Core Team; where there are specific concerns or high-risk reports, the ILM Senior Manager will share those with the BSL as necessary.

Responsible	Accountable	Consult	Inform
ILM Senior Manager	RMoq	ILM Core Team	BSL

Relevant policies and procedures:

Metrics:

Cadence: Monthly

#### Review ILM-Related Components of New Technology Solutions (IGMM-30)

When new technology projects and enhancements are requested by the business, they require review by the ILM Team to assess potential risks, privacy compliance, and records and information management considerations, such as classification and retention management.

This process is intended to produce a new technology deployment corporate record to document our business practices and highest standards of due diligence throughout the information

lifecycle from design and implementation until the lifecycle has ended (through disposition). This includes records and information management policies and procedures (such as: record type classification and retention) and privacy compliance expectations (such as personally identifiable customer or employee information). It begins at the beginning – when a new system that creates, collects, or stores our information assets is added into the environment.

When new technology projects and enhancements are requested by the business segments, the prospective system owner completes a questionnaire within the Meru Data Map to collect additional information to better understand and document the business goals and purposes of the information and respond accordingly to inform and engage with the business and system owners.

The ILM Core Team will review the questionnaire and follow up with interviews to understand the potential ILM-related risks associated with the new system. Based on the information gathered, the team may identify questions that should be answered at the outset of the project (the Discovery/Research phase), provide the project team with functional requirements that should be included in the project during the Design/Build phase, and/or add notes and risk register information.

Responsible	Accountable	Consult	Inform
ILM Core Team	RMoq	Information system owner Business owner	BSL

Relevant policies and procedures:

- New Tech Deployment ILM Team Process

Metrics:

- % systems requested for which a questionnaire is completed

Cadence: As individual systems are considered for implementation or upgrading

### Conduct Annual ILM Maturity Assessment (IGMM-19, 35, 38)

It is important to review the various ILM-related processes on an ongoing basis. The earlier issues are uncovered, the easier they are to address. This Playbook includes metrics for the various “plays” as well as general guidance on how frequently to review them. This helps the ILM Core Team to:

- Ensure that policies, processes, and procedures are being followed

- Ensure that policies, processes, and procedures remain accurate and applicable
- Identify any changes or updates that need to be made
- Identify and develop ILM/RIM-related reports to monitor applicable business activities
- Identify and establish how ILM/RIM-related metrics will be captured and applied
- Generate reports as needed from applicable information systems to evaluate the current state of ILM/RIM and processes within the organization. These reports may be system generated or built into workflows

**Comprehensive program assessment.** The overall program assessment is conducted using the ARMA International Information Governance Maturity Model. The ILM Core Team, working with external resources, develops and administers a survey to Discount Tire employees regarding how they use information throughout the lifecycle. This survey is conducted annually and the results are analyzed to generate a maturity score which informs what additional projects should be considered for the ILM Program roadmap.

Responsible	Accountable	Consult	Inform
ILM Core Team	RMoq	Records Manager Individual employees within business segments	BSL

Relevant policies and procedures:

Metrics: Assessment resulting score

Cadence: Annually

### Conduct a Digital Records and Information Inventory

The records and information inventory is the foundation of an effective ILM program. If you don't know what you have, you can't manage it. The inventory provides a listing of the information assets held by the organization and includes physical and digital information assets. This Play focuses on digital records and information assets; physical records and information assets are covered in Part 3, Records and Information Management.

The inventory supports a number of objectives<sup>3</sup>:

- Locates and describes the organization's digital information assets, including records
- Identifies redundant, outdated and obsolete, and trivial information assets
- Determines storage needs for active and inactive digital records
- Identifies vital and archival digital records

<sup>3</sup> Public Records Office, National Archives of the UK



- Identifies sensitive records that require added security and privacy-related measures
- Leads to recordkeeping improvements that increase efficiency
- Provides the basis for the development of the Records Retention Schedule
- Improves compliance capabilities
- Identify problems and inconsistencies in RIM practices

At Discount Tire, the digital records and information inventory is produced through file analysis provided as a managed service by OpenAxes. OpenAxes is a service that runs on the Discount Tire network and scans and reports on systems connected to it. The OpenAxes file analysis tool can be used to inventory data across individual data sources (aka endpoints). It can also be used to write policy patterns to identify specific data types and classification. It keeps a running inventory of trends over time such as data added or deleted. Finally, it provides the ability to take remediation actions to deduplicate, remove stale data, or apply retention policy.

Meru's Data Map also collects information related to retention and classification for all systems in the Discount Tire environment. Meru maintains a detailed mapping of retention by record type and the system in which it resides. It can also identify the original system of record vs the duplicate copies for retention management and classification. This provides an understanding of the current state of retention within Discount Tire and gaps in information categories and helps in the development of a more comprehensive Records Retention Schedule.

Responsible	Accountable	Consult	Inform
OpenAxes managed service Meru Data managed service	RMoq	ILM Core Team	BSL

Relevant policies and procedures:

Metrics:

- Total # systems identified via network analysis
- Total volume, age, and last modified and access of information stored
- Detailed mapping of retention by record type

Cadence: On an ongoing basis

## Privacy

In executing on our Corporate strategy of providing the most inviting, easy, and safe tire and wheel purchase and service experience in the world, Discount Tire collects the personal information of customers, employees, contractors, job candidates, and other third parties.





Discount Tire is committed to protecting the privacy, security, confidentiality, integrity, and availability of this personal information with which it has been entrusted by its customers.

In 2018, the California state legislature passed the California Consumer Privacy Act ("CCPA"). The CCPA, for the first time in the United States, created a comprehensive set of legislative rights and protections over the personal information of individuals. As a result of this law, each California resident has the right to access the personal information that a company doing business in California has collected, request that the company delete that person's information, and opt out of the sale of the person's personal information. Among a number of other legislative and regulatory requirements, the law granted California residents the ability to enforce this law against a company under certain circumstances when a person's personal information is accessed without authorization.

Since the passage of the CCPA, California voters have amended the law to include several more restrictive measures and Virginia and Colorado have passed their own consumer privacy protection laws that grant similar rights to these states' residents. Most of the remaining states are considering similar laws. Suffice to say, privacy is now a compliance and regulatory issue on top of a consumer expectation.

### Privacy Roles and Responsibilities

In furtherance of the ILM's mission to manage information, which includes personal information, throughout its lifecycle, ILM will be primarily responsible for the implementation, development, and overall maintenance of the company's Privacy Program while relying on the assistance of contributors from other segments. ILM will report to the Board of Directors/Business Segment Leaders, which will provide executive oversight of and strategic guidance for Discount Tire's privacy practices.

Specific responsibilities include:

#### ILM Core Team

The ILM Core Team offers overall program oversight for the Privacy program and ensures alignment between the Privacy Program and the other workstreams.

#### ILM Senior Manager

The ILM Senior Manager is the primary administrator of the Privacy Program.

#### Legal

The Legal team assists in the program administration, in particular by identifying and clarifying the requirements associated with particular privacy laws and regulations such as the California Consumer Privacy Act (CCPA).

#### Meru Data

The Customer Data Portal is managed as a managed service by Meru Data.



## Privacy Plays

These Plays focus on safeguarding personal data for customers as well as employees, compliance with state privacy laws, and responding to consumers' requests regarding Discount Tire's collection and use of their personal information.

## Conduct Awareness Activities

An effective privacy program requires that management support it, by providing resources and guidance, and that employees support it, by understanding the importance of privacy and their responsibilities within the Privacy Program. Awareness-raising activities are one part of a comprehensive change management program. Here, awareness activities include but are not limited to:

- Formal marketing initiatives, such as posters, infographics, videos, and other ways to explain the purpose and benefits of the Privacy Program and individuals' responsibilities. The more specific these are, in terms of responsibilities, the more effective they will be.
- Less formal activities, such as blog posts, informal videos, Knowledge Center articles, etc. Note that these can come from third parties as well (subject to intellectual property considerations).
- Regular reporting to, and communications with, the BSL and senior management about upcoming developments, for example new state privacy regulations, and the overall status of the program.
- Regular support from senior management in all of these channels. A note from the CEO about the importance of safeguarding Discount Tire customers' information can be very powerful.

RACI:

Responsible	Accountable	Consult	Inform
ILM Senior Manager	RMoq	ILM Core Team	BSL

Relevant policies and procedures:

Metrics:

Cadence: Varies by activity:

- Awareness and reporting activities with ILM Core Team: biweekly
- Staff-focused awareness activities: monthly
- Updates to BSL and senior management: quarterly

## Conduct Training Activities

It is important to ensure that employees have the knowledge and skills necessary to execute privacy-related tasks and processes effectively. While Discount Tire's Learning and Development (LD) team has responsibility for the technical development of learning assets, including those for training, they will



need assistance from subject matter experts from the Privacy Team to ensure that the training is complete and accurate for the various privacy roles and for employees in general.

Different roles will require different training; moreover, there will be a need for various levels/depths of training including onboarding to Discount Tire; onboarding and orientation to a particular segment/department; specialized roles like Privacy Coordinator; and periodic refresher training.

Privacy training should be reviewed by the Privacy Team at least annually to ensure it remains correct and relevant. If significant changes are identified sooner, they should be communicated to the ILM Core Team and L&D to determine the appropriate approach to update the training.

RACI:

Responsible	Accountable	Consult	Inform
ILM Senior Manager	RMoq	ILM Core Team Learning & Development	BSL

Relevant policies and procedures:

Metrics:

- % completion of required privacy awareness and training courses

Cadence: Annually; as part of onboarding

### Identify, Collect, and Analyze Privacy-Related Metrics

As the old management saying goes, “You can’t manage what you don’t measure.”

Measurements, or metrics, help to form and shape goals, drive decisions, and ensure accountability. They tell a story as to how efficient and effective a particular process is.

Metrics must be measurable, meaningful, clearly defined (with boundaries), indicate progress, and answer a specific question. Just because something can be measured does not mean that it provides insight or even correlates to the process in question.

Every process should have at least one metric identified that provides insight into that process and how effectively it is being executed. Some processes may have a number of metrics. For example, the Retention and Disposition process could include metrics as to how many requests for exceptions are received, and granted, per year; how much of Discount Tire’s records volume is disposed of annually; and how many disposition reports are reviewed in a timely manner. Today these metrics are collected and analyzed by the ILM Senior Manager.

Metrics will be different for different processes because different things matter to this process versus that one. This means that each of the workstreams will need to identify the metrics that matter most to their particular processes; determine the appropriate mechanisms for collecting



them; and analyze and report them to their senior management, the ILM Core Team, or even the BSL as appropriate.

And because processes change over time, metrics will need to be reviewed regularly to ensure they are still telling a meaningful story. If a metric no longer has value, it should be updated or replaced with one that does.

Throughout this Playbook, we've identified metrics for each of the Plays.

Responsible	Accountable	Consult	Inform
ILM Senior Manager	RMoq	ILM Core Team	BSL

Relevant policies and procedures:

Metrics:

Cadence: Weekly/monthly as applicable

### Leverage the Data Map

The Meru Data Map holds information about Discount Tire's systems that collect, use, and retain consumer personal information. Systems owners have provided or will provide information about a Discount Tire system concerning the collection and retention of consumer personal information, which will be documented in the Data Map, and they will subsequently review and update the information on the Data Map periodically.

Based on the information provided by the system owners, the Data Map will identify the systems that may contain information that is affected by the CCPA, Privacy Impact Drivers, and CCPA exceptions. The Privacy Team uses a ranking process to determine a risk rating for systems that are affected by those regulations. As new systems come online, or existing systems, processes, or regulations change, the risks will need to be determined and the risk rating calculated.

The Data Map also documents the rationale for collecting data – how and why it is collected, used, and retained.

The ILM team will receive a monthly report with information on the systems that are potentially affected by the CCPA, which will be reviewed by the ILM Core Team. The Data Map and these monthly reports will be used to review and update these procedures as needed. (metrics)

RACI:

Responsible	Accountable	Consult	Inform
Meru Data Managed Service	RMoq	System Owners ILM Senior Manager	ILM Core Team

Relevant policies and procedures:



Metrics:

Cadence: As new systems come online, or as new regulatory or process changes occur

### Conduct Privacy Risk Reviews for Information Systems

The continued development of new laws and regulations relating to privacy and the protection of personal and confidential information means that Discount Tire needs to become more proactive in its review of information systems that process or store those types of information. This Play is used to evaluate the privacy and data protection capabilities of Discount Tire's current systems, while also serving as a framework with which to evaluate new systems and their capabilities.

There are three similar processes that can be followed depending on the nature of the system.

**Review New Technology Questionnaires for Privacy Implications.** This Play is described in detail in the ILM Plays section. It is referenced here for completeness. When new technology projects and enhancements are requested by the business segments, the prospective system owner completes a questionnaire within the Meru Data Map to collect additional information to better understand and document the business goals and purposes of the information and respond accordingly to inform and engage with the business and system owners.

**Review Systems in Data Map to Identify High-Risk Systems.** Systems in the data map are given a privacy-based risk score based on attributes identified as relevant by the Privacy team. The attributes can be volume of data, whether data is encrypted at rest and in transit, whether the data is shared outside Discount Tire, who has access to the data, how long the data is retained, and whether it contains sensitive or personal information and the type of sensitive information present. The risk score can be simple weighted average score or a decision tree and the systems are ranked into high, medium or low category based on the scoring. This score helps in identifying and prioritizing high risk systems for privacy review. This scoring methodology and the resultant scores are reviewed quarterly by the ILM Senior Manager and the Privacy team.

**Cross Target Advertising and Cookies (Privacy for Ad Tech).** Discount Tire's Privacy team uses a third-party tool called NT Analyzer to identify how the data captured when customers or third party interact with the Discount Tire website and the Discount Tire mobile app. NT Analyzer provides a detailed report of the data captured and how its shared with third parties. The privacy team analyzes the results, identifying areas of concern that require action, discussing those with the Marketing and Web teams, and resolving any issues that do not comply with Discount Tire's privacy notices and disclosures.

NT Analyzer analyzes the network traffic and browser / mobile app behavior from an end-user perspective. It identifies and catalogs third party disclosures in order to either review and confirm that these disclosures are intended and clearly represented in the privacy notice, or



determine that these disclosures are as intended. The report provides the communication tool for the Privacy Team to go to the Marketing and Web Teams to drive compliance outcomes, which can include:

- No action required because it adheres to Discount Tire's Privacy Notice and is properly disclosed
- Working with the Marketing and Web teams to resolve potential non-disclosure issues

Responsible	Accountable	Consult	Inform
Privacy Team	RMoq	Litigation IT Marketing Web Team Information system owners	ILM Core Team

Relevant policies and procedures:

- New Technology ILM Questionnaire Process
- Data Map Privacy Fields
- DT Data Map v2

Metrics:

Cadence: Monthly

### Receive and Respond to Data Subject Access Requests (DSARs)

The California Consumer Privacy Act of 2018 ("CCPA") provides California consumers several new rights with respect to the collection and use of the consumer's personal information by an entity doing business in California. Among these new privacy rights is the consumer's right to delete personal information. In response to a consumer's verified deletion request, a business is required to delete the personal information of the consumer that it collects and that it has shared with service providers (with certain exceptions). Discount Tire is compliant with the CCPA regulation and has developed procedures to facilitate the proper deletion of consumer personal information in response to a deletion request.

The customer also has the right to restrict the sale of their personal data, the right to ask for a copy of any personal data held on them by Discount Tire, and the right to ask for summarized copies of their information.

Under the CCPA, a business has 45 days from the receipt of the request to perform the requested action. This time period is only 15 days for opt out requests. However, this time period may be extended by an additional 45 days when reasonably necessary, provided that notice of this extension is provided to the requestor within the initial 45-day period.



Requests can be made through the Customer Data Portal or the Data Subject Access Requests Portal. There is also a phone number that consumers can call to record a request; the calls are recorded and processed in the same fashion.

When a request is received, it is validated by the Privacy Team using an automated process that leverages robotic process automation (RPA). Once the request is validated, the RPA tool identifies systems that are potentially responsive to the request. The consumer's data is identified, if it exists, and then the request is fulfilled, e.g. deleting or providing a copy of the consumer's data. Some requests for deletion may require the system owner to be responsible for deletion or, where data cannot be deleted for technical reasons, anonymization.

RACI:

Responsible	Accountable	Consult	Inform
Meru Data Managed Service	RMoq	IT Information system owners	ILM Core Team

References:

- CCPA Consumer Request – SOP v4
- Discount Tire Opt Out Request.
- Discount Tire Privacy Policy.
- Privacy Policy – DT/AT Behavior.

Metrics:

- # requests of each type by day/month/year/year over year
- # requests unverified
- # requests open
- # requests completed
- Types of requests by number
- Resource effort to respond (average?)
- Average turnaround time
- # extension requests by DT
- Page view metrics for consumer views of the privacy policy

Cadence: Ongoing, as requests are received





### Review and Maintain Privacy Disclosures

Discount Tire has developed and maintains privacy notices in compliance with the CCPA for Discount Tire customers, employees, contractors, and job candidates. These outline Discount Tire's collection and use of personal information and its commitment to safeguarding customer information. There is also an Opt Out Request notice giving customers the ability to explicitly direct Discount Tire to not sell their personal information in the future.

As privacy regulations continue to be developed or updated, Discount Tire needs to review its Privacy Notice periodically to ensure it remains relevant and applicable. The Notice is reviewed by the Privacy Team quarterly and updated as required.

Responsible	Accountable	Consult	Inform
Legal	RMoq	Web Team Privacy Team	ILM Core Team

Relevant policies and procedures:

- <https://www.discounttire.com/customer-service/privacy-policy>
- <http://www.discounttirefamily.com/ccpa-notice/>
- <https://datagovernancetool.azurewebsites.net/PrivacyRequest/discounttire/datarequestform/detail>

Metrics:

Cadence: Quarterly

### Report Privacy Program Status

Some privacy regulations require that the privacy program prepare a regular report to the organization's Board of Directors describing the current status of the program and any significant concerns. The specific reporting requirements vary by regulation, as does the frequency. At a minimum, the Privacy Team will generate and present this report to the Discount Tire Board of Directors annually.

RACI:

Responsible	Accountable	Consult	Inform
Privacy Team	RMoq	ILM Core Team	Board of Directors BSL

Relevant policies and procedures:

Metrics:

Cadence: Annually



## Records and Information Management (RIM)

Records and information management (RIM) is one of the foundational elements of any ILM program. At Discount Tire, it is one of the four ongoing ILM workstreams, but it can be argued that it is “first among equals” because of its value to the other workstreams. It is possible to have a RIM program that does not support the principles of privacy, is not focused on litigation, and doesn’t directly address security (though this is certainly not recommended!). However, it is all but impossible to have an effective privacy program, effectively secure Discount Tire’s information assets, and respond effectively to litigation and other records and information management requests absent a well-executed and rigorous RIM program. Indeed, the RIM program provides documentation as to the efficacy of the privacy, litigation, and information security workstreams and their related activities and compliance requirements.

But RIM is more than compliance. The RIM program, and its goal of appropriate and effective management of Discount Tire’s records and other information assets, makes it easier to find and use information when needed. It allows employees to do their jobs more effectively. And it allows Discount Tire to comply with applicable laws and regulations and to more easily demonstrate that compliance when required, thereby reducing risk. Effective RIM supports improved business outcomes.

It is important to note that RIM is more than technology. While technology can support the RIM program, and make it more robust and more automated, a successful RIM program requires a knowledgeable and engaged Records Manager, appropriate policies and procedures, and appropriate and ongoing training and awareness. It also needs to be implemented and executed consistently across the entire organization. The RIM program should support the business, not vice versa, and be as unobtrusive and organically ingrained as possible. But there is a truism in RIM: It is better to not have a policy, a retention schedule, etc. than to have one and not follow it consistently.

## RIM Roles and Responsibilities

### Records Manager

As noted above, records management provides a solid foundation that allows Discount Tire to effectively capture, store, manage, and leverage its information as an asset in support of business outcomes. The Records Manager’s role is to own, develop, and maintain the records and information management program in support of those outcomes.

The Records Manager understands that records are generated across the organization, in every business segment and by every work process. Failure to manage records efficiently reduces their value to the organization and can cause or contribute significantly to potential financial and legal liabilities.



The overarching goal of the Records Manager is to support Discount Tire business processes. The role of the Records Manager is not to “say NO!” to new tools and processes, or to “take away employees’ information.” Rather, it is to enable efficient work processes in support of organization goals and objectives.

As part of this, the Records Manager must work closely with the business segments to understand how they work and what they are trying to accomplish and advise them on how best to meet those goals - while keeping the organization and its information safe and compliant with applicable regulations and policies.

The Records Manager also needs to work closely with IT to ensure that electronic records, and the systems that manage them, align with both the needs of the business segments and compliance requirements. At the same time, the Records Manager offers advice to IT and the business segments on how best to leverage incumbent and emerging tools and technologies in support of those outcomes.

Key responsibilities of the Records Manager include:

- Leading the design, development, implementation, and review of records management program elements, to include retention and disposition, archiving management, retention schedule and classification
- Working with the various business segments to ensure appropriate retention, and disposition, of their records, regardless of format
- Ensuring that electronic records are stored appropriately and that systems that store records have the appropriate functionality to do so
- Managing physical records as required
- Developing and maintaining the records retention schedule
- Issuing and updating the records management handbook
- Educating and training records coordinators
- Participating actively as a member of various ILM-focused committees, such as the ILM Core Team

A complete job description can be found in the Knowledge Center.

### Records Analyst

The Records Analyst role at Discount Tire focuses on maintaining and administering the primary records management system and answering general questions about its functionality. The analyst currently acts, with the Records Manager, as the voice of the RIM team in terms of questions about the retention schedule, records management concerns, and records in general.

The Records Analyst supports the Records Manager by attending meetings and can serve as the Records Manager’s surrogate for meetings and some other tasks.



Specific responsibilities of this role include:

- Maintaining the Records Retention Schedule
- Perform technical and administrative duties related to maintaining physical and electronic records
- Monitoring records management system usage and compliance
- Researching, analyzing, and recommending changes or updates to the records management system
- Partnering with business segments to understand their records management-related concerns and identify their risks
- Recommending records management program enhancements
- Troubleshooting and resolving issues with the records management system

A complete job description can be found in the Knowledge Center.

### Records Coordinator

Placeholder while we determine whether ILM Steward encompasses this.

The Records Coordinator serves as the lead records management person in their particular department or region. They serve as the single point of contact from their department or region with the Records Team.

Key responsibilities of this role include:

- Oversee record disposition within the department/region
- Assist in the adoption, training, and raising awareness of records management obligations within their department or region.
- Assist their department/region with security management, folder creation, etc., within the designated recordkeeping tool
- Provide primary first-responder support for records management and recordkeeping system issues within the department/region, prior to escalating to the Help Desk
- Monitor their department's/region's compliance with the Records Management Policy

A complete description of the Records Coordinator role & responsibilities can be found in the Knowledge Center.

### RIM Plays

These Plays focus more narrowly on managing Discount Tire's records, from creation or capture through disposition.

## Conduct Awareness Activities

An effective RIM program requires that management support it, by providing resources and guidance, and that employees support it, by understanding the importance of effective management of records and non-records alike. They also need to understand the business benefits of RIM, such as being able to trust the accuracy and currency of a particular record.

Awareness-raising activities are one part of a comprehensive change management program. Here, awareness activities include but are not limited to:

- Formal marketing initiatives, such as posters, infographics, videos, and other ways to explain the purpose and benefits of the RIM Program and individuals' responsibilities. The more specific these are, in terms of responsibilities, the more effective they will be.
- ARMA International, the international association for records and information management, designates April as RIM Month every year, and provides a number of pre-built resources and activities. For example, they suggest that organizations consider a "Shred Day" in April that can focus attention on the value of getting rid of information assets with no business value, and that can coincide with the U.S. tax filing deadline in April.
- Less formal activities, such as blog posts, informal videos, Knowledge Center articles, etc. Note that these can come from third parties as well (subject to intellectual property considerations).
- Regular reporting to, and communications with, the BSL and senior management about upcoming developments, for example new state privacy regulations, and the overall status of the program.
- Regular support from senior management in all of these channels. A note from the CEO about the importance of efficiently responding to customer and third-party inquiries can be very powerful.

RACI:

Responsible	Accountable	Consult	Inform
ILM Senior Manager	RMoq	ILM Core Team	BSL

Relevant policies and procedures:

Metrics:

Cadence: Varies by activity:

- Awareness and reporting activities with ILM Core Team: biweekly
- Staff-focused awareness activities: monthly
- Updates to BSL and senior management: quarterly

## Identify, Collect, and Analyze RIM-Related Metrics

As the old management saying goes, “You can’t manage what you don’t measure.”

Measurements, or metrics, help to form and shape goals, drive decisions, and ensure accountability. They tell a story as to how efficient and effective a particular process is.

Metrics must be measurable, meaningful, clearly defined (with boundaries), indicate progress, and answer a specific question. Just because something can be measured does not mean that it provides insight or even correlates to the process in question.

Every process should have at least one metric identified that provides insight into that process and how effectively it is being executed. Some processes may have a number of metrics. For example, the Retention and Disposition process could include metrics as to how many requests for exceptions are received, and granted, per year; how much of Discount Tire’s records volume is disposed of annually; and how many disposition reports are reviewed in a timely manner. Today these metrics are collected and analyzed by the ILM Senior Manager.

Metrics will be different for different processes because different things matter to this process versus that one. This means that each of the workstreams will need to identify the metrics that matter most to their particular processes; determine the appropriate mechanisms for collecting them; and analyze and report them to their senior management, the ILM Core Team, or even the BSL as appropriate.

And because processes change over time, metrics will need to be reviewed regularly to ensure they are still telling a meaningful story. If a metric no longer has value, it should be updated or replaced with one that does.

Throughout this Playbook, we’ve identified metrics for each of the Plays.

Responsible	Accountable	Consult	Inform
ILM Senior Manager	RMoq	ILM Core Team	BSL

Relevant policies and procedures:

Metrics:

- % of RIM Plays with metrics identified
- % of RIM plays with metrics collected and analyzed in a timely fashion

Cadence: Weekly or monthly as applicable

## Capture and File Physical Records

Physical records consist of three main types.

- Store customer invoices, which are stored and managed at the individual stores
- Store employee onboarding and evaluations, which are scanned and stored in the recordkeeping system
- Corporate files, which are kept at individual departments' offices. When a department runs out of room, some of the records are boxed up and sent to the Alameda warehouse, and a record of the boxes and their physical locations are created in the recordkeeping system.

Digital records are stored in a variety of systems and locations. Each department has their own processes and procedures for what records to declare and file and where and how to file them.

Responsible	Accountable	Consult	Inform
Records Manager	RMoq	ILM Senior Manager Individual departments	ILM Core Team

Relevant policies and procedures:

- Alameda Paper Warehouse New Box Storage Process
- Corporate Records (formerly TRIM) Reference Guide – v1.1 20170828 (located on the KC)
- Records Management Policy (located on the KC)
- RIM – Processes and Procedures Manual (TRIM record #D5507590)
- TRIM Process – How to Catalog Physical Boxes in TRIM (TRIM Record # D6538759)

Metrics:

- Aggregate size (# records, storage volume) of records stored in TRIM and other systems (by system)
- # systems used to store records / trend over time
- Growth/reduction rate/trends over time
- % corporate records that are stored in TRIM, other recordkeeping systems, other systems (e.g., file shares)
- # boxes, estimated volume of records stored in Alameda warehouse
- Growth/reduction rate/trends over time

Cadence: Ongoing, upon request

### Respond to Requests for Records

The RIM team does not generally get involved with requests for digital records – those are self-service by the individual departments and coordinators. However, the RIM team may get



involved from a support perspective if a department or coordinator cannot locate a particular record.

If a department determines that it needs access to its physical records stored at the Alameda warehouse, it can make a request to the RM team.

Responsible	Accountable	Consult	Inform
Records Manager	RMoq	ILM Senior Manager	ILM Core Team

Relevant policies and procedures:

- TRIM Process – How to Catalog Physical Boxes in TRIM document (TRIM Record # D6538759)

Metrics:

- # retrieval requests per month
- Trend over time
- Average time to respond to request
- Average time between request response and return of records to Alameda warehouse (i.e., how long do the records sit at the requestor's office?)

Cadence: Ongoing, as requests are received

### Conduct a Physical Records Inventory

Physical records – really boxes of records - are managed in the recordkeeping application (currently TRIM) and are inventoried part of Discount Tire's annual disposition process as described below.

Responsible	Accountable	Consult	Inform
Records Manager	RMoq	ILM Core Team	Litigation

Relevant policies and procedures:

Metrics:

- # of boxes stored at Alameda Warehouse/trend over time

Cadence: Annually

### Recommend Appropriate Retention and Disposition (IGMM-20, 22, 23, 24)

All information assets have a lifecycle. They are created or received, stored, and managed, and accessed and used, so long as they have business value to the organization. Once they no



longer have business value, they should be disposed of in accordance with the Records Management Policy. The RIM team recommends appropriate retention periods and disposition instructions via the Records Retention Schedule.

Once records have met their retention requirements as defined in the Records Retention Schedule, they need to be reviewed to ensure there are no other outstanding legal, audit, or other requirements preventing their disposition. Absent any such requirements, records should be destroyed in accordance with the Records Policy. As noted in the RIM Processes and Procedures Manual, "Destruction is the final step in the lifecycle of managing our Company records and information. The destruction process should be run at minimum once a year."

Disposition today is applied to physical records, including store records and those stored at the Alameda warehouse. It is also applied to records stored in the recordkeeping system (currently TRIM).

Responsible	Accountable	Consult	Inform
Records Manager	RMoq	Individual departments	ILM Core Team

Relevant policies and procedures:

- RIM Processes and Procedures Manual (TRIM record #D5507590)
- TRIM Administrators – Process for Annual TRIM & Physical Records Destruction (TRIM record # D7253068)
- RM - Policy - Invoice Storage and Destruction Policies and Procedures – 20150528 (located on the KC)

Metrics:

- % records destroyed on time
- % of records that have met retention date but not destroyed because of legal holds
- % of records that have met retention, have no legal holds, but have not been destroyed
- # of requests for exceptions to retention and disposition periods
- Volume of records destroyed annually (physical, digital)

Cadence: Annually

### Apply Legal Holds to TRIM

For the primary recordkeeping system, TRIM, legal holds are placed, and cleared, by the RIM team as described in the resource below.

Responsible	Accountable	Consult	Inform
-------------	-------------	---------	--------



Records Manager	RMoq	Litigation	Records Analyst
-----------------	------	------------	-----------------

#### Resources:

- TRIM Administrator – Process for Litigation Record Searches & Legal Holds – (TRIM record # D8074601)

#### Metrics:

Cadence: Ongoing, as requests are received

#### Administer the Recordkeeping System

System administration for Discount Tire's recordkeeping systems is an ongoing concern – users are added to the system, roles are expanded or changed, users are removed from the system, and so forth. Tasks are specific to each individual system and are generally executed on an ad hoc basis as circumstances warrant, e.g., when a new employee needs to be added to the system.

Records management system administration tasks that fall under the purview of the ILM team include, but are not necessarily limited to:

- Creating and removing user access to the system
- Modifying user access to the system, for example when changing a user to a different role
- Creating or updating taxonomies and folder structures within the system
- Creating or updating metadata fields, including dropdown menu options, within a particular system
- Creating labels for, and tracking, physical records within the system
- Defining and applying retention to folders or records within the system
- Applying and removing legal holds to folders or records within the system
- Destroying records within the system that have met their retention period and have no further legal or business value

As of late 2021, the most used recordkeeping system is TRIM. The details of how to execute these tasks and activities within TRIM are identified below.

Responsible	Accountable	Consult	Inform
Records Manager	RMoq	ILM Core Team & IT	Legal

#### Relevant policies and procedures:

- Corporate Records (formerly TRIM) Reference Guide – v1.1 20170828 (located on the KC)
- RM Processes and Procedures Manual – (TRIM record #D5507590)
- TRIM Process – How to Catalog Physical Boxes in TRIM (TRIM record #D6538759)
- TRIM Administrator – Process for Litigation Record Searches & Legal Holds (TRIM record # D8074601)
- TRIM Administrators – Process for Annual TRIM & Physical Records Destruction (TRIM record # D7253068)

#### Metrics:

Cadence: Ongoing basis

#### Support PCI Compliance – Cardholder Data Storage & Retention

As part of the Information Security PCI-DSS program, RIM is responsible for collecting evidence of compliance from the in-scope areas for the following PCI DSS requirements:

- Requirement 3: Protect stored cardholder data
- Requirement 9: Restrict physical access to cardholder data

The in-scope areas include Operations, Facilities, Accounting, Asset Management, DTD Customer Care. On an annual basis, RIM collects signed attestations of compliance from the senior leader of each area and keeps them on file for evidence as requested during the audit.

Responsible	Accountable	Consult	Inform
Records Manager	CISO	Information Security	CIO

#### Relevant policies and procedures:

- [D5507590 RIM Processes and Procedures Manual](#)
- [5054 PCI Compliance - 9.6 - Restrict Physical Access to Cardholder Data](#)
- [5055 PCI Compliance - 3.1 - Keep cardholder data storage to a minimum](#)
- [D7879804 PCI Regional Attestation - TXD](#)
- [D7874253 PCI Attestation - Facilities](#)
- [PCI - Data Security Standard - v3.2.1](#)

#### Metrics:

- Signed Attestations Tracking% attestations stored where they can be accessed efficiently



Cadence: Annually

## Information Security

The Enterprise Security mission is to enable Discount Tire to grow responsibly by ensuring the integrity, confidentiality, privacy, and accessibility of our information assets.

Enterprise Security supports ILM initiatives at Discount Tire through several key areas:

- **Cyber Security.** Enterprise Security supports effective ILM through policy and standards creation, risk assessments, security consultation, and other technical security measures.
- **Security Operations.** Enterprise Security also helps to ensure the integrity of Discount Tire's information systems and information assets through tools and approaches including security incident and event monitoring, digital forensics, and event trending and analytics.
- **Identity and Access.** The Identity Management Team supports accessibility to information systems and assets through enterprise directory services, user administration and user entitlement. In addition, Enterprise Security helps to align security tools and approaches with business requirements while supporting security-related standards and governance processes.
- **Information Management.** The Records and Data Management Team is responsible for effective information management across the various ILM workstreams. This includes ensuring PCI compliance, employee awareness of information management and information security best practices, and data loss prevention.

## Information Security Roles and Responsibilities

TBD

## Information Security Plays

These Plays focus on ensuring the physical and logical security of Discount Tire's information systems and the information assets they store and manage.

### Identify, Collect, and Analyze Metrics

As the old management saying goes, "You can't manage what you don't measure." Measurements, or metrics, help to form and shape goals, drive decisions, and ensure accountability. They tell a story as to how efficient and effective a particular process is.

Metrics must be measurable, meaningful, clearly defined (with boundaries), indicate progress, and answer a specific question. Just because something can be measured does not mean that it provides insight or even correlates to the process in question.

Every process should have at least one metric identified that provides insight into that process and how effectively it is being executed. Some processes may have a number of metrics. For example, the Retention and Disposition process could include metrics as to how many requests for exceptions are



received, and granted, per year; how much of Discount Tire's records volume is disposed of annually; and how many disposition reports are reviewed in a timely manner. Today these metrics are collected and analyzed by the ILM Senior Manager.

Metrics will be different for different processes because different things matter to this process versus that one. This means that each of the workstreams will need to identify the metrics that matter most to their particular processes; determine the appropriate mechanisms for collecting them; and analyze and report them to their senior management, the ILM Core Team, or even the BSL as appropriate.

And because processes change over time, metrics will need to be reviewed regularly to ensure they are still telling a meaningful story. If a metric no longer has value, it should be updated or replaced with one that does.

Throughout this Playbook, we've identified metrics for each of the Plays.

RACI:

Responsible	Accountable	Consult	Inform
Information Security Team	Chief Information Security Officer	ILM Core Team	BSL

Relevant policies and procedures:

Metrics:

Cadence: Weekly/monthly as appropriate

### Ensure PCI Compliance

The Payment Card Industry Data Security Standard (PCI DSS) was developed to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally. PCI DSS provides a baseline of technical and operational requirements designed to protect account data. PCI DSS applies to all entities involved in payment card processing—including merchants, processors, acquirers, issuers, and service providers. Below is a high-level overview of the 12 PCI DSS requirements.



#### PCI Data Security Standard – High Level Overview

<b>Build and Maintain a Secure Network and Systems</b>	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
<b>Protect Cardholder Data</b>	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
<b>Maintain a Vulnerability Management Program</b>	5. Protect all systems against malware and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
<b>Implement Strong Access Control Measures</b>	7. Restrict access to cardholder data by business need to know 8. Identify and authenticate access to system components 9. Restrict physical access to cardholder data
<b>Regularly Monitor and Test Networks</b>	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
<b>Maintain an Information Security Policy</b>	12. Maintain a policy that addresses information security for all personnel

Discount Tire is a PCI Level 1 merchant, defined as a merchant that processes more than 6 million credit/debit card transactions annually. As a PCI Level 1 merchant, Discount Tire is subject to a PCI DSS audit annually by an authorized PCI Qualified Security Assessor (QSA). Discount Tire has maintained PCI Level 1 compliance since 2007 through the following activities:

- Completion of an annual PCI DSS audit by a QSA
- Completion of an annual Report on Compliance (ROC) through a QSA
- Network scans performed quarterly by the Approved Scanning Vendor (ASV)
- Completion of the Attestation of Compliance (AOC) Form
- Maintaining compliance across all in-scope environments according to PCI DSS standards and requirements

PCI level 1 is the strictest PCI DSS compliance level and is the only level that requires an on-site PCI DSS audit every year. Therefore, becoming PCI compliant often takes longer for level 1 merchants.

Additionally, Discount Tire must report the results of the audit to the “acquiring banks” defined by the PCI SSC.

Responsible	Accountable	Consult	Inform
Sr. Info Sec Compliance Admin	CISO	Information Security	CIO, CFO

Relevant policies and procedures:

- [PCI - Data Security Standard - v3.2.1](#)

Metrics:

- Date of last Attestation of Compliance
- Non-Compliance Areas, Remediation Date, Actions (If any)



Cadence: Annually

### Review and Update the Acceptable Use Policy (AUP)

Discount Tire's Acceptable Use Policy is documented and published on the Knowledge Center. The AUP defines the acceptable use of the Company Technology Resources, establishes each employee's responsibilities when using Company Technology Resources, and raises awareness of the risks associated with such use.

On an annual basis, the AUP is reviewed and updated as needed by the CISO. Each employee is required to complete a short training module on the DTU to review the AUP and acknowledge their review of the AUP. Learning & Development tracks the completion of the AUP course and provides completion statistics to the CISO for follow-up and reporting purposes.

Responsible	Accountable	Consult	Inform
Sr. Info Sec Compliance Admin	CISO	Information Security	BSL

Relevant policies & procedures:

- [Security Awareness and Acceptable Use Policy](#)

Metrics:

- Annual Completion Statistics

Cadence: Annually

### Conduct Technical Security Assessments

The Discount Tire IT Technical Security Assessment is a component of the Discount Tire enterprise security program which assures low risk, high assurance, service delivery platforms and solutions.

This IT Technical security assessment criteria is based on industry standard assessment frameworks from: *CIS Critical Security controls, Cloud Security Alliance, National Institute of Standards and Technology – NIST (800-53, 800-171), OWASP – Open Web Application Security Project – security framework.*

The core principles of the IT Technical Security Assessment are:

- **Information Security** – Validation of solution security controls used to protect Discount Tire information from unauthorized access, disclosure, destruction, modification, or misuse. Verification of reasonable security controls are in place to protect Discount Tire information from the current cloud security threats and risks, application technical threats, and vulnerabilities associated with the service and or solution.
- **Availability** – Ensure the service can provide high availability regardless of hosting service, application failure, or user fault.
- **Confidentiality** – Ensure access to Discount Tire information is tightly controlled to limit access to the correct parties and no others. Data is fully protected through encryption, secure key management, and employs security boundary firewalls to protect against outside intruders.





- **Privacy** - Throughout the collection, storage, use, disclosure, and disposal of Discount Tire PII/NPPI information remains private and sharing of confidential information satisfies least privilege and need to know principles and nothing more.

The primary purpose of the security assessment is to verify and validate cloud service provider and SaaS application compliance with privacy, security certifications, and cloud service security architecture best practices. The technical security assessment will focus on application technical threats, cyber risks, and vulnerabilities associated with the SaaS service or hosting provider.

This security assessment is based on the following industry best practice cloud risk assessment frameworks:

- *Center for Internet Security — CIS Critical Security Controls (CIS First 5 / CIS Top 20)*
- *Cloud Security Alliance — Consensus Assessments Initiative Questionnaire (CAIQ)*
- *ISO/IEC 9126 standard (Information technology—Software product evaluation—Quality characteristics and guidelines for their use)*
- *National Institute of Standards and Technology — NIST (800–171)*
- *OWASP – Open Web Application Security Project – security framework*
- *Shared Assessments Group — Standardized Information Gathering Questionnaire (SIG / SIG-Lite)*
- *Vendor Security Alliance — VSA Questionnaire (VSAQ)*

Responsible	Accountable	Consult	Inform
Principal Security Engineer	CISO	Information Security	ILM

Relevant policies & procedures:

Metrics:

Cadence:

### Sustain Security Incident Response Plan

The Incident Response Plan (IRP) is intended to provide a well-defined, organized approach for handling threats to the security of The Reinalt-Thomas Corporation's information. The plan also identifies and describes the roles and responsibilities of the Incident Response Team members.

The Incident Response Team's mission is to prevent loss of profits, public confidence, or information assets by providing an effective and knowledgeable response to any potential security breach involving information systems, networks, databases, or other protected data repositories. These events can involve computer viruses, hackers, break-ins, improper disclosures of confidential information, system service interruptions, breaches of personal information and other events with serious information security implications.

Training Incident Response Team Members is the responsibility of the Information Security Team and must be conducted at least once per year. Additionally, a simulated incident response will be conducted

once per year for regulatory compliance and should result in a review of procedures for Continuous Strategic Improvement (CSI).

Responsible	Accountable	Consult	Inform
Sr. Security Engineer	CISO	IT SME's	IT Board

Relevant policies & procedures:

- [Link to Security Incident Response Plan](#)

Metrics:

Cadence: Annually

### Support and Sustain SAP Security

SAP Security is a balancing act for protecting the SAP data and applications from unauthorized use and access. SAP Security helps to ensure that users can only use the functionality of SAP which is a part of their job. SAP Security provides design, configurations, controls, and procedures in order to ensure users have a safe and effective working environment within the SAP ERP landscape. This is done by following the principle of Least Privilege in giving a user or process only those privileges essential in performing their intended role. This ensures appropriate access to sensitive functions and confidential information such as financial records, which pose the risks of fraud, data breaches and compliance violations.

SAP Security:

- Designs and builds Role Based Access Controls with appropriate restrictions in collaboration with stakeholders and Finance Team
- Defines and implements efficient SAP security processes adhering to SAP Security best practices
- Supports both IT and Business enterprise projects and initiatives that require SAP security
- Maintains SAP security compliance in accordance with external finance annual audit
- Provides escalated comprehensive SAP security support for complex security issues for the enterprise

Responsible	Accountable	Consult	Inform
Sr. SAP Application Admin	CISO	Information Security	IT; SAP Team

Relevant policies & procedures:

Metrics:

- Number of support tickets processed (new users, changes, terms) in a typical month
- Number of roles, new roles created in a typical month





Cadence: Ongoing, as requests are received

### Provide Identity & Access Management

Identity & Access Management provides the right users with the right access to the right resources for the right reasons at the right time. IAM enables:

- New employees, contractors, and business partners to quickly get access to the applications they need to be productive and for an organization to easily stay in sync with changes to employee access rights as their roles change
- E-commerce web sites to provide effective customer support and more targeted customer engagement and opportunities
- Businesses to open up portions of their network to vendors & suppliers, making for a more effective exchange of information

### IAM Objectives:

- Improve user experience
- Improve operational efficiency
- Improve security posture

### IAM Team Focus:

- Person identity (Employees, Contractors)
- Single logical view of an identity
- Delivery of capabilities
- Standards based integration & services
- Rules based entitlement
- Rules based role and group assignment
- Policy based security access (e.g. MFA)

Responsible	Accountable	Consult	Inform
Manager, IAM	CISO	IT; Directory Services	IT

### Relevant policies & procedures:

### Metrics:

- Number of support tickets processed (new users, changes, terms) in a typical month
- Number of roles, new roles created in a typical month

Cadence: Ongoing, as requests are received



## Litigation

The Risk-Litigation department is responsible for oversight of all escalated claims and litigated matters, except in real estate and employment matters.

Typical matters include service-related matters (wheel-offs, tire failures, defective products, etc.), injuries on store property, and executive auto accidents.

### Litigation Roles and Responsibilities

#### Litigation Team

When legal matters arise, such as the receipt of a subpoena, the Litigation Team manages the litigation process, from responding to subpoenas, to identifying and collecting potentially responsive documents and records, to providing them to the parties involved.

The Litigation department also issues legal holds to stores, regions and corporate records for all litigated matters as needed, well as legal holds for the Claims Dept. where the claimant is represented by an attorney.

Litigation is also responsible for document collection involving various Discount Tire departments, and for managing subpoena responses – from receipt of subpoenas, through gathering of responsive documents, to responding to subpoenas once the data has been collected.

Litigation also manages and retains all outside attorneys, experts, vendors.

#### OpenAxes Team (managed service)

On an as-needed basis, the Discount Tire in-house Litigation Team has a partner in OpenAxes to fulfill obligations specific to legal matters that require specific SME expertise in data identification, collection, and preservation. The contract includes optional eDiscovery services that include, but are not limited to, eDiscovery review in Relativity and forensic data collection. This covers the complete spectrum of the EDRM eDiscovery Reference Model (<https://www.edrm.net>).

#### Litigation Plays

Documents and records may be required to be produced in support of a legal matter, audit, or for other reasons. The litigation process is directed and primarily executed by the Litigation Team.

Legal holds ensure that documents and records potentially within scope of a matter are not edited or deleted, whether inadvertently or intentionally, which in turn safeguards their evidentiary value.



Once litigation has concluded, the Litigation Team will notify the system owners and the legal hold will be removed, which will allow retention to continue and/or disposition to be applied to records as applicable.

Legal holds follow different procedures based on their circumstances. There are three primary use cases and circumstances for legal holds: region/store (paper) records, routine/non-complex cases involving digital information assets, and more complex cases. Each of these is outlined below.

#### **Apply Legal Holds for Region/Store (Paper) Records**

The Litigation Team sends a legal hold notice to affect store(s) and the applicable Region as well. The store(s) identify potentially responsive records, box them up, and send them to the Litigation Team, and all destruction is put on hold until the matter is resolved.

Once the hold is released, the Litigation Team transmits that back to the store(s) and region and the regular retention and disposition process is put back into place.

Responsible	Accountable	Consult	Inform
Litigation	RMoq	Stores, region directors	ILM Core Team

Relevant policies and procedures:

Metrics:

Cadence: Ongoing, as requests are received

#### **Apply Legal Holds to Information Management Systems for Regular (non-complex) Cases**

When legal holds are to be applied for regular, non-complex cases, legal holds are issued to the system owners by Litigation in conjunction with outside council. Once the matter has concluded, the legal holds are released and retention periods resume.

Responsible	Accountable	Consult	Inform
Litigation	RMoq	System owners	ILM Core Team Records custodians within the departments

Relevant policies and procedures:

Metrics:



Cadence: Ongoing, as requests are received

### Apply Legal Holds to Information Management Systems for Complex Cases

For more complex cases involving significant numbers of systems or custodians, or other cases that require it, Litigation engages the OpenAxes Team. OpenAxes implements legal holds on the applicable system(s), and takes complete ownership of the identification, collection, and preservation steps of the eDiscovery process. OpenAxes also provides eDiscovery subject matter experts in support of the process.

Once the matter has concluded, the legal holds are lifted from the applicable system(s) and retention periods resume.

Responsible	Accountable	Consult	Inform
OpenAxes managed service	RMoq	Litigation Records Manager IT	ILM Core Team Records custodians within the departments

Relevant policies and procedures (for all three legal hold possibilities:

- Records Retention Policy
- Legal Hold Policy
- Data Discovery Intake Process

Metrics:

Cadence: