accenture

DATA PRIVACY

A platform for building trust-based relationships in financial services

The global financial services industry is undergoing the most rapid change in its history. Large-scale migration to the public cloud and a hyper-focus on personalization are just two examples of a revolution in the financial services experience. In this new environment, privacy is more important than ever.

Our analysis indicates that there is a financial "cost" to eroded trust in the digital economy. Over the next five years, large private sector firms risk losing an estimated $5.2 trillion in value creation opportunities, which translates to 2.8 percent in lost revenue growth over the period. But our Accenture 2019 Compliance Risk Study research also shows that mitigating privacy risk—an essential building block for improving trust between the financial services institution and client—is the most challenging priority for compliance programs to manage in the next year.[1]

Privacy concerns are not new, though they have evolved considerably from a more nationalistic focus around cross-border data flows, to an additional layer around information security standards from state-based regulators such as the New York Department of Financial Services (NYDFS), and now to a more holistic view touching on consumer rights. This latest development has elevated privacy from a purely regulatory-driven agenda to one impacting broader questions around trust and sustainable business growth.

The European Union's General Data Protection Regulation (GDPR) has been in force since May 2018 and has been instrumental in establishing a framework of specified rights for consumers with respect to their own data. Since implementation of GDPR, the California Consumer Privacy Act of 2018 (CCPA) that has been enacted is now in the formal rulemaking process, and could be subject to additional legislative changes before its effective date of January 1, 2020.[2] Unless a federal law is enacted that pre-empts multiple state laws like CCPA, we expect CCPA to be the de facto benchmark that sparks a wave of laws and regulations at the state level throughout the U.S., creating a patchwork of compliance requirements that could create new requirements and risk for financial institutions on top of those resulting from the federal Gramm-Leach Bliley Act (GLBA).

Industry groups—led by the Business Roundtable (BRT), a trade association representing 200+ CEOs from America's leading companies—are seeking common ground at a national level regarding a framework for consumer rights and data privacy. In 2018, as Chair of the BRT's Technology Committee and the Privacy Working Group, Accenture North America CEO Julie Sweet worked with CEOs across all major sectors, including financial services, to develop and put forward a framework in December 2018 for a national privacy law. While we believe a national privacy law is necessary and can eventually be achieved, in the interim, financial institutions should expect to face overlapping legal compliance requirements and potential litigation risk, each impacting their business strategy, risk management, and data and technology planning in an era of continued cost constraint.

Designing a Comprehensive Privacy Framework

Financial services institutions are investing in holistic activities, approaches and tools to address compliance needs related to emerging privacy regulations such as consumer rights.

Furthermore, financial institutions should take steps to understand how personal information enters their organization, how it remains in applications, and how unstructured data sources have generated a level of complexity over decades of organic and inorganic growth. Such monitoring, surveillance and reporting of data is also dependent on knowledge and close collaboration with a web of suppliers, who may be dependent on their own vendors, exposing the firm to potential and significant operational change.

Addressing this complexity in an efficient and effective manner that infuses innovation into current processes and technology can provide market differentiation for financial institutions, like increasing consumer loyalty in an era that places renewed premium on trust in client-financial institution relationships. Many institutions in the U.S. have put structures in place to respond to large-scale regulatory initiatives stretching back to GLBA and more recently NYDFS and GDPR. Many of these structures can be repurposed to proactively build stronger client relationship, with an emphasis on five core capabilities:

01 | PRIVACY PROGRAM GOVERNANCE

Following the lead of the GDPR, many financial institutions are either establishing a position in the organization that is responsible and accountable for consumer rights and data privacy, like the data protection officer (DPO) or the chief privacy officer (CPO) role or raising the stature of these existing roles and conferring upon them the authority to highlight risks and make required changes across the organization. Such decisions should be taken in accordance with the organization's privacy risk appetite.

02 | DATA DISCOVERY AND CLASSIFICATION

The discovery, inventory and classification of personal information is a significant area of focus of any privacy program given the specific guidance of various regulations. Scanning should be automated and at scale with fit-for-purpose tools that can access unstructured data sources, leveraging existing technologies or supplementing with accelerators from the market. Implementation of data discovery and classification tools can be complex due to the multitude of architecture patterns and platforms on which data can reside. This often necessitates prioritizing the discovery of certain sources, while in parallel preparing for the discovery of more complex areas in subsequent sprints.

03 | PROCESS DESIGN AND IMPLEMENTATION

Processes should be designed to manage all client requests related to privacy through to completion, such as access to information, opt out or erasure requests. Navigating the data supply chain across multiple third parties whose risk appetite, controls, and maturity may not match those of the financial institution is a key area of complexity, though persistence in closing out negotiations to update contract language and even to weigh the sustainability of certain relationships going forward is key.

04 | TECHNOLOGY

In addition to data discovery, capabilities should be leveraged to protect personal data across applications, workstations, servers, and the data supply chain in accordance with the overall privacy strategy. Identifying the remediation of legacy applications that may not support deletion, anonymization or other regulatory expectations is a key priority to support compliance, potentially requiring the adoption of more manual compensating controls in the short term, as a precursor to more strategic change.

05 | TRAINING AND AWARENESS

Investments in technology cannot prevent major lapses and large fines if not accompanied by updates to policy and procedure, and the necessary training around such changes to build a culture of awareness and respect for consumer rights and data privacy. Training should take place at two levels: first, at the enterprise level, to build awareness; and, second, in the form of role-based guidance for front line staff handling consumer inquiries, such as consumer contact teams, social media specialists or those managing online platforms.

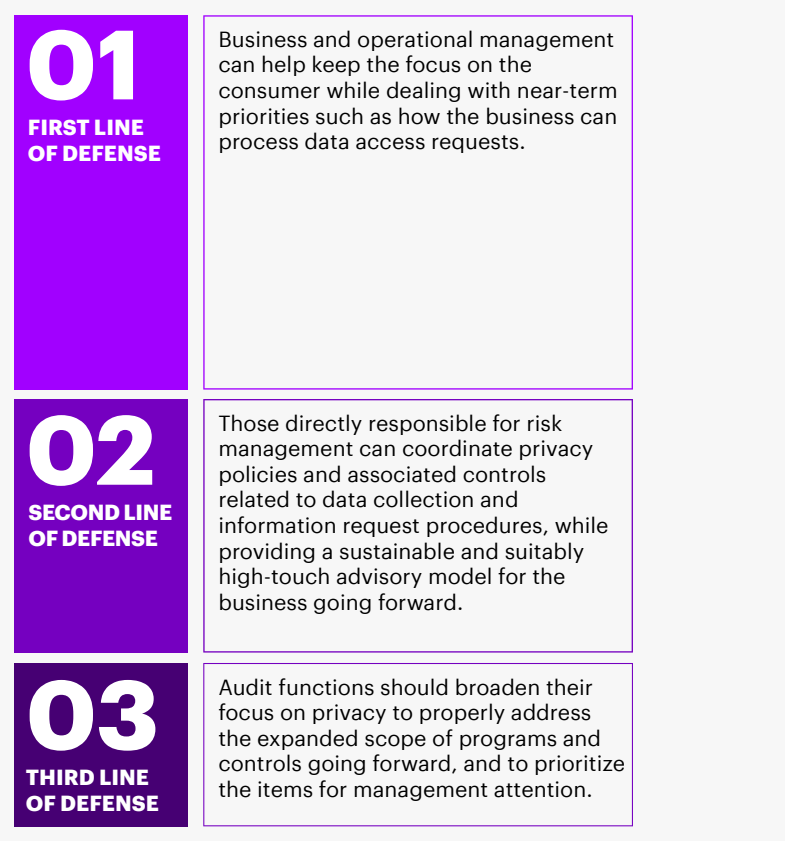
Establishing the Control Framework

The responsibility for establishing a culture of embedded privacy throughout the organization starts at the top, with the CEO and board of directors. Execution lays with senior managers establishing a control framework that can holistically address the dimensions of privacy risk.

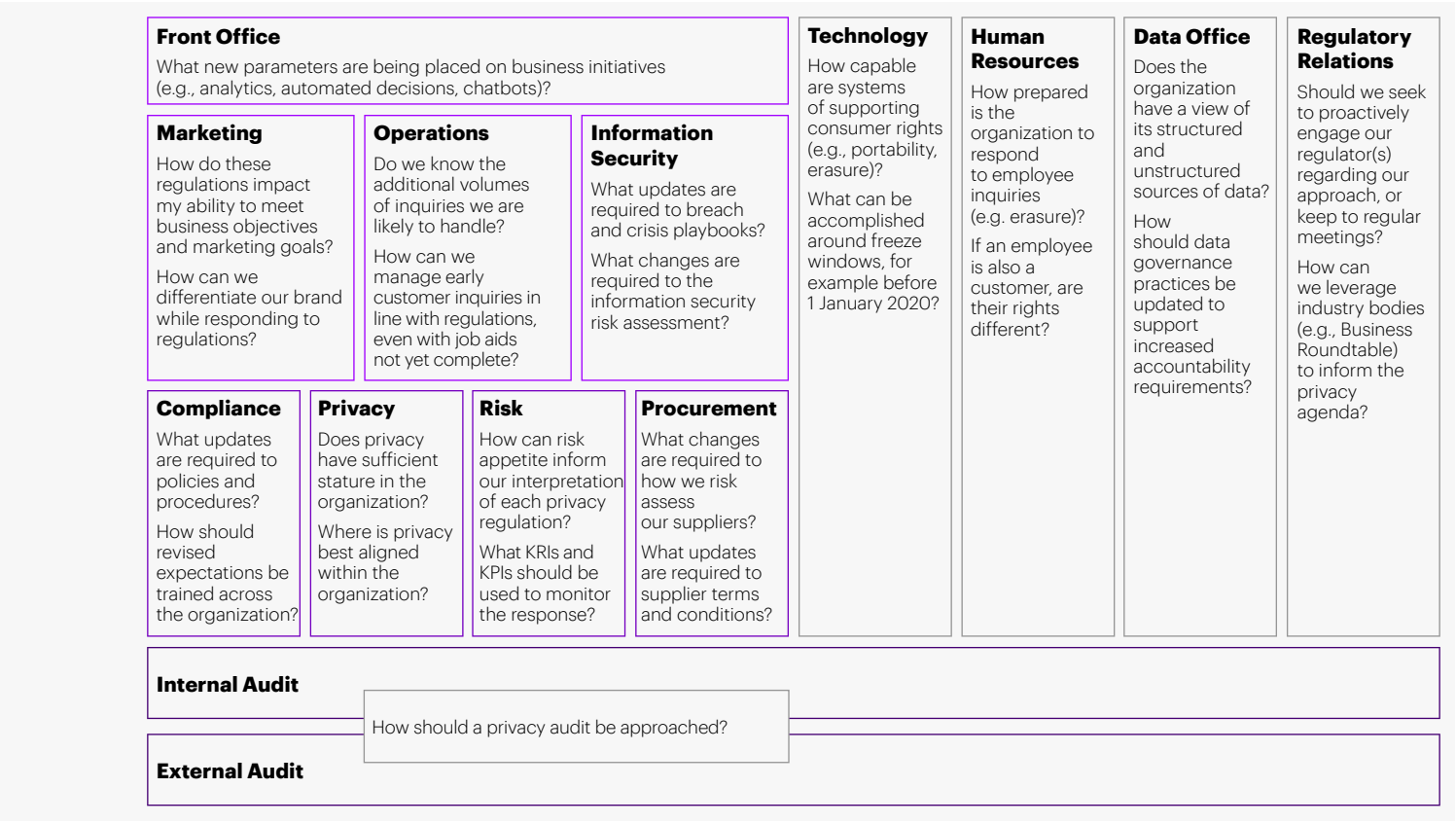
Supporting the CEO and board of directors, the chief risk officer (CRO), general counsel (GC), chief compliance officer (CCO) and chief privacy officer (CPO) are key stakeholders in establishing the appetite for privacy risk while engaging key partners within the organization, such as the chief information officer (CIO) and chief information security officer (CISO). Each function has a role to play, but all functions should be aligned in terms of business strategy and execution.

From a three lines of defense perspective, areas of focus can be summarized in Figure 1. It illustrates, dependent upon their vantage point, the key questions senior stakeholders and their teams are looking to address during the data privacy transformation journey.

Figure 1 Key questions being asked today around data privacy



Source: Accenture, March 2019


Front Office
What new parameters are being placed on business initiatives (e.g., analytics, automated decisions, chatbots)?
Marketing
How do these regulations impact my ability to meet business objectives and marketing goals?
How can we differentiate our brand while responding to regulations?
Operations
Do we know the additional volumes of inquiries we are likely to handle?
How can we manage early customer inquiries in line with regulations, even with job aids not yet complete?
Information Security
What updates are required to breach and crisis playbooks?
What changes are required to the information security risk assessment?
Compliance
What updates are required to policies and procedures?
How should revised expectations be trained across the organization?
Privacy
Does privacy have sufficient stature in the organization?
Where is privacy best aligned within the organization?
Risk
How can risk appetite inform our interpretation of each privacy regulation?
What KRIs and KPIs should be used to monitor the response?
Procurement
What changes are required to how we risk assess our suppliers?
What updates are required to supplier terms and conditions?
Technology
How capable are systems of supporting consumer rights (e.g., portability, erasure)?
What can be accomplished around freeze windows, for example before 1 January 2020?
Human Resources
How prepared is the organization to respond to employee inquiries (e.g. erasure)?
If an employee is also a customer, are their rights different?
Data Office
Does the organization have a view of its structured and unstructured sources of data?
How should data governance practices be updated to support increased accountability requirements?
Regulatory Relations
Should we seek to proactively engage our regulator(s) regarding our approach, or keep to regular meetings?
How can we leverage industry bodies (e.g., Business Roundtable) to inform the privacy agenda?
Internal Audit
How should a privacy audit be approached?
External Audit

Responding to the Emerging Privacy Policy Landscape

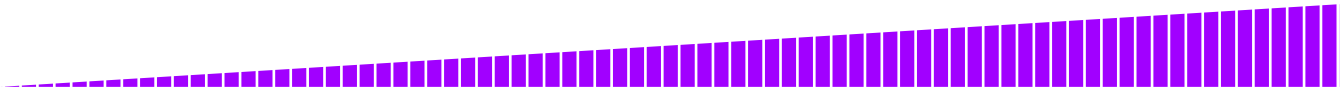
GDPR was the first to redefine the global thinking on privacy and consumer rights. However, new regulations may expand protections even further, such as the CCPA's provision for right to equal service for consumers.

There are different approaches that can be applied by financial services institutions in responding to emerging privacy regulations, depending on their risk appetite as well as the level of pre-existing capability built up through prior compliance efforts. Figure 2 provides some examples of these for institutions considering their response to CCPA.

Regardless of the approach taken, our experience supporting financial institutions on their journey to GDPR compliance has provided valuable lessons in the areas of scope and implementation. Key examples include the importance of operating in a truly cross-functional manner across the organization, reflecting the scope of new requirements and the opportunity to capture competitive advantage during the response. Another learning is to use a consumer perspective and focus in the design of revised process and technology capabilities, rather than a more siloed application-by-application view that can take more time to identify and understand interdependencies.

Figure 2 Responses to emerging privacy and consumer rights laws

TACTICAL — STRATEGIC

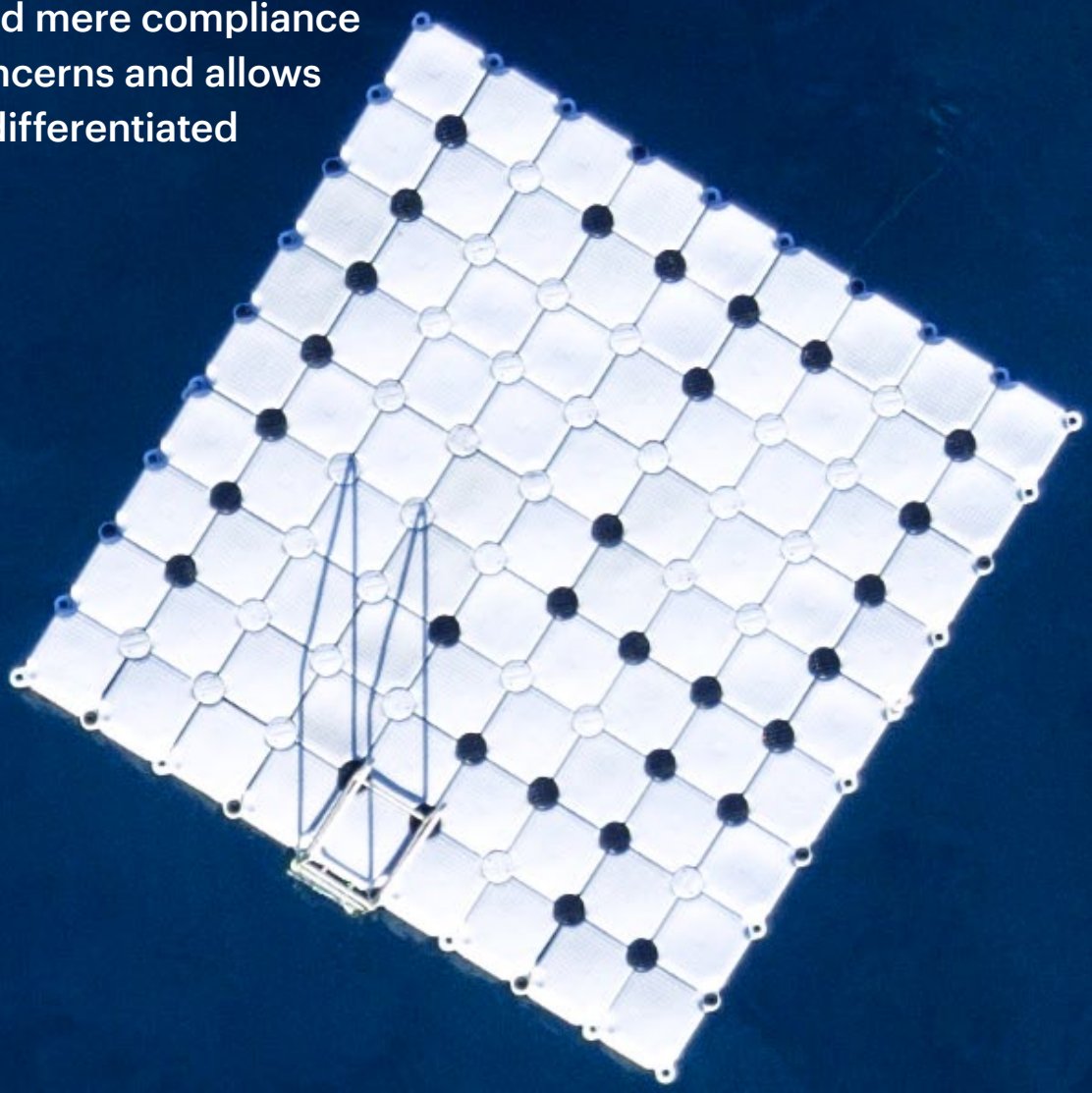


01	02	03
Implement Regulation for in-scope data subjects alone	**Enhance data privacy model for all data subjects to align with Regulation**	**Address Regulation within a broader "Consumer Rights" Program**
PROS		
Narrower scope, providing greater transparency to ROI	Opportunity to re-use prior enterprise capability development (e.g., NYDFS, GDPR, etc.)	Integrate efficiencies from "build once, solve for many" approach
May increase the chance of reaching compliance with the letter and spirit of the rule	Reduced complexity of capability development and deployment	Opportunity to develop capability ahead of legislation
CONS		
Less efficient as additional federal and state guidance comes onstream	May require re-work as federal and state guidance continue to change	Challenges defining "highest common denominator" across in-scope rules
Potential for an uncoordinated "patchwork" of compliance efforts without standardization	Potential resistance to performing compliance tasks that are not directly applicable	Gaining enterprise collaboration and alignment can impede agility

Source: Accenture, March 2019

Conclusion

Financial services institutions have been presented with an opportunity to create more transparent and trust-based relationships with their clients by taking a holistic approach that goes beyond mere compliance and security concerns and allows them to create differentiated outcomes.



About the Authors

Samantha Regan

Samantha is the Global Lead for the Regulatory Remediation and Compliance Transformation group within Accenture's Finance & Risk practice. She has over 17 years of global experience working with C-suite executives and their businesses in compliance and regulatory initiatives.

Gracie Pereira

Gracie is a Managing Director in the Accenture Security Financial Services team with over 18 years of experience in the field of cybersecurity and privacy, technology risk, system and operational audit, and IT transformation. She has held executive level positions at large financial institutions, and has extensive experience leading the information technology and risk group, with an emphasis on information risk management and infrastructure engineering.

Ben Shorten

Ben is a Senior Manager with Accenture Finance & Risk. Based in New York, Ben serves as the Compliance Transformation Offering Lead for Accenture in North America. Ben has extensive experience working with investment banks, retail banks and insurance providers in North America, the UK, and continental Europe to define compliance strategy in response to regulatory and government mandates and ongoing changes in the financial services ecosystem.

Gregory Ross

Gregory is a Senior Manager in Accenture's Finance & Risk practice, with responsibility for the Fraud Management Consulting area. Gregory brings his experience and knowledge in the areas of resiliency, regulatory and compliance, and operational risk management processes and technology solutions to help financial services organizations strategize and deliver robust and streamlined risk management capabilities. He also has deep experience driving strategy design and implementing risk management functions, as well as executing key risk management processes at-scale. Gregory also has significant experience organizing and running large-scale, regulatory-driven enhancement programs.

Timothy Lisko

Tim is a Security Principal Director in the Accenture Security practice. Tim focuses on assisting CxOs and boards on the journey to take control of their cyber security, privacy, and consumer rights programs, aligning them to the business goals and strategy, providing appropriate capabilities to the organization, and when possible creating market differentiation. Tim has been involved with the security and privacy industry for over 15 years.

ACKNOWLEDGMENT

The authors would like to thank the following Accenture employees for their important contribution to this document: Garrett Swanberg and Anwar Ali

REFERENCES

1 "Accenture 2019 Compliance Risk Study," Accenture, March 2019.

2 Californians for Consumer Privacy portal. Access at: https://www.caprivacy.org. "Proposed Technical Amendments to CCPA (3.25.19)," Californians for Consumer Privacy, March 25, 2019. Access at: https://www.caprivacy.org/post/proposed-technical-amendments-to-the-ccpa.

STAY CONNECTED

Accenture Finance Risk
www.accenture.com/us-en/financial-services-finance-risk

Finance and Risk Blog
financeandriskblog.accenture.com

Connect with us
www.linkedin.com/showcase/16183502/

Follow us
www.twitter.com/AccentureFSRisk

ABOUT ACCENTURE

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions—underpinned by the world's largest delivery network—Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With more than 469,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives. Its home page is www.accenture.com

DISCLAIMER

This document is intended for general informational purposes only and does not take into account the reader's specific circumstances, and may not reflect the most current developments. Accenture disclaims, to the fullest extent permitted by applicable law, any and all liability for the accuracy and completeness of the information in this document and for any acts or omissions made based on such information. Accenture does not provide legal, regulatory, audit, or tax advice. Readers are responsible for obtaining such advice from their own legal counsel or other licensed professionals.

12460716

190351