CAPCO

MANAGING DATA IN A REGULATED WORLD

HOW FINANCIAL INSTITUTIONS CAN NAVIGATE DATA RISKS WHILE ENSURING COMPLIANCE

a wipro company

TARGET AUDIENCE

This paper is intended for the producers, owners, and custodians of data who are ultimately responsible for ensuring regulatory compliance in financial institutions. We assume the reader has some context and understanding of data management and governance, and regulatory compliance. The focus is on the emerging techniques for managing data and ensuring compliance with the latest regulations. The term “enterprise information assets” is used to refer to enterprise applications and end-user computing (EUCs).

EXECUTIVE SUMMARY

Financial institutions are a major target of data breaches and deliberate attacks by cyber criminals. These data breaches can infringe upon the privacy of all stakeholders, often from unauthorized access to sensitive personally identifiable information (PII) data, such as social security numbers. Roughly 147 million customers were potentially affected by the Equifax data breach in September 2017.[1] Numerous recent violations have occurred in areas of security, integrity, and confidentiality. This trend prompted regulators to strengthen existing laws, rules, and regulations to ensure firms prevent breaches, or at least contain the risk substantially when a breach occurs. With this increase in regulatory mandates and the unpredictable nature of “what comes next,” firms are struggling to manage their data in a compliant manner.

Regulatory compliance is an often-underserved area. Since data is increasingly treated as an asset that drives decision-making, financial institutions can no longer ignore regulatory compliance. They must now remain fully compliant with all applicable regulatory obligations. By adopting a data governance program coupled with a regulatory intelligence function, financial institutions can govern their data effectively. Most importantly, this approach ensures adherence to regulatory compliance in an ever-changing regulatory landscape. Financial institutions can leverage the guidance in this paper to enact effective programs from scratch or improve existing ones.

GENERAL VIEWPOINT

Data is growing exponentially, and the regulatory landscape continues evolving. As financial institutions strive to keep up with the pace of change, substantial gaps are forming resulting in non-compliance. Regulatory compliance is the adherence to laws, rules, and regulations (LRRs) that are created by government and industry regulatory authorities. Financial institutions must demonstrate full compliance with LRRs to ensure they are not met with regulatory fines.

Regulatory compliance can go unnoticed if it is not strictly enforced internally within the institution. A primary diagnostic of non-compliance is a data breach. These breaches expose the inadequate state of a compliance program in a public and often detrimental fashion. Regulatory examinations of the existing data management practices have revealed clear violations, or at least the lack of a mature regulatory compliant data program. These investigations have sounded alarms in several data management functions especially in data governance. As an epicenter of data functions, data governance formalizes the management of data assets within an organization. It is a framework of policies, processes, and procedures that govern the management, usage, and flow of data across an organization. This makes data reliable, trustworthy, and readily available for driving effective reporting and decision-making. Data breaches and scrutiny from regulators have only prompted institutions to restructure their data governance programs.

REPERCUSSIONS OF NON-COMPLIANCE

Regulatory compliance is emerging as a critical area, and institutions are left with no choice but to remain compliant with regulatory obligations. Regulations are created to ensure banks operate lawfully while protecting customers, stakeholders, employees, and the company itself. Institutions that cannot demonstrate compliance or those subject to violations may face any or all the following repercussions:

A. **Monetary Penalties / Fines –** Regulators are not hesitant to impose penalties on banks that do not meet regulatory obligations. According to data acquired from the Bank Fines Report 2020 by Finbold.com indicates a total of $15.13 billion in aggregated fines in 2020. The United States accounts for the highest fines, at $11.11 billion or 73.4 percent of the issued fines.[2]

B. **Audits –** Breaches are often the trigger points for an audit. It prompts regulators to investigate the bank's functions, processes, and financials more regularly.

C. **Reputational Damage –** Non-compliance can negatively influence an institution's public reputation. This can result in loss of confidence among customers, resulting in a loss of its market share and valuation in case of a publicly traded company.

D. **Cessation of Business –** An increase in the frequency of violations can adversely affect the institution. They will ultimately be left with no choice but to cease business operations.

ENABLING REGULATORY COMPLIANT DATA GOVERNANCE PROGRAM

Financial institutions can easily ensure their data supports regulatory compliance. This can be accomplished by building an effective data governance program alongside regulatory guidance.

A. **An effective data governance program –** Data management defines systems, processes, and standards that determine the way data is created, stored, consumed, and reported in an organization. Data governance is a function of data management; it is the strategy applied to govern its management and facilitate the sequence of a data lifecycle. This function involves documenting data types, ownership, consumers, and assessing its fit for the desired purpose. It democratizes data and ensures it is trusted at its source and is readily available, while establishing high levels of integrity, quality, consistency, accuracy, confidentiality, privacy, and security.

Executing data governance is not a one-person or a one-team job but requires the collaboration of the whole organization from IT staff and business executives to subject matter experts and decision makers. The processes in a data governance program guide people to follow a defined path to formally manage, store, deliver, and share data to enable key reporting and decision-making capabilities. Subsequently, policies and procedures are enacted to ensure organizations comply with applicable regulations and thereby prevent and counteract any potential data risks. Policies and procedures are essentially controls in actions that are guided by LRRs issued by federal, and industry specific regulators. These mandates are applied at all levels of data to ensure compliance.

Financial institutions must execute data governance on all their enterprise information assets that support critical business processes, especially those that have a financial, analytical (decision-making), operational and/or regulatory purpose. To execute a successful data governance program, organizations must ensure the following steps are executed:

1. **Data Classification and Catalog –** The first essential step in data governance is classifying the organization's data into structured and unstructured formats. It is necessary that this data is organized and managed in data catalogs. As part of this step, all data attributes need to be identified, and mapped onto locations where they are physically stored. Simultaneously, banks can also establish their Authoritative Data Sources to ensure data is trusted at its source. An authoritative data source is considered as the most reliable source of data that has all necessary data controls in place. They are classified based on the system of origin and authorized distributor of source. The sensitivity of data is also rated for risk and classified depending on its confidentiality.

2. **Fit for use and purpose –** Organizations have long been using their enterprise information assets for inappropriate applications. Hence, their use must be periodically reviewed to determine the purpose and their utility for fulfilling the needs of consumers. The data residing in these information assets must be usable and achieve the intended purpose. This review can be accomplished as part of the firm's recertification process when enterprise assets are verified and certified based on criticality/sensitivity of data residing within applications and EUCs. User access controls are also reviewed to ensure data is only provided to the requested consumers and all other unwarranted system access is revoked.

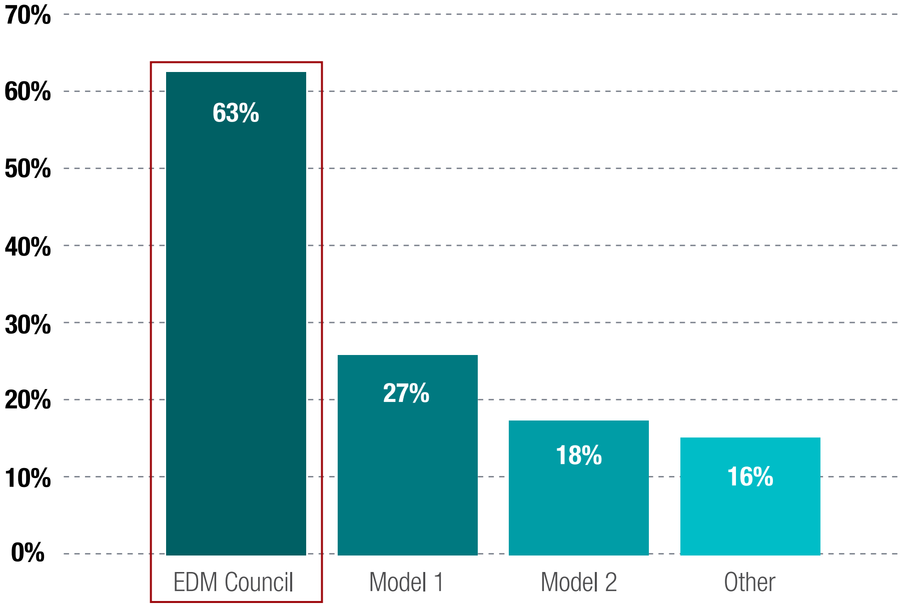
3. **Data Lineage -** Documenting the journey of data from its source and to the destination (i.e., where it is consumed) is necessary for organizations to ensure traceability. This process illustrates the flow of data through applications and EUCs while undergoing various transformations along the way. All necessary interfaces that facilitate the flow of data must be documented, as well.

4. **Minimum Controls –** After the enterprise information assets and data residing within are documented, classified, and rated for risks; minimum controls need to be determined. A controls framework may be established for this purpose to document and organize the institution's internal controls. These guidelines associate controls to the risks for a financial institution. As controls are applied, it is necessary that periodic gap assessments relative to the existing control environment are performed to ensure high levels of data integrity and quality. These controls must be tested rigorously for performance and effectiveness; any gaps and weaknesses must be duly remediated.

B. **Assessing existing data management and governance capabilities using DCAM Assessments –** Financial institutions must assess their existing data governance program against industry standards to determine any gaps in the program. This step will help detect inadequacies even before regulatory examinations identify them. It is also an early opportunity to determine compliance with regulatory requirements. As part of the assessment process, organizations must prioritize, classify, and subsequently rate their information assets (such as applications and EUCs) for risks. This procedure evaluates the extent to which they may be susceptible to vulnerabilities. Based on these risk ratings, controls can then be applied at all levels of data as prescribed by the organization's policies, procedures, and data risk policy documents.

Capco is a member of the EDM Council and a Data Management Capability Assessment Model (DCAM) authorized partner that is certified to conduct formal DCAM assessments. We strongly advocate for firms to assess their data program using DCAM assessments. By performing a DCAM assessment, firms evaluate their data management functions based on DCAM capabilities and dependencies, the result of which is a formal review of the firm's data management program, including a gap analysis and a list of agreed priorities.[3]

DCAM is the industry-standard, best-practice framework designed to assist today's information professionals in developing and sustaining a comprehensive data management program.[4] Our DCAM assessments provide a holistic analysis of the data management office's maturity in dealing with compliance requirements. Criteria range include data strategy, data and technology architecture, data quality management, data analytics, and more.



Source: EDM Council

Which model are you using?
Many of the respondents claim to use a hybrid of models. The following graph represents the percentage of the model used.

CAPCO'S CENTER FOR REGULATORY INTELLIGENCE (CRI)

Risk management and compliance functions are overwhelmed by the velocity and volume of regulatory information, often missing key trends and context leading to missed compliance obligations that can be mapped. Capco's Regulatory Intelligence Library and Regulatory Data Feed helps clients minimize risk by illuminating regulator expectations, identifying obligations, and defining the risks and controls. Capco supports institutions as they work to minimize risk, by proactively identifying legal and regulatory requirements and supervisory expectations and analyzing the impact of geopolitical events to their business. Our Center for Regulatory Intelligence ("CRI") is a single source of comprehensive research and analysis from primary source documents, government surveillance, industry networks and qualitative and quantitative data.

Our SMEs accordingly synthesize these developments to create impact analyses our clients can use to mitigate risk at the first sign of change and to effectively identify, measure, monitor, control for risk exposures. CRI further supports Capco consultants as they help institutions comply with regulatory changes; remediate violations of laws and compliance weaknesses; prepare for regulatory examinations; and explore new product offerings or functionalities. Institutions can further leverage CRI to periodically revise their existing controls in their mandatory procedures and data risk policies to ensure they are aligning themselves to latest regulatory changes and trends. Capco recommends financial institutions supplement their Data Governance programs with regulatory guidance, such as Capco's Center for Regulatory Intelligence (CRI), to enable an effective and responsive Regulatory Compliant Data Governance Program.

CONCLUSION

The business units for financial institutions own the data assets of the firm, and therefore play a critical role in defining the data governance strategy. We believe that prior to undertaking any data compliance discussions, financial institutions must ensure there is participation from all business, compliance, and IT units. Technologists are responsible for ensuring controls are effectively in place and tested on data assets. Compliance must ensure the controls are adequate and meet existing regulatory requirements. Institutions must realize that regulators are here to ensure a healthy and a law-abiding financial ecosystem, and the landscape is ever-changing. To stay truly compliant, a financial institution must have a clearly defined data strategy, supplemented with a regulatory intelligence function. By adopting this approach, it can be both agile and adaptive in responding to continuously evolving regulatory needs and conditions. Stay tuned for more insights, guidelines, and best practices specific to a range of services within financial services, from Retail Banking and Capital Markets to Wealth and Investment Management.

REFERENCES

1. https://www.ftc.gov/enforcement/refunds/equifax-data-breach-settlement
2. https://www.corporatecomplianceinsights.com/banks-15b-in-fines-in-2020/
3. https://edmcouncil.org/page/dcamassessmentsuppor
4. EDM Council

AUTHORS

Varun Putchala
Principal Consultant
varun.putchala@capco.com

Glenn Kurban
Partner
glenn.kurban@capco.com

CONTACT

Glenn Kurban
Partner
glenn.kurban@capco.com

Peter Dugas
Executive Director, RISC Services
peter.d.dugas@capco.com

ABOUT CAPCO

Capco, a Wipro company, is a global technology and management consultancy specializing in driving digital transformation in the financial services industry. With a growing client portfolio comprising of over 100 global organizations, Capco operates at the intersection of business and technology by combining innovative thinking with unrivalled industry knowledge to deliver end-to-end data-driven solutions and fast-track digital initiatives for banking and payments, capital markets, wealth and asset management, insurance, and the energy sector. Capco's cutting-edge ingenuity is brought to life through its Innovation Labs and award-winning Be Yourself At Work culture and diverse talent.

To learn more, visit www.capco.com or follow us on Twitter, Facebook, YouTube, LinkedIn Instagram, and Xing.

WORLDWIDE OFFICES

APAC
Bangalore
Bangkok
Gurgaon
Hong Kong
Kuala Lumpur
Mumbai
Pune
Singapore

EUROPE
Berlin
Bratislava
Brussels
Dusseldorf
Edinburgh
Frankfurt
Geneva
London
Munich
Paris
Vienna
Warsaw
Zurich

NORTH AMERICA
Charlotte
Chicago
Dallas
Hartford
Houston
New York
Orlando
Toronto
Tysons Corner
Washington, DC

SOUTH AMERICA
São Paulo

WWW.CAPCO.COM