Chorology.ai
KNOW YOUR DATA

Modern Data Compliance Program and Processes

A Practitioner's Guide

Summary

Welcome to "Modern Data Compliance Program and Processes; a Practitioner's Guide," an insightful resource for data compliance professionals seeking to establish modern, automated compliance programs within their organizations. In this introductory white paper, we'll delve into the intelligently automated components and processes that make up a modern, AI-based enterprise data compliance program. This overview is also designed to help practitioners navigate with confidence, the challenges in managing data security, compliance and security posture facing today's digital enterprise.

1. Introduction:

In the fast-paced digital landscape of today, where data flows freely and information is currency, one term stands out as a beacon of corporate responsibility and security: Data Compliance. As beginners and experienced professionals alike enter the complex realm of data compliance, understanding the elements of modern data compliance programs is paramount. In this white paper, we embark on a journey to demystify modern data compliance programs, shedding light on what makes their components,

processes, and solutions state-of-the-art and how these AI-based advancements future proof global enterprises and organizations of all sizes for the fast-evolving digital landscape.

Exponential Challenges for Data Compliance and Security

Important trends in the data landscape are driving the need for modern, next-level data compliance programs. Today enterprises face an exponential rise in structured and unstructured data volumes with almost 80% of companies estimating that 50%-90% of their data is unstructured (text, video, audio, web server logs, or social media activities)[1]. Recent sources state there exist on average, over 400[2] data sources per organization. More importantly global data volumes including data created, captured, copied, and consumed is expected to pass 180 zettabytes[3]. Of these 180 zettabytes of global data, a 2022 G2 Survey estimates that over 60% of it will be stored in the cloud (with global cloud data rising to 100 zettabytes by 2025)[4].

Layered on top of this hockey stick growth in data volume, enterprises are experiencing exponential rises in data breaches, cyber threats, and privacy concerns as governments worldwide tighten their data protection regulations. In the face of these exponentially rising data security and compliance challenges, businesses are rapidly investing in modern data compliance platforms to leverage AI and intelligent automation to better protect their enterprise and their customers.

The surge in data volume, regulatory scrutiny, data compliance policies and security breaches have birthed a modern data compliance industry. This next level industry of data compliance innovators are dedicated to providing intelligently automated tools, technologies, and expertise to help enterprises and organizations navigate an increasingly complex data compliance landscape.

Data Compliance and Privacy Enforcement: A Strategic Imperative

Data compliance refers to all the rules and guidelines concerning how businesses collect, store, use, and protect information. The decades-old industry has been providing tools for robust data compliance programs that help keep organizations safe while instilling trust among customers and partners. The importance of a comprehensive program extends across the entire spectrum of enterprises, irrespective of their size or industry.

For small businesses, data compliance ensures credibility and trust among customers, fostering loyalty and enhancing brand reputation. Medium-sized enterprises benefit from data compliance by streamlining operations, minimizing risks, and gaining a competitive edge in the market. Large, global corporations face substantial legal and financial repercussions for non-compliance, including hefty fines, lawsuits, and reputational damage.

[1] Statista, Taylor, 2023
[2] Matillion, 2022
[3] Statista, 2024
[4] G2, October 2022

Since its inception, data compliance has transformed from a burden on an internal team tasked with keeping up with regulations, to a strategic business imperative. To protect (exponentially expanding) volumes of data from rising cyber-attacks of increasing sophistication, modern data compliance programs must combine AI-based intelligent automation innovations in data discovery, classification, mapping, security posture management and privacy enforcement with comprehensive global data compliance standards and processes.

With intelligent automation of modern generation data compliance programs, enterprises and organizations will further demonstrate their commitment to ethical business practice and continue earning the trust of consumers and partners alike. Compliance adherence must also include automations in data security posture and privacy enforcement to enable the responsible use and sharing of data. Modern and compliant methods of data sharing will unlock new opportunities for partnering, growth and development in today's world of rising enterprise data sophistication.

The Emergence of Modern Data Compliance Programs

A new class of data compliance operators have emerged who apply AI to intelligently manage enterprise data privacy, compliance, and security. Today's modern, intelligently automated capabilities comprehensively discover and map a baseline data security posture and use this security posture and data map to quantify enterprise data privacy and compliance risk. The compliance engine maintains a comprehensive set of policies, procedures and solutions which are automatically enforced to track and mitigate this risk. This balance between an enterprise's data compliance program and the data security posture resulting from it is shown in Figure 1.

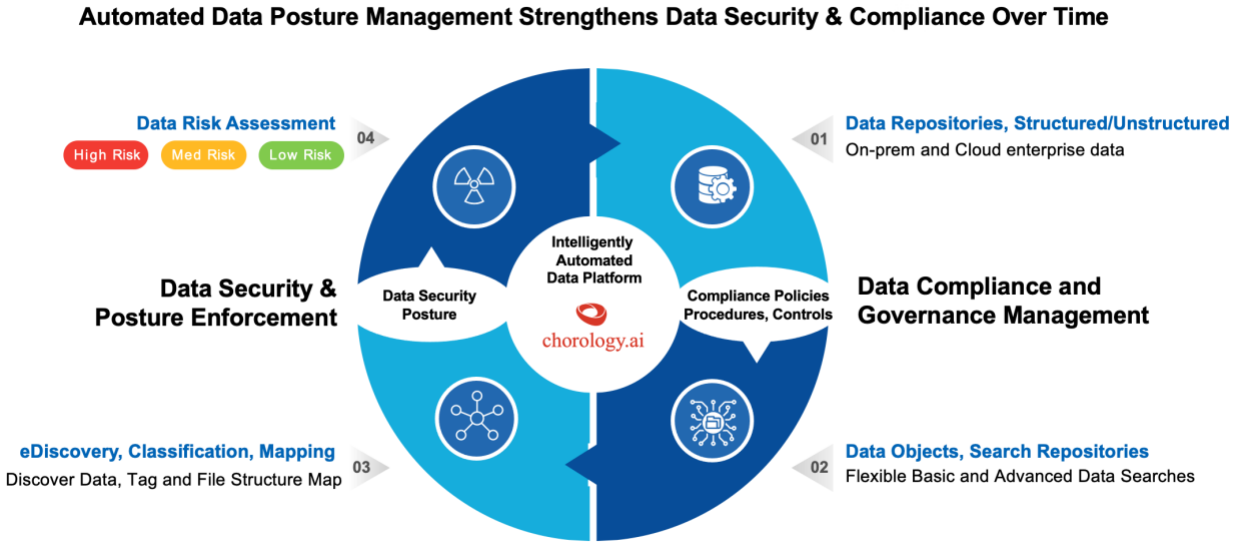

Figure 1.

The iterative process of managing your data compliance program to continuously improve your data security posture and manage data risk is circular in nature and never-ending. Intelligent AI-powered

automation of modern compliance programs increases the speed of these iterations. It is a testament to the growing significance of data in modern (digital) business enterprises.

2. Setting up a Modern Data Compliance Program

Data Governance is a Cornerstone

Setting up a modern data compliance program requires data compliance personnel to establish robust security, privacy, and compliance measures within their organization. Data governance is the first focus and cornerstone of any effective data compliance program. It is the set of processes, policies, and standards established to ensure the proper management, quality, and security of an organization's data assets throughout their lifecycle.

How is Data Compliance Different from Data Governance?

Data governance provides a framework for decision-making, accountability, and risk management related to data within your organization - from data collection to disposal. The data compliance program is then the framework and platform that ensures your organization adheres to laws, regulations, and standards governing the collection, processing, storage, and sharing of data. Your modern data compliance program ensures that organizations can intelligently handle data ethically, transparently, and securely, in compliance with regulatory requirements in the most efficient and scalable manner. Your data governance framework is therefore a foundational block and enabler for the effectiveness of your modern data compliance program.

How to Evaluate Your Current Data Compliance Program

Now more than ever, businesses and organizations need a scalable data compliance program that can understand and manage their data security posture. In addition, intelligent automation is needed to adequately manage data risk while enforcing privacy laws, regulations, and standards governing the collection, storage, processing, and sharing of data at scale.

Examples of regulations affecting both your data security posture and enterprise data risk include a spectrum of rules ranging from regional privacy laws like GDPR (General Data Protection Regulation) in Europe to industry-specific standards like HIPAA (Health Insurance Portability and Accountability Act) in the healthcare sector, or even state-level compliance like CCPA (California Consumer Privacy Act).

Questions to consider when assessing a Modern Data Compliance Program should include:

Compliance Policies, Rules, Laws

- Does your compliance program contain all the policies and rules of global data regulations relevant to your industry?
- Does your compliance program receive updates automatically as regulations change?

Data Discovery, Classification and Mapping

- Does the core of your data compliance program have a deep AI learning engine that can automatically discover, classify, and map your data security posture?
- Does your program create a comprehensive understanding of sensitive structured and unstructured data across all your cloud and on-prem enterprise repositories?
- Does your program automatically classify and map your sensitive data so your compliance team can accurately see which type of classified data is stored where?

Data Risk Posture Management

- Does your program automatically output a measure of risk for each category of your sensitive data as part of your data security posture?
- Can your compliance platform automatically quantify data compliance risk based on the rules, policies and laws codified in your compliance program?
- Does your program automatically dashboard your security posture resulting from the policies, processes, and solutions of your data compliance program?

Automated Compliance and Privacy Enforcement

- Can your program auto-enforce safeguards while monitoring this data posture to reduce data risk, protect data privacy and prevent data misuse?
- Is your compliance enforcement automated to help your data compliance personnel develop new policies and procedures at scale?
- Does automation exist to help personnel more responsibly, ethically, transparently, and securely handle data while safeguarding individuals' sensitive data stored in the enterprise?

3. Modern Data Compliance: New Building Blocks

Modern data compliance programs are now designed to dramatically increase the effectiveness, efficiency and scalability of data privacy and compliance with new building blocks based on intelligent automation.

Three building blocks are illustrated in the figure below. The output is a persistent map or Universal Data Map (UDM) for the data/information objects that exist in the enterprise corpuses representing what data type resides where. These intelligently automated data compliance components are summarized in Figure 2.

Figure 2.

Automatic Data eDiscovery

The first component of modern data compliance is the ability to accurately discover an increasingly more complex set of relevant data/information in a large corpus. In this modern paradigm, a new type of compliance or IT professional configures “data objects” first, using a front-end tool to define sensitive data using “Basic” and “Complex” data objects.

These data objects are then grouped or combined and scheduled as backend enterprise repository searches. Data connectors provide access for these searches to run continuously across all on-prem and cloud data stores to discover sensitive data by matching configured data objects across structured and unstructured repositories. By first defining what types of data are sensitive, compliance personnel can then let the “deep-AI core” do the heavy lifting of discovering sensitive data automatically, intelligently, and at scale.

Automatic Data Classification

Sensitive data identified across enterprise repositories must also be auto classified by compliance type to properly enforce compliance requirements such as GDPR, CCPA and other compliance mandates. Modern data compliance platforms that configure data objects, also must enable metadata tagging at scale by classifying sensitive data in real-time as it is discovered and identified. Sensitive data is auto classified in real-time as it is discovered, in any specified format, without human intervention, enabling very accurate data classification at significant scale and speed.

Automatic Data Mapping

The next data/information privacy component is automatic data mapping - the process of creating an inventory of all relevant data/information that exists in an enterprise’s corpus and mapping it out over the enterprise’s data infrastructure. A modern data mapping system automatically creates a persistent and logical layout of what type of data resides where across all the enterprise’s repositories. Comprehensive, global data mapping is an automated, scalable process enabled by AI, that replaces the “data inventory” step in legacy compliance programs, and greatly facilitates efficient navigation to sensitive data across large storage systems and corpuses.

Automated Risk Assessment and Remediation

After a persistent global data map is created across all data repositories, a risk profile is created based on data classification and compliance rules that quantifies the financial risk for enterprises. This risk profile takes the form of a data risk assessment for all the sensitive structured and unstructured data stored, with clear visual illustrations of both the classification type and its location across the enterprise. Sophisticated mechanisms can then remediate the risks identified. An example of this visual illustration is in Figure 3.

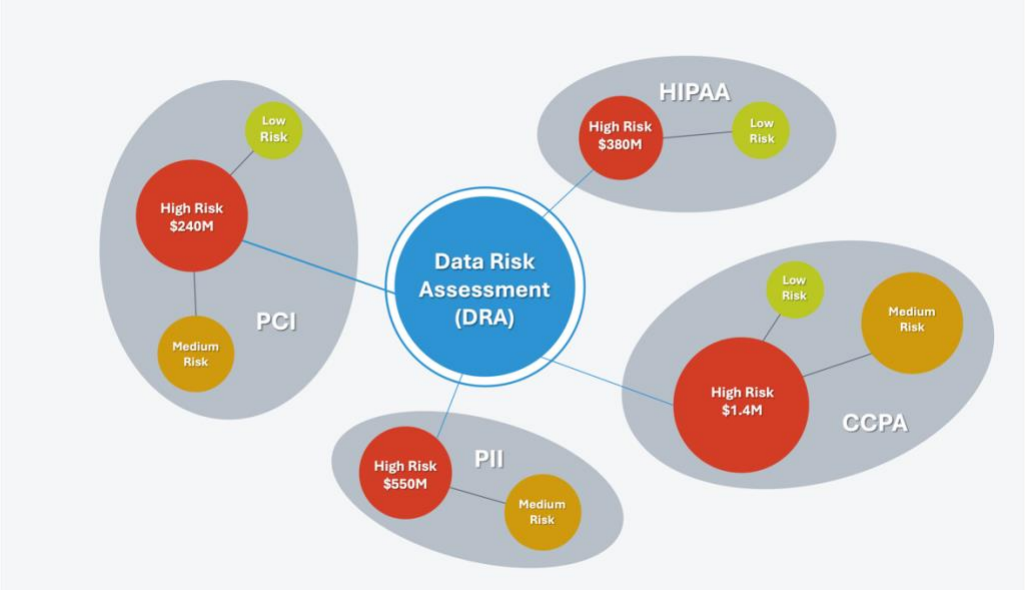

Figure 3.

Enterprises conduct risk assessments to evaluate the likelihood and impact of compliance breaches, prioritize mitigation efforts, and allocate resources effectively. Continuous monitoring and adjustment of risk management strategies ensure proactive risk mitigation.

Automated Data Subject Access Request (DSAR) Handler

In addition to having a global data map and an understanding of the relative risk of sensitive data, every enterprise must respond to incoming DSARs and DSRs. In the data privacy world, a DSR refers to the realm of "Data Subject Rights", meaning the legal rights that consumers or users ("subjects") have, to obtain a copy of their personal information and other supplementary information (by filing out a DSR request)[5]. A DSAR, (not to be confused with a DSR) is a "Data Subject Access Request" in which an individual can request access to their personal information/data an enterprise stored, and can also request the enterprise delete, correct, transfer their data, or opt out of collecting or sharing their personal data[6].

At the rate of today's exponential growth of data, a modern data compliance program (especially consumer data compliance) and its workflows MUST have the ability to handle DSRs and DSARs efficiently, in a timely and scalable manner. Manual legacy DSAR workflows are often very inefficient. The OPEX of an enterprise with a legacy compliance program will (unacceptably) grow exponentially with data volume as compliance personnel respond to rising inbound DSARs and DSRs.

A modern, intelligently automated DSAR workflow employs a "deep AI engine" and a DSAR Handler. These can automatically discretize or "parse" the incoming DSAR or DSR jobs into corresponding sets of 'primitives' (or atomic) tasks that then become actionable by a system. The parsed tasks are automatically "serialized" into a "task sequence" that understands logical and "precedence" dependencies between tasks in the sequence. The

[5] https://www.datagrail.io/blog/data-privacy/what-is-a-dsr/
[6] https://termly.io/resources/guides/dsar/

modern compliance system must also provide access control to repositories. The concepts of (job) "actors", "actor's job entitlement" and "segmentation of duty" must be present with the proper business logic between data objects and relevant actors, to control which system actors or processes can access to edit which repositories in fulfilling an inbound DSAR or DSR. In this model, relevant actors serve as "custodians" of data objects - building on the foundation laid by mapping data objects in the Discovery, Classification and Mapping phases of intelligent automation. In summary, an intelligently automated compliance program handles inbound data requests by automatically generating primitive tasks from the DSARs and DSRs, assigning these tasks to actors, which are then dispatched for execution to service the users' data requests.

Automated Data Security Posture Management (DSPM)

Data security posture management (DSPM) is a "cybersecurity technology that identifies sensitive data across multiple cloud environments and repositories and assesses its vulnerability to security threats and risk of regulatory non-compliance"[7].

With sensitive data risks quantified and compliance violations identified and remediated, a modern data compliance program can intelligently automate the management of its Data Security Posture. Modern compliance programs must be able to output a clean Data Security Posture and then be able manage this posture by automatically formulating actions to maintain it. Each component of a modern data compliance program ,(efficiently powered by a deep AI engine from Discovery to Mapping to DSAR/DSR Handling), is designed to monitor and elevate the data security posture of an enterprise over time automatically and comprehensively.

4. How to Think About Where to Begin

As one of the first vendors to re-imagine data security, privacy, and compliance by working with enterprises of all sizes, CAPE's team has seen that legacy enterprise data compliance programs fall into four categories of "compliance readiness". A modern data compliance mindset with intelligent automation powered by a deep AI engine, will significantly and positively impact enterprises falling into each of these four states of compliance readiness.

Ad Hoc Compliance Readiness

Organizations in the **ad hoc readiness** category have minimal or inconsistent data compliance practices in place. Compliance efforts are typically reactive, with little formal structure or oversight. A modern data compliance program with intelligently automated processes can create a stair-step improvement in compliance readiness, by enabling the company to become proactive. Comprehensively updated regulations, and automated compliance activities with AI-powered workflows will effectively manage compliance and security posture proactively, with minimal dedicated resources.

Defined Compliance Readiness

Organizations in the **defined readiness** category have begun to formalize their data compliance practices

[7] https://www.ibm.com/topics/data-security-posture-management

but still have room for improvement. They have established basic policies, procedures, and controls for managing compliance, but these efforts may not be consistently applied across the organization. A modern data compliance program with intelligently automated workflows, will significantly improve process consistency across the organization. Enabled by these consistent and automated workflows, the enterprise will then be able to scale its compliance program while embracing new regulations as they emerge over time.

Managed Compliance Readiness

Organizations in the **managed readiness** category have implemented mature data compliance programs with defined processes, controls, and oversight mechanisms. They have established a culture of compliance throughout the organization, with dedicated resources and leadership support for compliance initiatives. Compliance activities are integrated with broader business operations, and there is ongoing monitoring and reporting of compliance performance.

In these managed data compliance programs, we find CISOs, and their compliance teams can map, identify, quantify, and remediate risks of stored sensitive data on-prem and in cloud. Intelligent automation gives them additional control over their data security posture with more consistent processes to manage and scale their posture. By addressing each type of data risk produced by a data security posture, these teams can more quickly understand and act on the cause-and-effect relationship between their data policies and procedures and their data risk, while elevating their data posture quickly and efficiently.

Optimized Compliance Readiness

Organizations in the **optimized readiness** category have achieved the highest level of data compliance program maturity. They have implemented best practices and continuous improvement processes to optimize their compliance efforts continually. Compliance is ingrained in the organization's DNA, with a focus on innovation, efficiency, and risk management. These sophisticated organizations are best positioned to leverage intelligent automation in data compliance because their current rules and policies are already managing data risk. With modern data compliance technologies, these organizations can further reduce their overall data risk posture, by establishing, tracking, and managing data risk and security postures for each of their business units operating in their respective regulatory compliance environment.

With the efficiency of intelligent automation, the corporate compliance and privacy organization can cost effectively customize and manage a data compliance program for each BU while maintaining consistent processes and procedures across the organization. With a consistent, modern, and efficient data compliance, security, and privacy platform, each BU can scale their separate compliance program resulting in cost efficiencies for the entire corporation. Since the intelligent automation of a modern compliance program is designed to work across any compliance regulation (SOCs, Privacy, GDPR, HIPPA, or regional compliance laws like CCPA) the corporation will also be futureproofed for each new data, privacy, and security regulation as these emerge.

5. Conclusion

Modern data compliance programs leverage deep AI to intelligently automate the data discovery, classification, mapping, security posture management and privacy enforcement of global data compliance standards and processes. These modern components, policies and procedures enable a new class of efficient, highly scalable, and responsible data management in the digital age. Intelligent automation powered by AI changes the paradigm from inconsistent data compliance programs always reacting to new regulations, into proactive, quantifiable, and scalable data compliance processes with automation to optimize policies and improve data security posture and risk.

By having the ability to efficiently assess, manage and control data risk, organizations will increase their confidence in their data security, privacy, and compliance operations – even as their business evolves. They will also quickly increase their proficiency in responding to changes in today's dynamic data compliance landscape while futureproofing their compliance organization for tomorrow's regulatory environments.

About Chorology

CHOROLOGY is headquartered in San Jose, Silicon Valley, California with development offices in South Asia. Contact info@chorology.ai, (408) 713-3303, 2001 Gateway Place, Ste: 710 West Tower, San Jose, CA-95110, USA. Learn more by visiting www.chorology.ai.