FORTRA™

SOLUTION BRIEF (DATA CLASSIFICATION)

SAMA Compliance Support That Works For Your Business

Fortra's Data Classification Suite (DCS) Enables Financial Institutions To Effectively Identify And Minimise Their Cybersecurity Risks.

Maintaining the confidentiality, integrity and availability of customer data while safeguarding against increasingly sophisticated cyberthreats is an evolving concern. The Saudi Arabian Monetary Authority (SAMA) cybersecurity framework was developed to help you more confidently protect your customers' assets by creating a common approach to cybersecurity amongst SAMA member organisations.

DCS supports your compliance with the SAMA cybersecurity framework and helps you meet data protection obligations at home and abroad by complementing your existing cybersecurity infrastructure.

> "We see ROI through prevention. We've calculated that a breach would cost $350 per record. DCS is the vehicle we use to get effective enforcement by providing identity to the data."
>
> **— Fortune 500 customer.**

How DCS Supports Your SAMA Cybersecurity Framework Compliances

DCS works in concert with your existing cybersecurity infrastructure to help you achieve end-to-end SAMA cybersecurity framework compliance. The open, configurable policy engine enables your organisation to enforce detailed data identification and information handling policies with awardwinning machine learning, while monitoring compliance and continuously reinforcing a culture of security.

Discover

Sensitive information must be identified wherever it sits and however it is created. DCS solutions enforce identification through easily adoptable workflows, ensuring protection of all your critical information.

Classify

The powerful DCS policy engine ensures that information is classified correctly according to your information security policy. Multiple layers of classification allow for very granular control. Machine learning technology can be deployed to assess the information, recognise sensitive data and determine appropriate categories.

Protect

DCS enforces your policies across all your security systems, including messaging, data loss prevention (DLP) and electronic data rights management (EDRM) using open metadata embedded in documents at their creation.

Leaders can give their staff more freedom to innovate while knowing that sensitive information will be kept safe.

DCS supports SAMA compliance using cybersecurity controls that complement your existing security infrastructure, ensuring protection of commercially sensitive and personal data throughout your organisation and wider ecosystem.

The DCS platform is open by design, integrating seamlessly with your existing security stack. As your partner in deploying your security strategy, DCS implements our proven methodology built over 10 years of experience in data identification and security. Our solution set is designed to support compliance with the SAMA cybersecurity framework control standards to at least maturity levels 3 (operational) and 4 (monitoring).

3.3.3 Asset Management

DCS uses an advanced policy engine that applies protection according to highly granular levels of classification. You can also enable machine learning to suggest or enforce classification.

3.4 Third-Party Cybersecurity

DCS uses an advanced policy engine that applies protection according to highly granular levels of classification. You can also enable machine learning to suggest or enforce classification.

3.1.6, 3.1.7 Awareness And Training

By using DCS in their everyday work, users are continually reminded of the value of the information they encounter. Users learn to follow retention, clear-screen and clear-desk policies as well as disposal and reuse of equipment policies.

3.3.5 Identity And Access Management

By using DCS in their everyday work, users are continually reminded of the value of the information they encounter. Users learn to follow retention, clear-screen and clear-desk policies as well as disposal and reuse of equipment policies.

3.3.10 Bring Your Own Device
3.4.3 Cloud Computing

Mobile and cloud technologies are essential business tools but come with higher risk of data leakage. Sensitive data on mobile devices and in the cloud can be discovered and classified manually or automatically.

3.2.5 Cybersecurity Audits

Mobile and cloud technologies are essential business tools but come with higher risk of data leakage. Sensitive data on mobile devices and in the cloud can be discovered and classified manually or automatically.

3.3.6 Application Security
3.3.8 Infrastructure Security
3.3.9 Cryptography

Operational, DLP, EDRM and encryption systems operate more effectively with DCS. DCS classifications are implemented as persistent metadata and X-headers in data files to trigger your existing systems to engage actions and restrictions.

3.3.2 Physical Security
3.3.11 Secure Disposal Of Information Assets

DCS enables the classification of data throughout its entire life cycle, from creation and storage to destruction. Sensitive information is labelled digitally and physically on printed copies to continually remind users and third parties of the value of information when handling and sharing it.

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.