CONGRUITY | 360

DATA GOVERNANCE & DATA SECURITY FRAMEWORK:

Where Does Classify360 Fit?

DATA GOVERNANCE & DATA SECURITY FRAMEWORK: Where Does Classify360 Fit?

CONTENTS

Management and Security within the Data Security Governance Framework 1
What is Governance? 1
Data Management vs. Data Security 2

Security Market Challenges & The Shift to A Data-Focused Approach 3

Classification Enhances Your Data 3

Classify360: The First Step to Data Governance 5
Features of Classify360 Supporting Data Security & Management 6
Important Considerations 7
Classify360 & Data Security Tools 7
Classify360 & OEM File Analysis Tools 7
Classify360 & Data Quality 7

Related Data Frameworks 8
Data-Centric Security Architecture (DCSA) 8
Continuous Adaptive Risk and Trust Assessment (CARTA) 8

Classify360 Technology Matrix 10

Summary 11

Works Cited 11

Management and Security within the Data Security Governance Framework

Research has proven that no single product offering can mitigate or eliminate data risk entirely. Each organization has its own needs based on unique business requirements, regulatory guidelines, and data silos. The concept of “business risk” continuously evolves as new policies are implemented in response to technical, social, and environmental challenges. These challenges push us to reevaluate the business-critical workflows within our organizations. Rather than just implement *X* solution to meet *Y* requirement, businesses must consider how to dedicate limited resources to solutions that fulfill several business requirements.

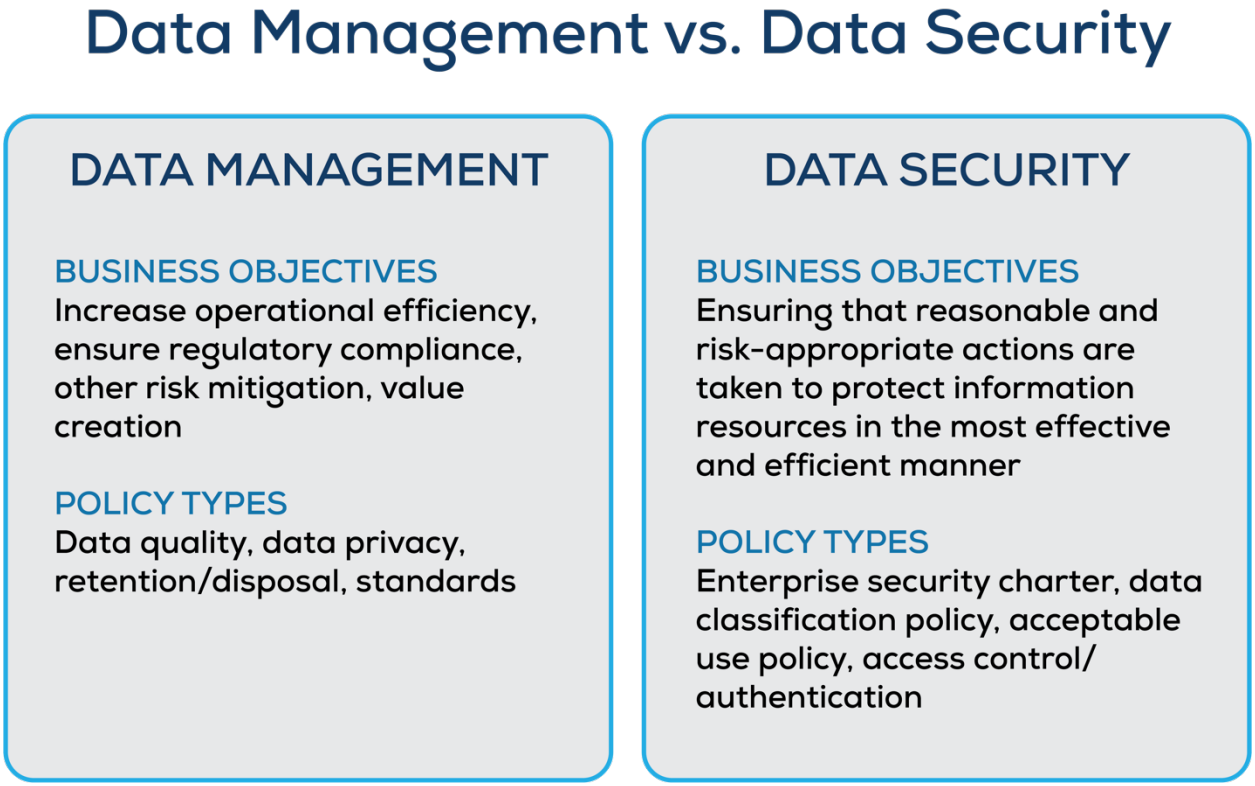
Data management and data security solutions share one primary goal: to address, prioritize, and mitigate a complex array of business risks. Classify360, Congruity360’s data classification and information governance solution, is one of many possible tools that can achieve the desired outcome. Classify360 works in the data governance stage of the data security governance framework, when the identification and proper analysis of data lays the foundation for privacy, security, and specialist tools.What is Governance?
Gartner defines "governance" as the process of:

DATA GOVERNANCE & DATA SECURITY FRAMEWORK: Where Does Classify360 Fit?

- PRESERVATION AND GROWTH OF SHAREHOLDER VALUE – Setting decision rights and accountability, as well as establishing policies that are aligned to business objectives
- COHERENT STRATEGY REALIZATION – Balancing investments in accordance with policies and in support of business objectives
- COMPLIANCE AND ASSURANCE – Establishing measures to monitor adherence to decisions and policies
- RISK MANAGEMENT – Ensuring that processes, behaviors, and procedures are in accordance with policies and within tolerances to support decisions

Data Security Governance (DSG) is the combination of Information Management Governance and Information Security and Risk Governance.

Data Management vs. Data Security



Data Management Governance

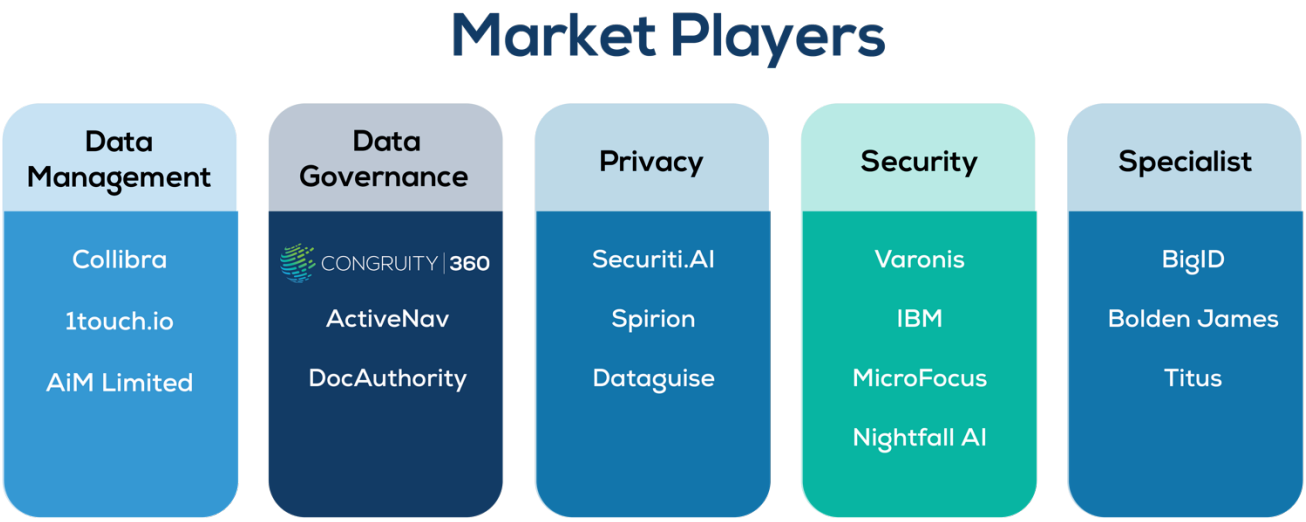
- Business objectives: increase operational efficiency, ensure regulatory compliance, other risk mitigation, value creation
- Policy types: data quality, data privacy, retention/disposal, standards

DATA GOVERNANCE & DATA SECURITY FRAMEWORK: Where Does Classify360 Fit?

Data Security Governance

- Business objectives: ensuring that reasonable and risk-appropriate actions are taken to protect information resources in the most effective and efficient manner
- Policy types: enterprise security charter, data classification policy, acceptable use policy, access control/authentication

DSG uses various modeling and assessments that illustrate how classification fits into the broader landscape of data governance.



A- Key data vendors across the data governance and data security landscape.

Security Market Challenges & The Shift to A Data-Focused Approach

Digital businesses face ever-evolving liabilities as enforcement of new data protection and privacy requirements (like GDPR and CCPA) add to compliance issues; additionally, threats of data breaches are omnipresent due to hacking, malicious insiders, and accidental disclosures. While protecting data has always been the goal for organizations, security controls historically focus on users and systems and are rarely architected to focus on the data itself or address business risk. As businesses adopt new IT infrastructure on-prem and in the cloud, they are failing to develop the proper data security policies to offset these risks.

Classification Enhances Your Data

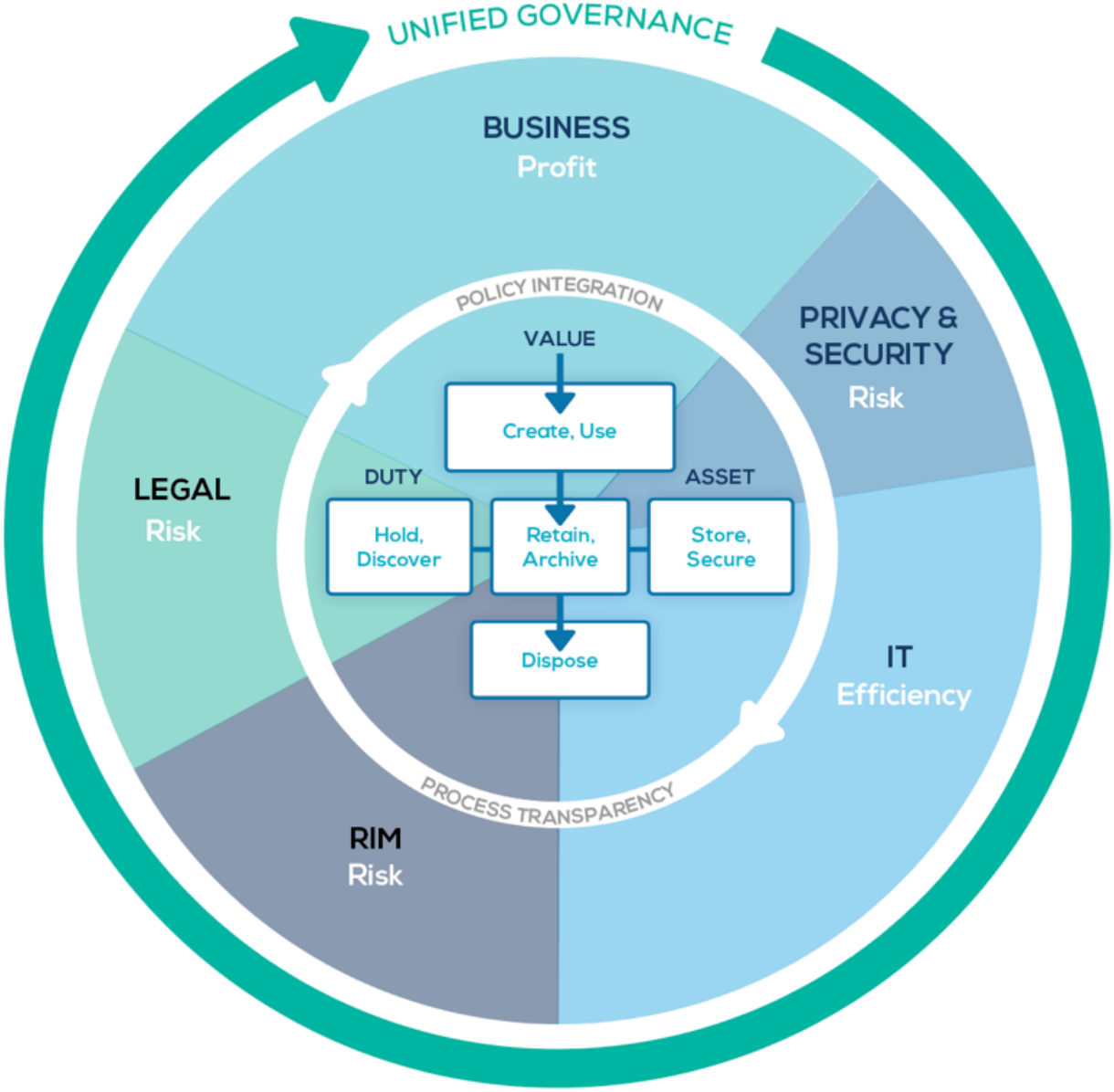
By beginning your data journey with classification, you are inputting the best quality, most relevant data into the tools you utilize. Whether data management or data security is your primary goal – or if you are focused on both – the process should always begin

with data mapping, data inventory, data discovery, and data classification to properly implement your security tools of choice.

Without identifying and properly classifying data, organizations cannot fully move forward with data governance products. Classification compiles a data catalog that supports all subsequent governance processes and maintains data quality along the way. Properly classified and indexed data enables enterprises to optimize the value of other technology investments by improving the quality of data through tagging and strategic insight. Cleaner, more accurate data for these tools produces the best possible output from a data security suite.

DATA GOVERNANCE & DATA SECURITY FRAMEWORK: Where Does Classify360 Fit?

Simply stated: better data in, better data out.



B- Gartner's model of complete unified data governance framed by policy integration and process transparency.

Classify360: The First Step to Data Governance

Classify360, a universal information engine, spans across on-prem and cloud data sources to provide content-level insight for the entire enterprise. Data is indexed behind the firewall, eliminating the risk and cost burden of creating a copy. Classify360 also leverages machine learning to provide the data insights in real-time and enable

actionable workflows. Policy tools provided by Classify360 can also help process these workflows.

Features of Classify360 Supporting Data Security & Management

- Redundant, Obsolete, and Trivial (ROT) Data Analysis
- Risk Analysis
- Data Storage Consolidation
- Retention Policy Workflows
- Metadata Injection

Classify360 compliments and facilitates the proper implementation of other technologies further in the data management and security process such as data loss prevention (DLP), enterprise metadata management (EMM), data activity monitoring (DAM), and master data management (MDM).

DATA GOVERNANCE & DATA SECURITY FRAMEWORK: Where Does Classify360 Fit?

Important Considerations

- Is granular data classification required?
- Is all data and its location known?
- Is ROT analysis required?
- Does the data include sensitive, privileged or risk data?
- Is the data subject to privacy acts or regulatory compliance?
- Is there legacy data that needs to be deleted or archived?
- Is any of the data subject to litigation or under legal hold?

Classify360 & Data Security Tools

Classify360 can be implemented alongside many data access and data usage solutions that lack robust content level classification or risk analysis, like DLP solutions. DLPs focus on security and preventing data leakage while Classify360 focuses on data management to support a broader data governance strategy.

Example technologies: Symantec, Digital Guardian, Spirion

Classify360 & OEM File Analysis Tools

Many OEM file analysis tools support use cases such as data storage consolidation, deduplication by location and cloud migration. However, these tools may lack critical classification and analysis features for complex use cases.

Example technologies: EMC Data IQ, EMC ClarityNOW, NetApp Cloud Insights, NetApp Talon

Classify360 & Data Quality

MDM solutions ensure data quality and integrity across the entire organization. This is an important component of data governance that requires a full picture of all data in the organization before MDM solutions can be successfully implemented. Classify360 provides a full analysis of the data and can be used alongside MDM solutions.

Example technologies: Informatica, TIBCO, SAP, IBM

DATA GOVERNANCE & DATA SECURITY FRAMEWORK: Where Does Classify360 Fit?

Related Data Frameworks

Data-Centric Security Architecture (DCSA)

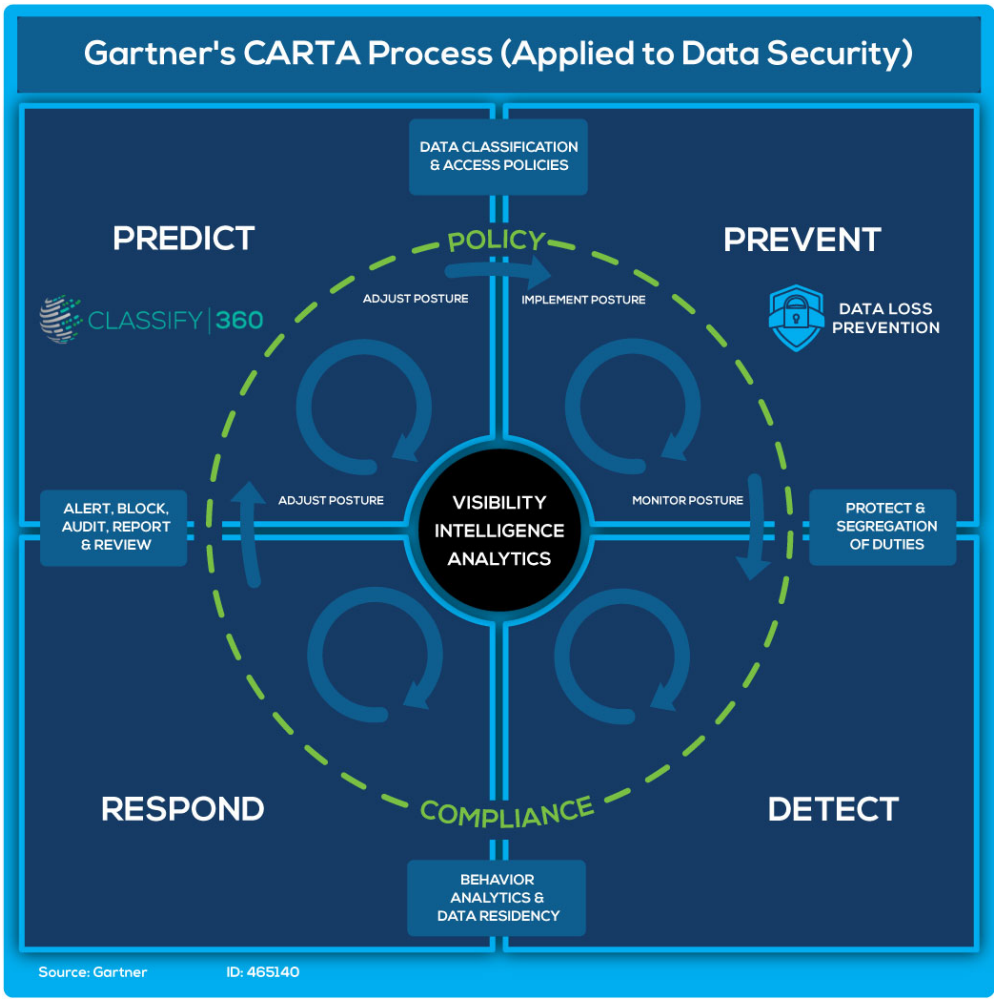
DCSA is a framework of data centric controls to discover, classify, protect and monitor data throughout its lifecycle on prem or in the cloud.

Continuous Adaptive Risk and Trust Assessment (CARTA)

CARTA is a framework used to select product security controls or policy rules across all systems and devices for interoperability with digital trust (see following image).

Both DSCA and CARTA help an organization understand its requirements for security functionality and how these requirements will be implemented at each stage in a given workflow. They are cyclical frameworks that will evolve over time and should be reevaluated and updated regularly.

DATA GOVERNANCE & DATA SECURITY FRAMEWORK: Where Does Classify360 Fit?



C- Gartner's continuous and adaptive risk and trust assessment (CARTA) envisions enterprise security infrastructure as continuously adaptive based on real-time assessments of risk/trust throughout the life cycle of a user's access.

DATA GOVERNANCE & DATA SECURITY FRAMEWORK: Where Does Classify360 Fit?

Classify360 Technology Matrix

CONGRUITY 360 TECHNOLOGY MATRIX

	CLASSIFY360	DLP	MDM	OEM FILE ANALYSIS & DATA MANAGEMENT
HOW IT'S USED	Classify360 is a universal information engine spanning on-prem and cloud sources to provide content-level insight across the entire enterprise. Data is indexed behind the firewall, eliminating the risk and cost burden of creating a copy. Machine learning is leveraged to provide real-time insights into the characteristics of data, enabling and providing actionable workflows.	Provides visibility into data usage based on the content and context of data. Address risks of inadvertent or accidental data loss, and the exposure of sensitive data. It is part of a larger data security process.	Technology enabled business discipline to ensure data quality and consistency across data silos.	File analysis and analytics tools used alongside traditional on-prem storage to optimize data management. Assist with cloud migrations and/or using OEM storage solutions as a part of a l arger cloud strategy.
INFO GOV COMPONENT	Multiple	Security	Quality	Data Management
DATA DISCOVERY	✓			Limited
METADATA DATA CLASSIFICATION	✓	✓	Limited	✓
CONTENT LEVEL CLASSIFICATION	✓			
GRANULAR, CUSTOMIZABLE DATA CLASSIFICATION TEMPLATES	✓			
ROT ANALYSIS	✓			Limited
RISK ANALYSIS	✓	Only for data usage		
EXTENSIVE DATA REPOSITORY CONNECTIONS	✓	Limited	Limited	Limited
UNSUPERVISED MACHINE LEARNING	✓	✓	Only for data quality	
SUPERVISED MACHINE LEARNING	✓	✓	Only for data quality	
SUPPORTS DATA SUBJECT REQUESTS	✓		✓	

DATA GOVERNANCE & DATA SECURITY FRAMEWORK: Where Does Classify360 Fit?

Summary

Successful information governance is an ongoing process that will not be solved with one solution. A suite of tools protecting the entire data lifecycle is required, each tool addressing specific data needs. Data workflows beginning with classification ensure more accurate, higher-quality results from all tools within a given data suite.

A successful data governance program consists of a set of formalized processes targeted at specific situations, with no one-size-fits-all approach or one solution to handle every need.

Without first identifying and classifying data, organizations cannot effectively move forward with any governance tools. No matter what the desired data outcome may be for an enterprise, it must start with Classify360.

Works Cited

- *Gartner Defines 'Governance'*. Gartner September 2015, Analyst Julie Short et.al. ID G00237914
- *Using Classification to Improve Unstructured Data Security*. Gartner August 2020, Analyst Mike Wonham ID G00726896
- *Align Information Security Governance With Your Broader Information Governance Initiatives*. Refreshed May 2016, Published August 2013, Analysts Ted Friedman & Tom Scholtz ID G00252004
- *How to Use the Data Security Governance Framework*. Gartner April 2018, Analysts Brian Lowans et.al. ID G00351128
- *How to Successfully Design and Implement a Data-Centric Security Architecture*. July 2019, Analysts Joerg Fritsch & Mike Wonham ID G00390767 *a*