Informatica

Workbook

Get Compliance-Ready with Integrated, AI-Powered Data Management

A step-by-step adoption guide for CDOs

Where data & AI come to LIFE

Contents

Introduction

As we move into 2025, significant shifts and disruptions are reshaping the modern enterprise. Technology advances, such as generative AI (GenAI) systems, are entering into the mainstream. Sustainability has become a vital business imperative, while AI-powered cybersecurity threats highlight the growing need to protect data. Hyperautomation[1] is driving greater enterprise intelligence.

A common thread that crosses each of these areas is the challenge of managing increasingly complex regulations. For organizations to remain competitive, they must stay compliant.

Enterprise Key Compliance Trends:

ESG Compliance: Shifting from voluntary to mandatory, ESG requirements are central to business operations. Companies now need to disclose their environmental impact, social responsibility and governance practices.

Data Privacy and Cybersecurity: With increasing data breaches, regulations tighten. Strong data governance is essential to comply with GDPR, SOX, HIPAA, and avoid severe penalties (e.g., $1.8 billion in GDPR fines in 2023).[2]

AI Regulation: AI boosts business opportunities but poses governance challenges. New regulations focus on transparency, fairness and accountability in AI use.

Transparency and Accountability: Enhanced regulations demand greater transparency in ownership, supply chains and Anti-Money Laundering. Regular risk assessments help align with compliance standards.

Technological Integration: Traditional data management practices are outmoded. AI-powered automation is key, using an integrated, modular platform to enhance compliance and manage AI risks.

Of 350 chief information security officers recently surveyed on the new DORA fulfillment preparations, 47% of those in the UK and 38% in the EU said their organization spent over €1m on compliance.[3]

[1] https://www.forbes.com/sites/bernardmarr/2024/09/30/the-5-biggest-business-trends-for-2025-everyone-must-be-ready-for-now/
[2] https://www.cpomagazine.com/data-protection/lessons-learned-from-gdpr-fines-in-2023/
[3] https://www.infosecurity-magazine.com/news/dora-compliance-costs-soar/

Purpose of the Guide

This guide is designed to help organizations like yours streamline and enhance regulatory compliance efforts amid growing regulatory complexity. Balancing data management with compliance standards and business growth is no small feat.

That's where **Informatica Intelligent Data Management Cloud** (IDMC) comes in. It offers a complete solution for managing your data efficiently, boosting compliance, reducing risks and opening the door to better business opportunities.

Our goal with this guide is to demonstrate how IDMC supports seamless compliance and maintains trust in today's ever-changing regulatory landscape.

IDMC Compliance Capabilities:

Data Catalog
Automatically discover, classify and catalog data across the enterprise, helping to ensure that sensitive data is identified and managed according to regulatory requirements, such as GDPR and CCPA.

Data Integration
Facilitate the accurate and secure integration of data from various sources. Maintain data integrity and compliance with regulations by providing a single, consistent view of data.

Master Data Management (MDM)
Enable accurate, consistent and complete data across the organization, essential for compliance with regulations that require accurate reporting and data consistency.

Data Governance
Provide a comprehensive data governance framework that includes policies, processes and standards to ensure data accuracy, security and compliance, helping your organization meet regulatory requirements and maintain data integrity.

Access and Privacy
Protect sensitive data from unauthorized access and breaches with automated, policy-based security and privacy controls to support data protection regulations.

Data Quality
Maintain high standards of data accuracy, completeness and reliability, crucial for compliance with regulations that require accurate and reliable data for reporting and decision-making.

Data Marketplace
Support secure and governed data sharing within the organization to facilitate responsible data sharing and in compliance with regulatory requirements.

API and Application Integration
Integrate various applications and data sources securely, helping ensure that data flows are managed in compliance with regulatory standards.

Part One

Conquering the Compliance Frontier

The regulatory landscape is complex, and the mandate for compliance programs continues to expand. Managing compliance risk now includes areas such as environmental, social and governance (ESG) and inclusive work practices.

As KPMG forecast in their *Ten Key Regulatory Challenges of 2025* report, "2025 will be the Year of Regulatory Shift fueled by a new Administration, agency leadership changes, and expanded regulatory divergence. Companies will look to 'roll through the shift' but must remain vigilant to potential new, emerging, and downstream risks — even amidst an agenda to reduce regulatory burden."[4]

Enterprise Key Compliance Challenges:

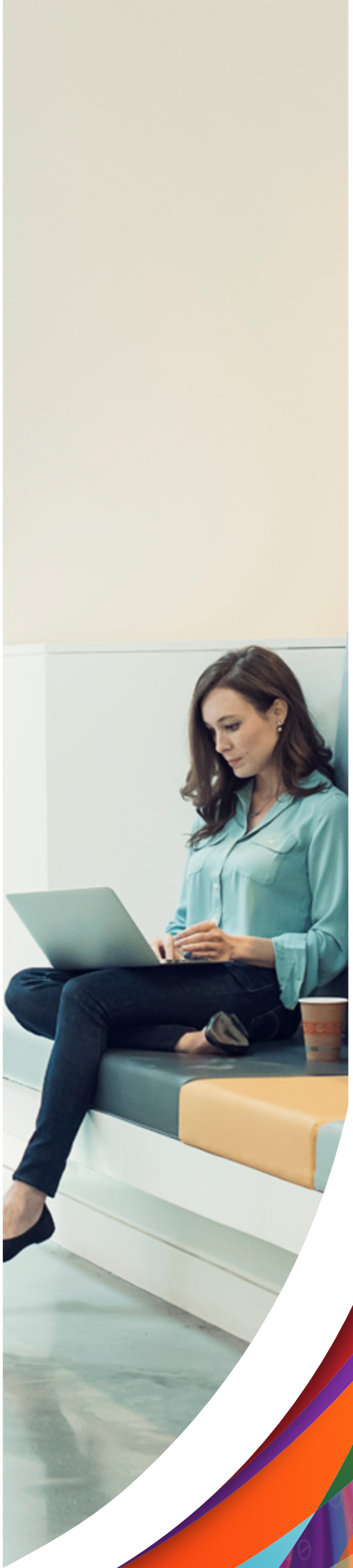
1. **Enabling Trusted Reporting for Regulatory Compliance**: Protect customer data and operations, developing robust programs for data privacy and regulatory adherence through strong governance and policy alignment.
2. **Enhancing Operational Efficiency**: Improve productivity, detect risks and reduce costs by streamlining compliance operations using technology, training and data analytics.
3. **Managing Regulatory Complexity**: Address challenges of global reporting requirements and mitigate financial risks from compliance lapses.
4. **Maintaining Reputation and Trust**: Uphold customer privacy and data integrity to reinforce brand reputation, align with regulatory and ESG standards, and ensure reporting transparency.
5. **Ensuring Unified Reporting**: Reduce costs, non-compliance risks and penalties with centralized reporting for efficient data management.

88% of global companies say that GDPR compliance alone costs their organization more than $1 million annually,[5] while 40% spend more than $10 million.[6]

[4] https://kpmg.com/kpmg-us/content/dam/kpmg/pdf/2024/ten-key-regulatory-challenges-of-2025.pdf
[5] https://www.itgovernance.eu/blog/en/how-much-does-gdpr-compliance-cost-in-2020
[6] https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/privacy-reset.html

6. **Driving ESG & Sustainability**: Tackle ESG data challenges to drive operational efficiency and competitive advantage while respecting diverse regulations.
7. **Enabling Technology Integration**: Support collaboration, data insight, efficient operations and compliance by using automation and real-time monitoring.
8. **Promoting a Compliance Culture**: Ensure accountability and overcome change with risk management, training and transparency.
9. **Establishing Data Democratization**: Foster continuous learning with AI fluency to ensure adaptation to evolving regulations by enabling accessible data with policy controls.

Compliance lapses can lead to fines, penalties and remediation expenses, with GDPR fines of up to 4% of a company's annual global turnover.[7]



[7] https://www.gdpradvisor.co.uk/gdpr-fines-and-penalties

Step One

Define Goals and Objectives

First things first. Let's start by developing a comprehensive compliance strategy. This is about helping your teams maintain safe and efficient data management processes, while ticking all the boxes for business goals and adhering to relevant regulatory mandates.

Remember those key challenges we discussed earlier? Our aim is to tackle them head-on as you work through the exercises in this workbook. Keep these challenges in mind to ensure your goals and objectives are not only comprehensive but also directly responsive to the pressing issues of your organization.

A compliance strategy with well-defined goals and objectives establishes a strong foundation for a compliance program that everyone can get behind. This is key to setting your organization up for success.

Let's dive into some of the critical goals you should consider for a robust compliance strategy, detailed in Figure 1 below:

Step	Consideration for compliance objectives	Example objectives	Use this space to draft your compliance objectives and align them with the listed consideration
A. **Clarity**	Compliance objectives should be easily understandable, unambiguous and clearly articulated for all stakeholders involved.	*"Ensure all departments comply with the General Data Protection Regulation (GDPR)."*	
B. **Measurability**	Objectives must be measurable to evaluate progress and assess compliance levels. Organizations must define quantifiable metrics or key performance indicators (KPIs) to track their compliance efforts and identify areas for improvement.	*"Achieve 100% compliance with the GDPR principles policy."* *"Maintain a 98% accuracy rating in reporting data incidents to regulatory bodies."*	
C. **Timeliness**	Setting specific yet realistic timelines helps ensure that compliance-related activities are completed within the expected timeframes and reduces the risk of non-compliance due to delays.	*"Respond to and fulfill all data subject access requests within the 30-day timeframe mandated by GDPR".*	

D. **Accountability**	Defining compliance objectives assigns responsibility to specific individuals or teams, fostering a culture of accountability. Establish clear lines of accountability to encourage proactive management of compliance tasks and adherence to policies.	*"Designate the IT department with the responsibility of maintaining accurate records of all data processing activities."* *"Designate the HR department to deliver GDPR training to all employees annually."*	
E. **Alignment with regulations**	Compliance efforts must be aligned with relevant laws, regulations and industry standards. Keep objectives up to date with regulatory changes to help avoid potential violations and mitigate compliance-related risks before they escalate.	*"Ensure compliance with GDPR Chapter V by using approved mechanisms for international data transfers."*	
F. **Continuous improvement and adaptability**	Compliance objectives should encourage continuous improvement in compliance practices. Regularly evaluate and review objectives, allowing organizations to identify areas for enhancement, implement necessary changes and assess how effectively compliance activities are meeting their intended outcomes.	*"Improve organization GDPR compliance scores by 10% annually."* *"Strive for a 5% annual increase in overall data quality metrics."*	

Figure 1. An exercise to set clear goals and objectives for managing compliance within a robust framework.

Genesis Energy reduced operating costs and compliance risk
By using Informatica CDQ scorecards and exception reports, Genesis's customer operations team saved thousands of dollars in monthly operating costs and reduced pricing compliance risk.

READ MORE

Step Two

Build a Roadmap for Success

Let's take the process a step further by creating a roadmap to success based on your goals. This will help you adopt the right compliance plan, supported by ideas on best practices.

Ready to dive into the following 6 stages to map out your journey? Let's go.

1. ASSESSMENT

Figure out where your organization stands with regulatory compliance and determine areas where you can improve. You'll want to establish a baseline, pinpoint risk areas and make sure resources are allocated effectively. The aim here is to drive continuous improvement by staying adaptable to changing regulations and operational needs.

Use the checklist below to get started with the assessment phase of your roadmap:

- ❑ Do we have a comprehensive inventory of data? Do we know where our sensitive data exists?
- ❑ What data management policies are in place?
- ❑ What metrics are in place to evaluate compliance performance?
- ❑ Is compliance documentation maintained? How is it reported?
- ❑ Who is accountable for data and AI compliance matters?
- ❑ Other _____

Best Practices

- Make sure to include key stakeholders in the compliance process right from the outset. This helps ensure everyone is on board and facilitates smooth implementation.
- You'll also want to get secure alignment with executive leadership to prioritize compliance efforts, allocate necessary resources and build a strong communications plan. Deloitte outlines this "regulatory engagement function" (REF) approach in their report, "Regulatory Management as a Strategy."[8] Check out Figure 2, Page 4 of the report for more details.

[8] https://www2.deloitte.com/content/dam/Deloitte/us/Documents/Advisory/us-advisory-regulatory-management-as-strategy-june-2024.pdf

2. IDENTIFICATION

Set the foundation for your compliance programs by recognizing and evaluating significant compliance elements and any gaps that could impact the organization. Make it a priority to stay abreast of current regulations and take a proactive approach in handling potential compliance challenges.

Use the checklist below to explore insights about your current compliance initiatives:

- ❑ Are we up to date with the latest data and AI regulations? Are there compliance gaps?
- ❑ Are there gaps in stakeholders engaged in compliance?
- ❑ Have we identified and assessed risks associated with data and AI?
- ❑ What data protection measures are in place to mitigate risks?
- ❑ Is there a well-defined incident response plan for compliance breaches?
- ❑ Other _____

Best Practices

PWC advocates setting up a control mechanism by conducting a gap assessment and benchmarking of internal governance.[9] This process involves understanding regulations, industry standards, and internal policies, defining key controls and risks, engaging appropriate stakeholders (using frameworks like REF), and leveraging technology for better process automation to enhance operational efficiency.

[9] https://www.pwc.ch/en/services/consulting/governance-risk-and-compliance.html

3. ACTION

Now, turn those assessments and plans into concrete steps that ensure regulatory adherence. Make sure your practices align with regulatory requirements and put systems and processes in place that support ongoing compliance.

Use the checklist below to guide the implementation of your compliance strategy and plug identified gaps:

- ❑ Align data management policies and practices with regulatory requirements.
- ❑ Define, document and communicate data usage policies to stakeholders.
- ❑ Enforce policies governing data integration, quality, access, retention and disposal.
- ❑ Implement mechanisms for regulatory reporting and audit trails.
- ❑ Explore opportunities to boost efficiency with AI in compliance-related tasks.
- ❑ Other _____

Best Practices

- Set clear data governance policies that align with compliance requirements to ensure data integrity and accountability.
- Establish accurate and transparent reporting mechanisms that stakeholders can rely on for decision-making.
- Implement systems that provide a consolidated view of all compliance-related reporting, minimizing the risk of oversight.
- Use the latest technologies and tools to automate and enhance compliance processes, reducing manual workload and potential human error.
- Ensure transparency across the value chain when leveraging data to enhance business performance; and align data with analytics for decision-making processes that affect business outcomes.

Informatica's Data Strategy Playbook shows how a strong data governance strategy turns data vision into value for each business function. Refer to the table on page 6 for insights on how these functions align to create and capture business value while addressing risk and compliance.

4. MONITORING

At this stage, focus on ensuring effective regulatory adherence through continuous tracking and improvement. Ongoing tracking, evaluating and enhancing of compliance measures helps ensure their effectiveness.

Consider the checklist items below as a starting point to navigate the basics of monitoring compliance programs:

- ❑ Set up dashboards to provide sufficient insights for tracking compliance performance.
- ❑ Build a cadence for conducting audits and assessments to ensure compliance.
- ❑ Deploy methods to evaluate AI systems for identifying and mitigating bias.
- ❑ Maintain documentation of compliance procedures and actions taken.
- ❑ Conduct simulation exercises to test response plans for breaches or AI failures.
- ❑ Other _____

Best Practices

- Implement continuous monitoring practices to assess compliance status and promptly identify areas for improvement.
- Be agile in updating compliance practices to adapt to regulatory changes and new organizational needs.

Continuous compliance means security measures and policies are not just static checkpoints but actively and consistently enforced. The **Splunk framework** illustrates that achieving continuous compliance involves embedding compliance deeply into an organization's operations through seven key steps, including assessment and planning, policy management and training, continuous monitoring and establishing feedback loops to measure its effectiveness.

---

5. REPORTING

Demonstrate effective compliance efforts to build trust and transparency. Establish a framework for continuous learning and adaptation to evolving regulatory landscapes. Keep all stakeholders informed about the progress, changes and expectations to ensure transparency and accountability.

Set up a compliance reporting framework that can effectively support your organization's needs, by doing the following:

- ❑ Make compliance documentation accessible for review by internal and external parties.
- ❑ Establish clear communication channels for reporting compliance issues or breaches.
- ❑ Deploy collaborative platforms for reporting policy and compliance updates.
- ❑ Report findings from periodic security audits and vulnerability assessments.
- ❑ Implement feedback systems to capture inputs on compliance processes.
- ❑ Other _____

Best Practices

- Make sure data is accessible across organizations to promote data-driven decisions, vital for effective compliance reporting. This enhances team collaboration, accountability and a culture of learning. Real-time data and a single source of truth are crucial for aligning teams with shared goals.

Gras Savoye centralized views to boost compliance
Gras Savoye's compliance journey with Informatica involved creating a consistent, centralized view for enhanced compliance with KYC requirements and a better way to manage the risk of fraud and financial exposure.

READ MORE

6. TRAINING

Empower your employees and foster a compliance-focused culture. Run awareness programs to educate your team about applicable data protection laws, ensuring they understand their legal responsibilities and the importance of safeguarding data.

By building a knowledgeable workforce that understands and prioritizes regulatory obligations, you'll help reduce risks and support the organization's compliance goals.

Use the below checklist to examine and determine the training needs of your organization:

- ❑ Drive awareness programs about applicable data protection laws.
- ❑ Improve data literacy for a better understanding of responsible AI principles.
- ❑ Up-level proficiency in data collection, storage and handling techniques.
- ❑ Keep training materials up-to-date and easily accessible.
- ❑ Measure training effectiveness and identify areas for improvement.
- ❑ Other (Please add your own examples here) _____

_____

Best Practices

- Ensure users are well-trained in compliance procedures and familiar with relevant tools. Continuous support is crucial for maintaining compliance effectiveness, integrating guidance into daily workflows.
- Enhance support and training by hiring local compliance teams in high-risk areas, offering rewards and recognition for ethical behavior, and conducting trust-focused investigations.

"Compliance is critical to every part of an organization. It helps to define its culture, build trust with customers, suppliers, investors, regulators and other stakeholders and gives it a license to operate in a global market that expects transparency and the highest standards from leaders and employees. This means the human dimension of compliance is evolving as quickly as the regulations." – **PwC Global Compliance Survey 2025**[10]

[10] https://www.pwc.com/gx/en/issues/risk-regulation/global-compliance-survey.html

Regulatory Compliance Roadmap: An Iterative Journey

The dynamic and evolving nature of regulatory and business landscapes demands that CDOs and data leaders consider compliance an iterative journey. New regulations and developments require continuous adaptation of compliance strategies.

As PwC's Global Compliance Survey 2025 observes, "Global regulation — driven by myriad macro forces and crises — is adding unprecedented complexity and cost to companies. Against a backdrop of commercial pressures, some have adapted and become 'compliance pioneers', evolving their processes, technology and talent model to mitigate risks, manage cost and offer new insights."[11]

By employing an iterative roadmap approach, CDOs can ensure their organizations remain aligned with the latest legal requirements, technological advancements and business challenges. (See Figure 2.)

Regulatory Compliance Roadmap

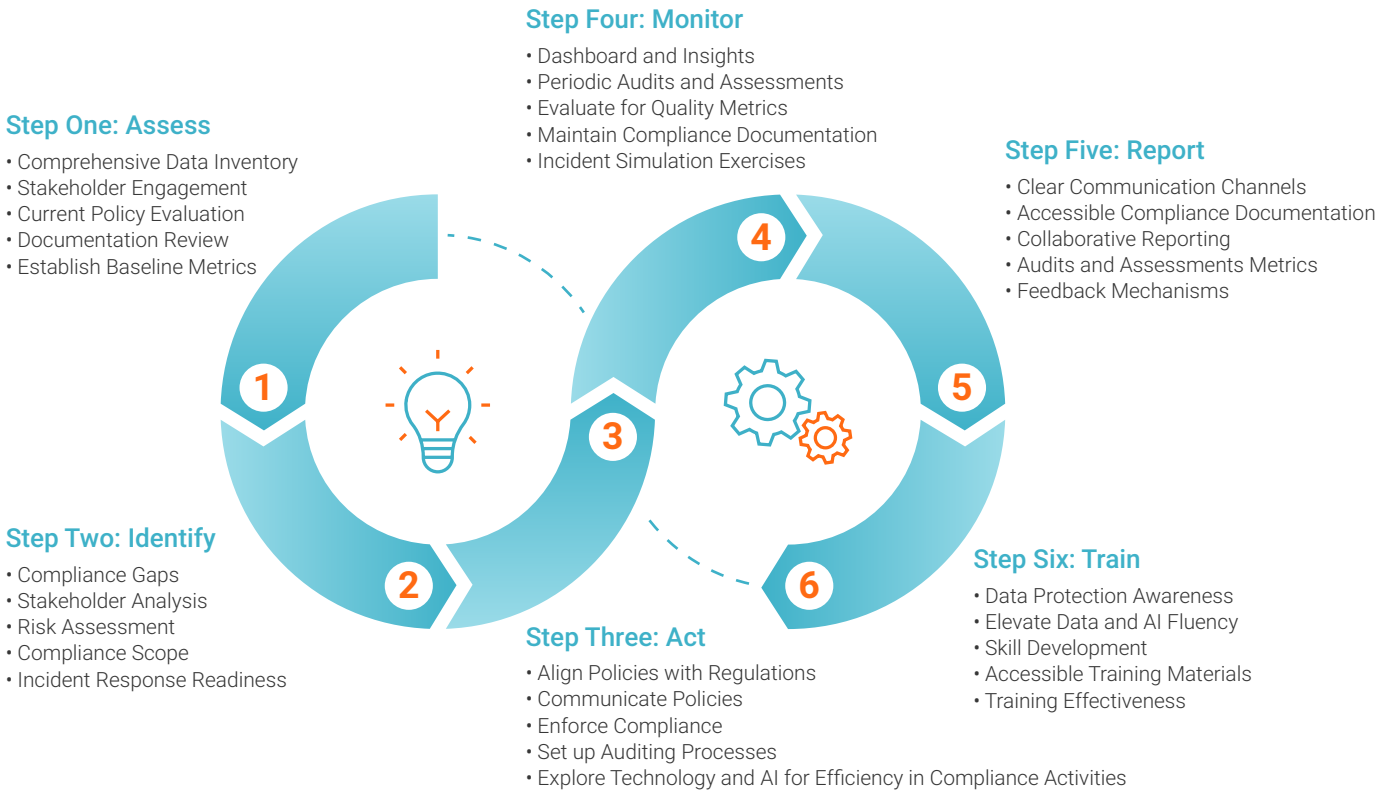


Figure 2: A detailed 6-step regulatory compliance roadmap.

[11] https://www.pwc.com/gx/en/issues/risk-regulation/global-compliance-survey.html

It is critical to adapt the roadmap to the specific priorities and requirements of the business units as you progress along your compliance journey. Figure 3 illustrates how key disciplines for compliance success in ESG or cybersecurity may vary from those for anti-money laundering or financial reporting.

Steps Toward Compliance Success	Financial Reporting (SOX, COSO)	Sustainability (ESG)	Cybersecurity & Privacy (GDPR, HIPAA, ISO 27001)	Banking Capital Adequacy Risk Management (BCBS 239, CCAR)	Anti-Money Laundering (AML)
	Include finance and audit teams to align on reporting requirements	Involve sustainability officers and key departments to set ESG metrics	Engage IT, legal, and HR stakeholders to manage data privacy	Involve risk and finance departments in aligning strategy	Collaborate with compliance officers to understand AML directives
Data Governance Implementation	Implement a framework for financial data management	Develop systems for tracking and reporting sustainability data	Align data governance with privacy standards and IT policies	Enhance accuracy and accessibility of risk data	Establish protocols for transaction and customer data management
Data Privacy and Protection	Ensure financial data meets confidentiality standards	Protect sensitive environmental data and company metrics	Regularly update privacy policies and ensure GDPR compliance	Secure sensitive risk-related data against breaches	Implement controls to protect customer information from unauthorized access
Auditability and Reporting	Automate SOX compliance reporting	Create transparent ESG reporting channels and audit systems	Set up systems for GDPR data processing documentation	Develop automated risk reporting systems for BCBS 239	Implement transaction monitoring and reporting for AML compliance
Risk Management	Conduct financial statement risk assessments	Identify and mitigate risks related to sustainability impacts	Perform regular data security risk assessments to mitigate breaches	Evaluate capital adequacy and stress test regularly	Assess and mitigate risks related to money laundering activities
Data Quality Improvement	Implement data validation routines	Ensure ESG data accuracy and integrity	Run data quality programs to maintain accurate personal information	Improve quality of data for risk calculations	Cleanse data to avoid false positives in AML monitoring

Continuous Monitoring	Monitor compliance with financial reporting standards	Regularly assess sustainability practices and impacts	Perform continuous data privacy monitoring and updates	Regularly review capital reserves and risk strategies	Constantly monitor transactions for suspicious activity
Training and Support	Train finance teams on new compliance software	Educate employees on sustainability policies and practices	Provide training on GDPR compliance and cybersecurity awareness	Train risk management teams on BCBS 239	Conduct regular AML training for relevant staff

Figure 3: An exercise to manage each step of compliance with major regulations.

By following this process and learning how to build a roadmap to success, your organization can stay ahead of the key challenges facing every business. It lays the groundwork for managing compliance more efficiently and supporting business growth opportunities.

Part Two

Staying Ahead in Compliance with IDMC

The recent **Informatica CDO Insights 2025 survey** highlights that regulatory concerns significantly impact generative AI (GenAI) adoption, with 93% of data leaders citing restrictions and 39% experiencing stalled projects. Managing regulatory compliance should not inhibit business opportunity and productivity. However, as we have seen in Part One, the business challenges of managing regulatory compliance are significant.

By leveraging **Informatica's Intelligent Data Management Cloud** (IDMC), an AI-powered comprehensive platform for regulatory compliance including ESG standards, you can reduce data risk and enhance transparency. This ensures data is suitable for business use throughout its lifecycle. It allows you to govern and protect your data per company policies and make data securely available to virtually all data users.

IDMC Key Compliance Benefits

Enhancing Regulatory Reporting: Ensure sensitive data is identified and managed according to regulatory requirements, such as GDPR, CCPA and the EU AI Act. IDMC data cataloging capabilities automatically discover, classify and catalog data across the enterprise.

Mitigating Risk for Reliable Outcomes: Reduce compliance risks and penalties through effective integration and accurate data management across platforms. IDMC proactively identifies compliance issues to maintain profitability and reputation.

Empowering Data Sharing and Collaboration: Enhance data literacy and stakeholder collaboration with partners, customers and regulators. IDMC enables transparent and efficient data democratization, allowing secure access while adhering to compliance policies and fostering informed decision-making.

Automating Compliance Processes: Free up budget for growth and innovation from optimized resource usage and a reduction in manual workload with a scalable cloud-native platform.

Advanced Analytics for Strategic Insights: Support strategic planning and competitive advantage through richer business insights and improved performance. IDMC AI capabilities such as CLAIRE offer advanced analytics to detect patterns, enabling efficient regulatory reporting and informed decision-making.

"We have consolidated over 1 million records for our customers and contacts across disparate systems and are predicting that our work will support up to 33% reduction in fraud. Our marketing powered by data provided by the CDP [customer data platform] is expected to deliver significant benefits based on reduction of retargeting spend through our paid performance marketing."
– Andrea Fitzsimmons, Senior Director Group Customer Data and Insights, RS Group

---

With this all-in-one solution, illustrated in Figure 3, you have access to data governance with privacy controls, improved data quality and AI-driven data cataloging to ensure data transparency, reliability and integrity.

Operating across multiple vendors and clouds, including AWS, Azure and Google, while supporting both on-premises and cloud-based data storage and management, IDMC automates data management tasks and facilitates seamless data integration. This boosts operational efficiency and establishes a single source of truth.

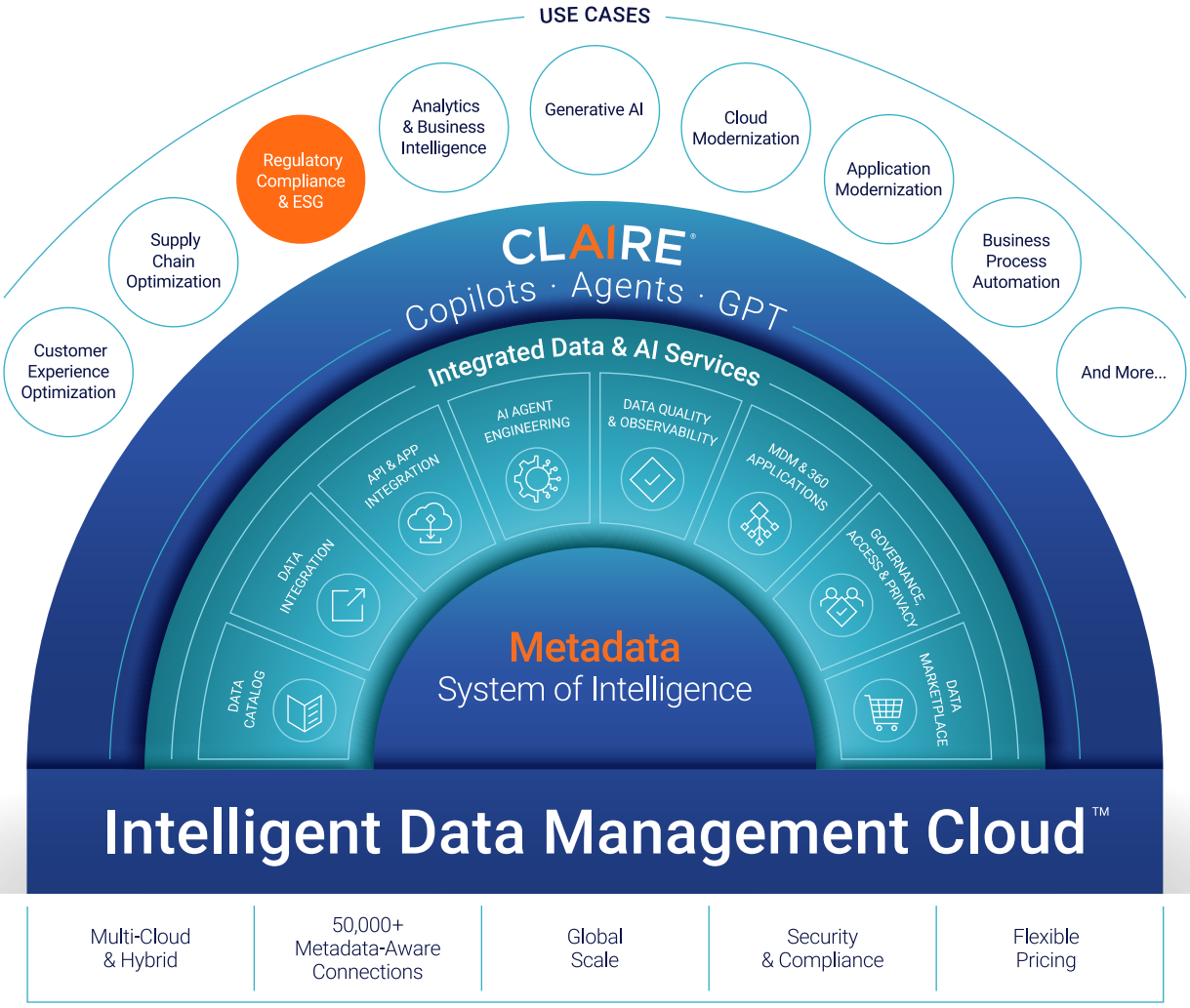


Figure 3: IDMC's unified data management platform to support regulatory compliance.

Congratulations!

You are well on your way to equip your organization with the strategies to tackle several compliance challenges, including setting up trusted reporting systems, ensuring operational efficiency and maintaining brand reputation while meeting regulatory compliance requirements and leveraging technology.

By using IDMC, you now have access to a powerful AI-driven data management platform. This comprehensive solution supports regulatory compliance by automating data management processes, minimizing risks and ensuring data integrity. This proactive approach not only ensures compliances by enhancing transparency and accountability, but it also helps your organization meet various regulations like GDPR, CCPA and ESG frameworks effectively.

Here's to your ongoing journey toward compliance success!

Further Reading

Chart the Course for Responsible AI Governance

READ EBOOK

AI Fluency: Turning Data Professionals into Value-Driving AI Champions

READ EBOOK

How one Global Financial Services Organization is Managing and Governing Its Data to Accelerate ESG Initiatives

READ EBOOK

Navigating ESG Regulations with Intelligent Data Management

READ BLOG

Informatica Demo Center

VISIT NOW

About Us

Informatica (NYSE: INFA), a leader in enterprise AI-powered cloud data management, brings data and AI to life by empowering businesses to realize the transformative power of their most critical assets. We have created a new category of software, the Informatica Intelligent Data Management Cloud™ (IDMC), powered by AI and an end-to-end data management platform that connects, manages and unifies data across virtually any multi-cloud, hybrid system, democratizing data and enabling enterprises to modernize their business strategies. Customers in approximately 100 countries and more than 80 of the Fortune 100 rely on Informatica to drive data-led digital transformation. **Informatica. Where data and AI come to life.™**

Where data & AI come to

Worldwide Headquarters
2100 Seaport Blvd.
Redwood City, CA 94063, USA
Phone: 650.385.5000
Fax: 650.385.5500
Toll-free in the US: 1.800.653.3871

informatica.com
linkedin.com/company/informatica
x.com/Informatica

CONTACT US

IN18-5124-0525