FORTRA™

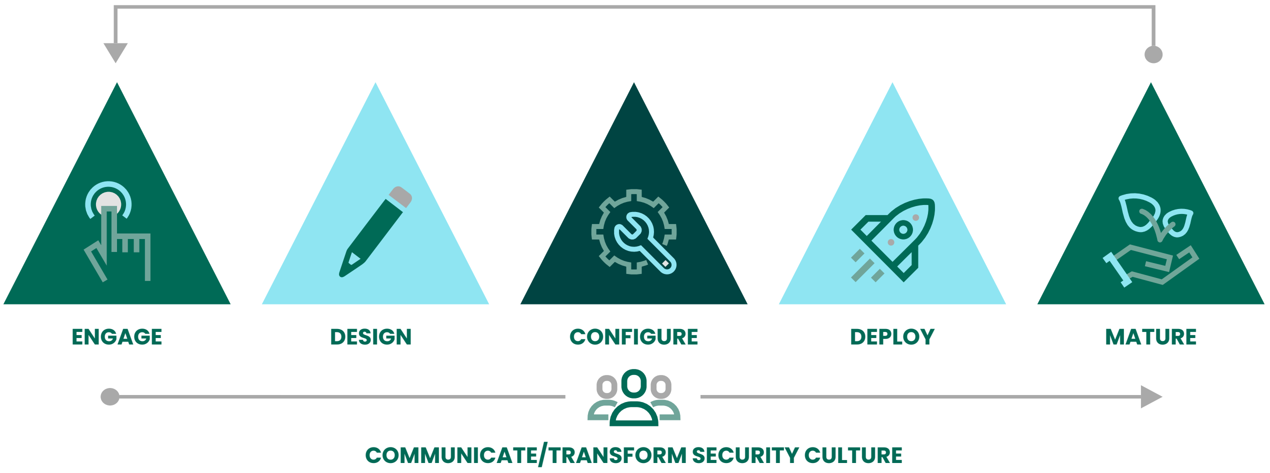
SOLUTION BRIEF (Data Classification)

Fortra Deployment: Implementation Timelines

Our proven deployment methodology accommodates strategic timelines for classifying data at creation, in motion, and at rest.

Fortra's Data Classification Suite (DCS) has had the privilege of deploying data classification and security solutions to the largest, most modern, and complex organizations in the world. Throughout these experiences, DCS has continued to learn and absorb best practices to make existing and future customers successful with their data classification deployments. In some instances, DCS customers already have a clearly defined approach to data security software deployment. In other cases, DCS can provide guidance based on best practices from other organizations to augment a data classification deployment strategy designed to meet business needs.

The DCS deployment methodology offers organizations an iterative framework to effectively deploy policies in a manner that ensures a positive user experience and with eye toward ongoing evolution.



ENGAGE

DESIGN

CONFIGURE

DEPLOY

MATURE

COMMUNICATE/TRANSFORM SECURITY CULTURE

ENGAGE

- Identify and onboard business stakeholders
- Identify and agree upon implementation phases, success criteria, and signoff process
- Provide resources to stakeholders and users

DESIGN

- Agree upon high-level solution architecture
- Develop schema and governance controls
- Create a policy workflow to meet phased criteria.

CONFIGURE

- Implement technical requirements from the design phase
- Perform testing across user communities
- Review, adjust, and update configuration based on feedback
- Obtain technical signoff

DEPLOY

- Announce the deployment to the organization via phased communications
- Roll out in phases across user communities
- Identify feedback that may require a configuration change

MATURE

- Produce reports that measure key success factors from the planning phase
- Review the next evolution of configuration to close the gaps toward meeting your evolving data security strategy

Our Methodology

DCS first helps you align on your program strategy and define your overall project goals. Key to your program's success is the readiness of your user community and business leaders to apply data classification policies on a daily basis that support your data security program. We recommend implementing your data classification program across three phases:

- **Phase 1:** Educate
- **Phase 2:** Empower
- **Phase 3:** Enforce

The outcomes of each phase will vary depending on the organization; however, the goals of awareness and planning, implementation, and enforcement and evolution typically remain the same. The below graphic explains how you might break your data classification deployment across these three phases:

EDUCATE

Why: Introduce the value of data protection to employees, and clearly articulate "What's In It For Me (WIIFM)."

What: Deploy DCS globally as a silent experience supported by corporate communications to explain WIIFM.

How: Deploy DCS to all desktops in phases. Consider having data classifications and categories appear on the ribbon but with no policies enforced. DCS could log sensitive data types and focus on integration with downstream technologies such as data loss prevention (DLP) while users get familiar with data protection policies.

EMPOWER

Why: With employees educated about data protection, begin to start automating policy decisions, but offer an option for employees to bypass the decision.

What: Turn on automated policies to identify and classify data with a justification option if they choose to violate the policy.

How: Tune DCS Accelerator for Privacy as well as regular expressions to identify sensitive data types and automate policy decisions for data at creation. with data protection policies.

ENFORCE

Why: Automate enforcement and control the protection of data that is shared externally based on data context.

What: Tie data protection policies to encryption as well as cloud security rules.

How: Trigger digital rights management (DRM) and encryption based on data contextual headers in email to ensure protection of data shared to external recipients. Integrate with cloud security solutions to control data going to and from the cloud based on data context.

Once you've identified the requirements for each phase, DCS will collaborate with you to create a deployment timeline based on the specific tasks outlined. The first step in defining your timeline is alignment on a required capabilities matrix to support each phase of deployment.

Deployment Timelines

DCS has learned that the time it takes to progress from planning to implementation and eventually to evolution varies greatly depending on an organization's IT environment, policy complexity, and overall readiness. Many organizations break the classification of data down into two separate projects:

1. **Data at creation or in motion.** Organizations often first address the identification and classification of all data that is being created and transmitted today.

2. **Data at rest.** Once an organization becomes comfortable with identifying data as it is created, it can be less overwhelming to begin classifying all the data at rest on servers, hard drives, and other locations across the company.

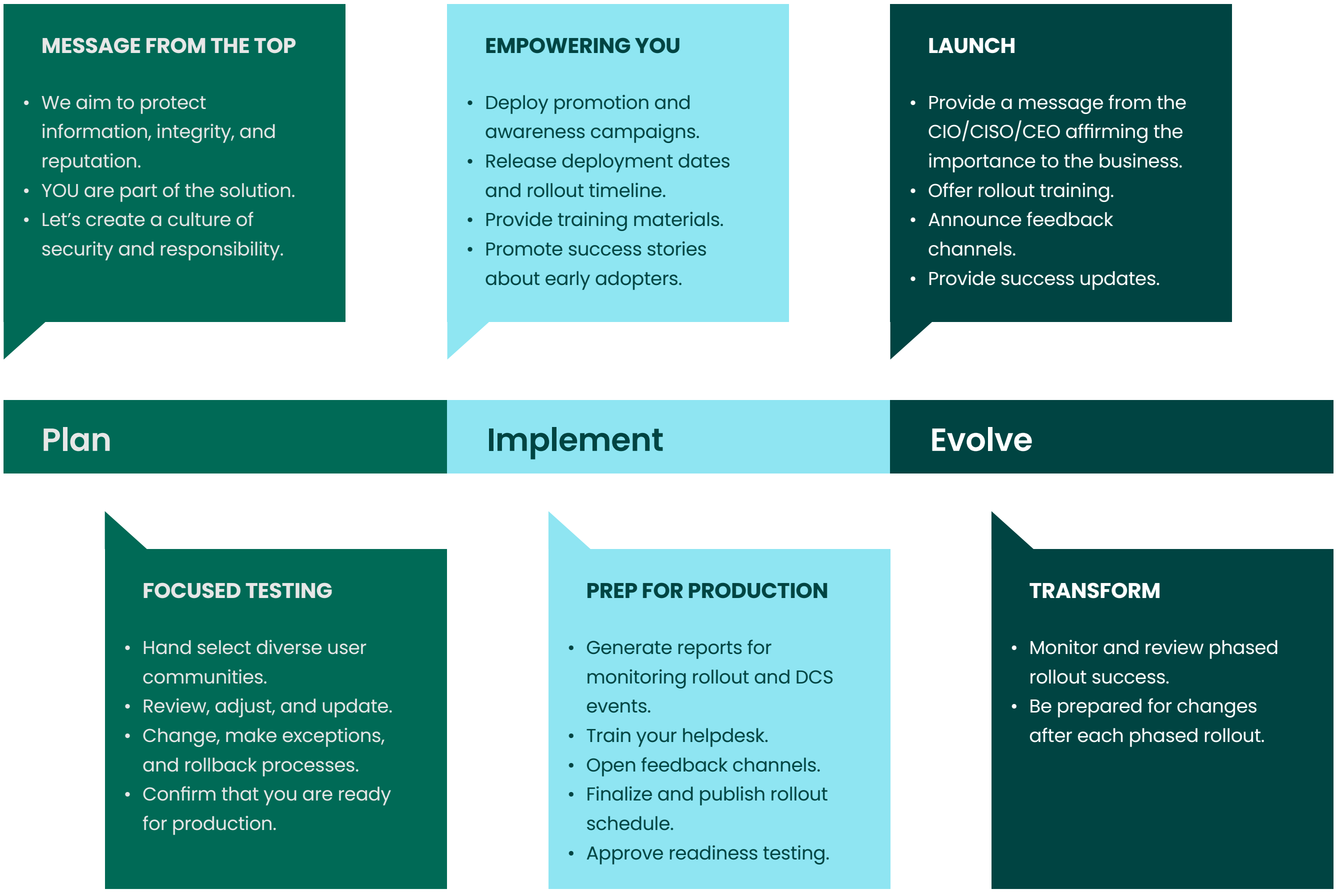
Both project streams can be run in parallel, but the data-at-rest project should not start until configuration and policies are defined.

Data At Creation And In Motion

The time it takes to implement a classification solution for data at creation will vary from organization to organization. For larger enterprise organizations, with more than 50,000 employees, the deployment timeline can take from 6 to 12 months to get the entire employee population up and running. The biggest variables driving this timeline are:

- Level of policy complexity
- IT program readiness
- Overall corporate culture

Once the initial solution implementation is complete (Empower), the program moves into the Evolve stage, where IT administrators adjust policies based on user feedback or the organization's ongoing data security evolution.



MESSAGE FROM THE TOP

- We aim to protect information, integrity, and reputation.
- YOU are part of the solution.
- Let's create a culture of security and responsibility.

EMPOWERING YOU

- Deploy promotion and awareness campaigns.
- Release deployment dates and rollout timeline.
- Provide training materials.
- Promote success stories about early adopters.

LAUNCH

- Provide a message from the CIO/CISO/CEO affirming the importance to the business.
- Offer rollout training.
- Announce feedback channels.
- Provide success updates.

Plan

Implement

Evolve

FOCUSED TESTING

- Hand select diverse user communities.
- Review, adjust, and update.
- Change, make exceptions, and rollback processes.
- Confirm that you are ready for production.

PREP FOR PRODUCTION

- Generate reports for monitoring rollout and DCS events.
- Train your helpdesk.
- Open feedback channels.
- Finalize and publish rollout schedule.
- Approve readiness testing.

TRANSFORM

- Monitor and review phased rollout success.
- Be prepared for changes after each phased rollout.

DCS recommends that you define a detailed road map for your evolution across the Educate, Empower, and Enforce phases of your implementation. With required capabilities outlined, DCS can work with your deployment team to create a realistic timeline. As mentioned earlier, the ability to accomplish each stage will vary from organization to organization.

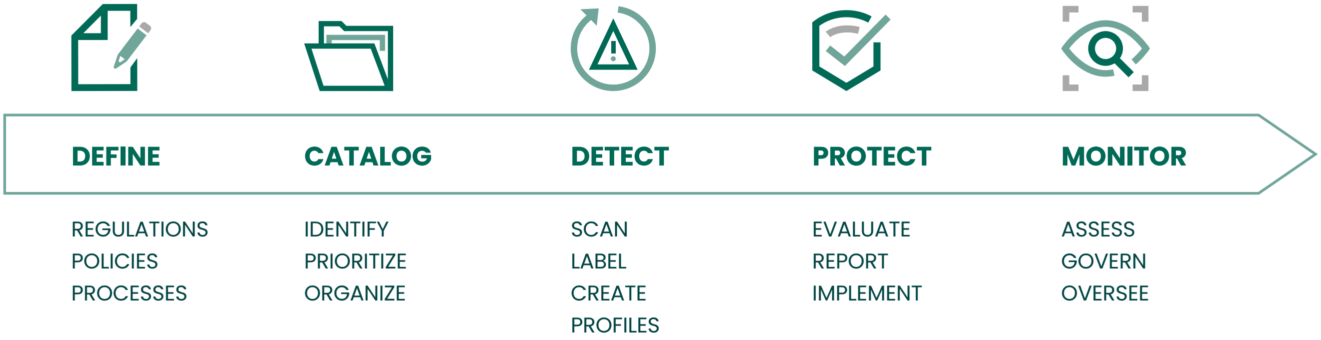
Below is a sample timeline for implementing a data-at-creation classification solution, with clear benchmarks along the way.

ID	REQUIRED CAPABILITIES	DEPLOYMENT PLANNING		DEPLOYMENT IMPLEMENTATION & EVOLUTION		
1	Identify and classify data at creation and in transit.	3-6 months	3-6 months	Educate	Empower	Enforce
2	Promote user awareness and culture change.	3-6 months	3-6 months	Educate	Empower	Enforce
3	Automatically apply proper visual indicators to documents, emails, and calendar invitations.	3-6 months	3-6 months	Educate	Empower	Enforce
4	Report on user behavior and classification landscape.	3-6 months	3-6 months	Educate	Empower	Enforce
5	Identify high-value keywords in content of emails and documents.	3-6 months	3-6 months	Educate	Empower	Enforce
6	Address regulatory compliance issues.	3-6 months	3-6 months	Educate	Empower	Enforce
7	Implement machine learning models based on existing data categories.		3-6 months	3-6 months	Empower	Enforce
8	Apply retention tags and Legal Hold/Consent Decree indicators (user-driven).		3-6 months	3-6 months	Empower	Enforce
9	Address DLP integration.			3-6 months	3-6 months	Enforce
10	Provide data context for future IRM integration.			3-6 months	3-6 months	Enforce

Data at Rest

It's important to address your vast amount of unstructured data at rest on its own and consider this an ongoing activity. To be successful in classifying data at rest, start with a clear inventory of that data. Try to focus on specific repositories or cloud file shares, and recognize that each location may have its own set of specific functional requirements.

The following diagram depicts a logical set of stages to classifying data at rest:

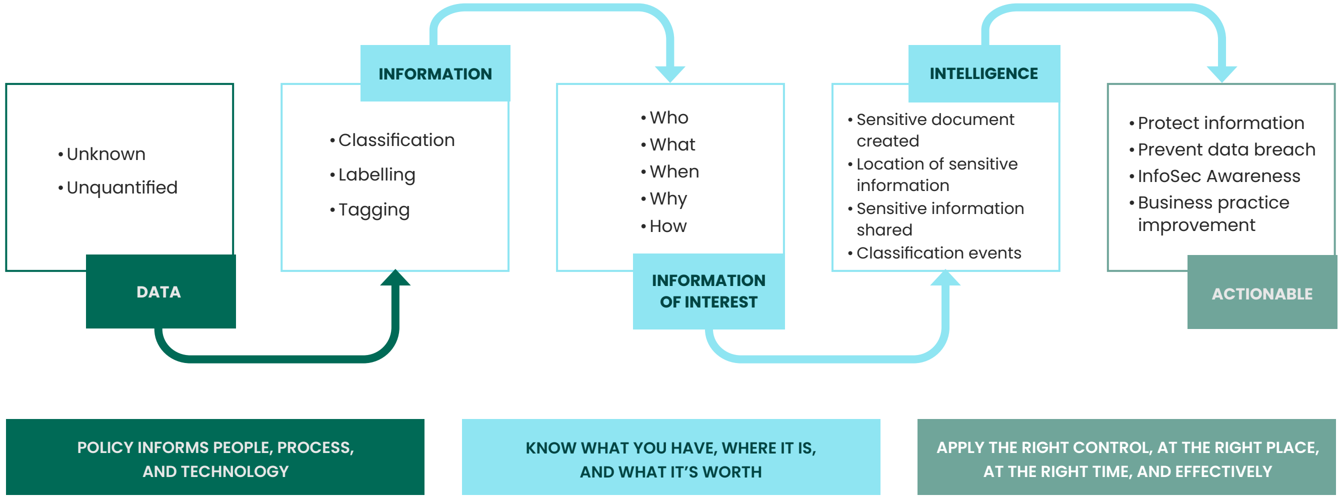


DEFINE	CATALOG	DETECT	PROTECT	MONITOR
REGULATIONS POLICIES PROCESSES	IDENTIFY PRIORITIZE ORGANIZE	SCAN LABEL CREATE PROFILES	EVALUATE REPORT IMPLEMENT	ASSESS GOVERN OVERSEE

The timeline for implementing your data-at-rest classification solution should not apply to all of your data at rest simply because you likely will need to address vast amounts of data. Instead, consider addressing data within specific repositories on an individual basis. The time required to scan and classify data within each repository will vary depending on the amount, size, type, and location of data that needs to be protected. Most organizations, however, can start to see value in their program within one or two months.

Considerations For Data Classification Evolution

Data classification is generally considered a foundational element to establishing a successful data security strategy. DCS solutions trigger the policies that identify, protect, and control data sharing based on corporate security rules and industry regulations. The application of data classification rules, policies, and metadata is the first step in a successful data security life cycle.



- Unknown
- Unquantified

DATA

INFORMATION

- Classification
- Labelling
- Tagging

- Who
- What
- When
- Why
- How

INFORMATION OF INTEREST

INTELLIGENCE

- Sensitive document created
- Location of sensitive information
- Sensitive information shared
- Classification events

- Protect information
- Prevent data breach
- InfoSec Awareness
- Business practice improvement

ACTIONABLE

POLICY INFORMS PEOPLE, PROCESS, AND TECHNOLOGY

KNOW WHAT YOU HAVE, WHERE IT IS, AND WHAT IT'S WORTH

APPLY THE RIGHT CONTROL, AT THE RIGHT PLACE, AT THE RIGHT TIME, AND EFFECTIVELY

Most organizations will embark on different projects at different times during the implementation process. While the priority of each project will differ for each organization, the objectives of translating data from an unknowN state to identifying it in a way that intelligent policies and actional protection can be applied remains the same.

The following table shows six data classification projects to support your data security life cycle.

					6
				5	Inform data governance
			4	Data security orchestration	Data security orchestration
		3	Leverage data identification	Leverage data identification	Leverage data identification
	2	Collect events for risk analytics	Collect events for risk analytics	Collect events for risk analytics	Collect events for risk analytics
1	Apply data classification policy	Apply data classification policy	Apply data classification policy	Apply data classification policy	Apply data classification policy
Label unstructured data	Label unstructured data	Label unstructured data	Label unstructured data	Label unstructured data	Label unstructured data

These projects play out as follows:

1. **Label unstructured data.** Apply metadata and tags to unstructured information at creation or at rest.
2. **Apply data classification policy.** Use policy to create logical decisions on how and when data should be classified by a user or automated means.
3. **Collect events for risk analytics.** Collect data classification events and policies for presentation in a centralized business intelligence or security information and event management (SIEM) tool, such as Splunk.
4. **Leverage data identification.** Deploy more advanced detection capabilities powered by machine learning to automatically detect privacy and unique data types defined by the organization.
5. **Data security orchestration.** Leverage DCS metadata and logs to power downstream security solutions such as data loss prevention (DLP) technologies, cloud access security brokers (CASBs), and rights management and encryption tools.
6. **Inform data governance.** Use DCS metadata to inform data governance solutions about the deletion, archiving, or retention of unstructured data.

For a more detailed breakdown of the
DCS implementation methodology, please visit:
www.titus.com/solutions/methodology

FORTRA™

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.