FORTRA™

SOLUTION BRIEF (DATA CLASSIFICATION)

Fortra's Data Classification Suite (DCS) Methodology

DCS Deployment Methodology

Our proven implementation strategy empowers any organization to successfully deploy a data classification solution based on their unique data security needs.

IT professionals understand all too well the importance of implementing some level of technology that will help secure their organization's critical data and give users a way to follow consistent information handling practices. However, "how" to accomplish a successful implementation and rollout can be complicated and perplexing.

DCS follows a well-tested methodology when helping customers deploy any of our solutions, regardless of the size of the business. First and foremost, it's critical to outline your business needs around data classification from the beginning — before actual technology discussions even begin. That means stakeholders from across your organization should be included in early planning sessions so that as the solution rolls out, everyone has an agreed-upon blueprint to follow.

Another key component of the methodology is a well-thought-out strategy for user engagement. Implementing data classification technologies is not simply a matter of flipping a switch. For true success, you've got to build a security culture within your organization, and that requires strategic communications to help everyone understand why it is important. As part of the process, DCS can help you understand how to measure and document the outcomes of your implementation so that you and your users can continue to adopt best practices as your company evolves.

This methodology was built over years working with organizations in 137 countries around the world, including more than 70 organizations with over 20,000 employees.

Educate, Empower, Enforce

The DCS Professional Services team is here to help you plan, implement and evolve your data security strategy to meet your specific organizational needs. For every organization, our deployment process follows three phases designed to help you meet three very important goals:

HIGHLIGHTS

DCS deployment process follows three phases designed to help you meet your goals:

- Educate stakeholders and employees on best practices for handling personal
- Empower users with the information and tools they need to make suggested classifications based on your organization's policies.
- Enforce your policies through data handling restrictions and integration with your other data security investments.

- **Educate.** Before any technology discussions occur, we engage with you for deep planning. Key stakeholders become steeped in the DCS deployment methodology and align on the functionality your organization needs for its data classification strategy. From the beginning of this process, you need to start building a culture of security early on to enable a smooth transition to new workflow practices. For the most secure environment, all users must be on board. Thorough communications during the planning and early design phases of your project are key to helping users understand why you are implementing the new solution, what assets need to be classified, and how they can help. They also need reassurance that their day-to-day workflow will be minimally disrupted. As your solution matures to meet your evolving needs, education will continue at the same time.
- **Empower.** DCS works with your team to configure your solution within the DCS administration console according to your requirements outlined during the design process. Initial user groups across your organization are engaged for testing and feedback to ensure all business and workflow needs have been considered. As you move into full deployment, users are empowered to make suggested data classifications based on your organization's policies — which by this time, should be very familiar to all employees. During this phase, you will continue to refine your policies and how to apply them. Integrating DCS solutions into user workflows, helps lighten the load in terms of the classification process.
- **Enforce.** As your implementation matures, you can take your data classification strategy to a deeper level. At this stage, restrictions are applied around data handling practices. It's best to layer in these restrictions after users fully understand your data classification strategy and have become accustomed to using the new technologies. By integrating DCS solutions with other data security technologies automatic security actions can be triggered for specified situations. An outside professional services provider can help ensure you get the most from all your security investments. Both users and IT admins will continue to adapt processes to the new system. Be sure to encourage feedback for ongoing policy refinement and configuration updates

Two implementation streams

Your technology team obviously plays a key role when deploying a data classification solution, but your business stakeholders are equally important.

Business Stream

Executives from the top of your organization as well as from every business area, including HR and operations, should be involved in the planning, design and implementation process. Their involvement ensures that policies meet their specific departmental needs and that approvals along the way go smoothly, with no surprises or critical missed details.

Communications about the project should come from the top-down to ensure a consistent message about the importance of data classification. You want your users to see the implementation for what it is – a business-driven project that has some IT aspects to it.

If new tools are suddenly installed on users' machines, it can produce culture shock — and resistance. If key stakeholders get involved early, they can educate users and help manifest a cultural change around security and data handling within the organization. Internal awareness and employee communications campaigns should be launched at the beginning of your implementation project and at key points in the process, with updates on how testing is going, when the solution will launch, and how training will be delivered. In addition, it should be made clear that user input is critical for the success of the new security strategy.

Technology Stream

Meanwhile, on the technology side, your IT team begins to learn all about the DCS solution and its capabilities. Up front, you'll identify key roles and responsibilities for the project, including hardware setup, change management, communications and training. As part of the planning phase, DCS reviews business policies, procedures and requirements around data protection with each client, and scopes out each phase of the rest of the project, including well-defined success metrics.

During implementation, DCS helps with the build and testing process. We conduct policy workshops to ensure our technologies are configured to meet your needs, including running through specific use case scenarios. We also work with your corporate communications team to ensure they understand the project design and support your full rollout.

As the project evolves, we help you establish a focused in-house test team and train your admins. We work with your team on the ground to integrate user feedback and make amendments to your policies as needed.

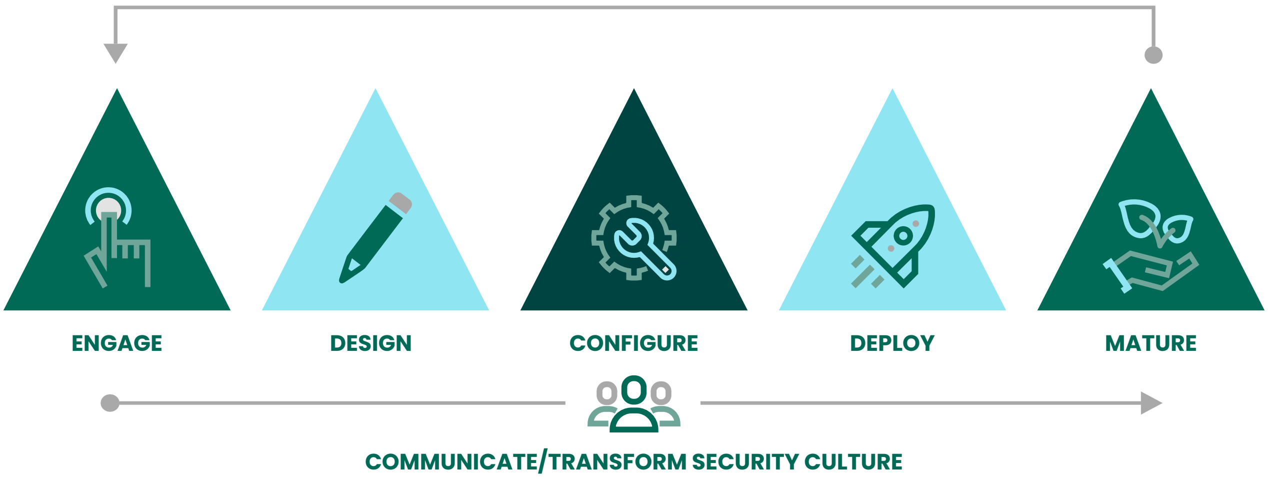
A Flexible Structure

We rely on our detailed, methodical approach to implementation so that no data security detail falls through the cracks. At the same time, we work closely with organizations to understand their unique industry and how their data handling practices might differ from other organizations'. That means each implementation process tends to look a little different from the others.

Many organizations want to know how long the process will take. It actually varies pretty dramatically between companies, depending on company size, stakeholder involvement, and approval processes. Organizations should give themselves plenty of time to truly educate business leaders as well as users on the concepts of data security and best practices of information handling.

Timelines for the sign-off process can vary greatly from organization to organization. In smaller companies and those with designated team members for approving each step, the sign-off process is likely to go more smoothly and take less time. Linking the approval process to the correct level of stakeholder is key. These stakeholders should be involved during the planning process rather than assigning a more junior-level project manager who then has to route plans around to stakeholders.

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



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.