
burnmark
CUBE
RegTech
for Information Governance
December 2018 | info@burnmark.com
@burnmark_
@CUBEGlobal

TABLE OF CONTENTS

WHY INFORMATION GOVERNANCE, AND WHY NOW?

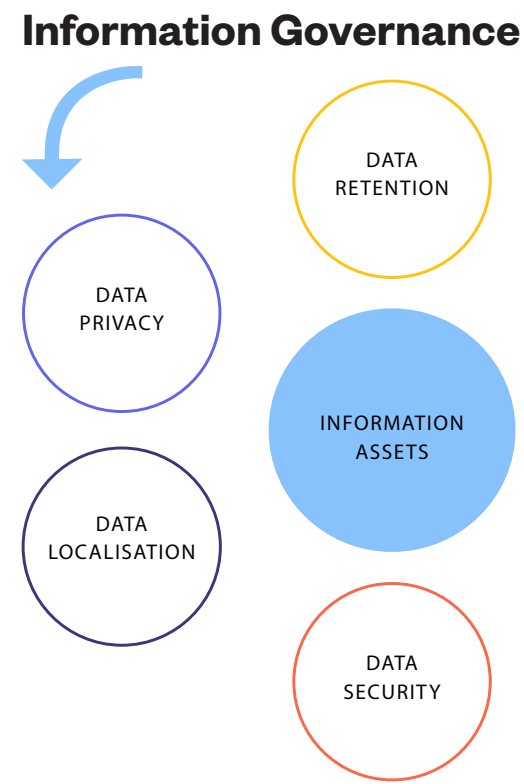
The banking and financial services industry's core competence is no longer its products and services - data is most institutions' core business today. Whether it is data - and data transformed into information - for marketing and personalisation, customer service, offer creation, privacy or security, the priority for organisations is to maximise the value of data and information assets available to them, while also managing the huge amounts of risk associated with holding and using this data and information.

Since the days when financial services record-keeping involved archiving paper-based files physically, or in scanned form on write-once media, there has been a huge transformational shift. In those days what mattered was where records were stored, in what format and who had access. Technologically, there was no possibility of handling data within records independently, and pre-2010 regulation relating to data privacy was scarce. Digitisation has changed this entire industry. Records, especially those with regulatory significance, have become critical information assets containing valuable personal data that must be protected and governed with care, under the watchful eyes of regulators and legislators.

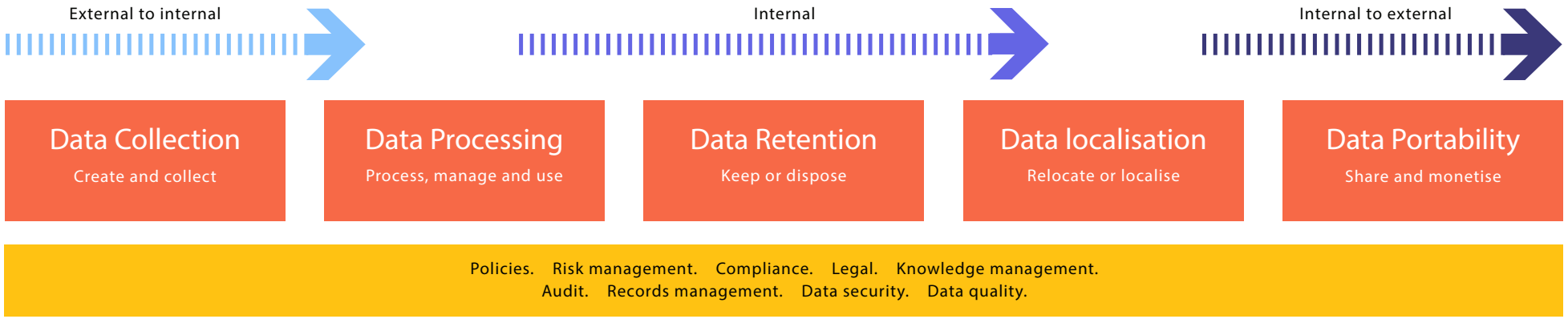
Regulators across the globe have come up with directives that support legislation and have altered the nature and process of how organisations collect, process, share, manage, transfer and destroy business data. Notably:

- Modern data protection and privacy laws put greater emphasis on individual consent which dictates organisations' actions in how they manage their information assets. Extra-territoriality and differences in interpretation of regulation at a national level have exacerbated the challenge of managing information assets throughout the customer lifecycle.
- New regulations with significant geographic impact like PSD2 and GDPR have made 2018 an interesting year to look at the way large global organisations are viewing information governance. New data points like social media data and new processes like credit scoring using mobile phone usage have increased the complexities of information governance even further in the past couple of years.
- The scope, frequency and scale of cybercrime has increased significantly in the past five years, and there is increased pressure to use cross-border data to handle these challenges.
- There is also significant regulatory divergence in data legislation around the world, making us wonder how, for example, a US-based global bank is dealing with pan-European legislation like GDPR.
- The cost of regulatory fragmentation is immense and banks are looking for new ways to achieve operational efficiencies.

Burnmark and CUBE are pleased to publish this report where we have looked at some of the complexities faced by multi-jurisdictional financial institutions (FIs) in complying with modern legislation related to information assets. We have conducted a survey of large global FIs in order to validate some of our findings and interviewed leaders from the industry who gave us valuable input and direction.



Information Governance is the set of policies, controls and metrics that specify how an organisation's information is managed as a business asset, while maintaining data privacy, data protection, data security, data residency and data retention aspects.



The information governance process is active throughout the lifecycle of data and records assets

Data collection and data privacy

Strict KYC/AML rules require FIs to collect more information about their customers, and demands additional compliance with data privacy laws. As FIs shift to digital channels like online banking and mobile transactions, it increases their vulnerability to cybercrime.

Data processing and transparency

Banks are increasingly looking to process customer data through analytical algorithms to offer personalised products and services to customers. GDPR brings transparency and fairness principles to ensure banks proactively and clearly communicate the context of data processing to customers and obtain explicit consent for various types of data processing.

Data retention and data disposal

It is no longer adequate for FIs to just store information indefinitely to meet compliance obligations, the new data protection laws warrant FIs to responsibly and defensibly delete information when it has served its purpose or when customers specifically ask them to. Inadequate classification can result in ineffective management of records and data that are subject to system or legal holds, for example.

Data transfer and data localisation

While FIs look to transfer data across borders to ensure internal efficiency and improve fraud and money laundering detection, transferring private data to countries that do not uphold the same data protection rules may result in significant fines.

Data portability and data protection

PSD2 and Open Banking require FIs to make a customer's data more accessible, while GDPR and other data protection laws are about controlling access to customers' data and keeping track of data shared with third parties.

COMPLIANCE CHALLENGES AMIDST NEW COMPLEXITIES

Regulatory compliance has always been a challenge for global FIs in terms of costs and resources. In this report, we have looked at a set of rising complexities that have contributed to increasing the compliance challenges for global FIs in the recent years.

Arguably, compliance challenges emanating from new data privacy and protection regulations have been the most impactful of all recent governance developments, along with changes in the types and sources of information assets that are now owned and managed.

#1

REGULATORY DIVERGENCE IS THE NEW NORM

#2

DATA PROTECTION IS A GLOBAL "PUSH" PHENOMENON

#3

THERE IS NOW A WIDER SCOPE FOR INFORMATION GOVERNANCE

#4

THERE ARE EMERGING DATA LOCALISATION IMPERATIVES AND CONSEQUENCES

#5

INFORMATION ASSET OWNERSHIP AND VALUE FOR BUSINESS LEADERS HAS SEEN MAJOR CHANGES

#6

THERE IS A HEAVY COST TO REGULATORY FRAGMENTATION

The Complexities

#1 COMPLEXITY

REGULATORY DIVERGENCE IS THE NEW NORM

Data protection takes centre stage in regulatory divergence

Since 2008-09, financial industry regulators around the world have generally been committed to strengthening capital, liquidity, and leveraging standards for banks. Ten years after the financial crisis, the resulting push for global regulatory harmony is giving way to divergent stances on the need for compliance, as long-awaited major reforms take effect in the EU and the deregulatory agenda of the Trump Administration comes into effect. For banks with a global presence, this divergence can create uncertainty, complexity and an uneven playing field.

The crises driven regulatory era (2008–2014)

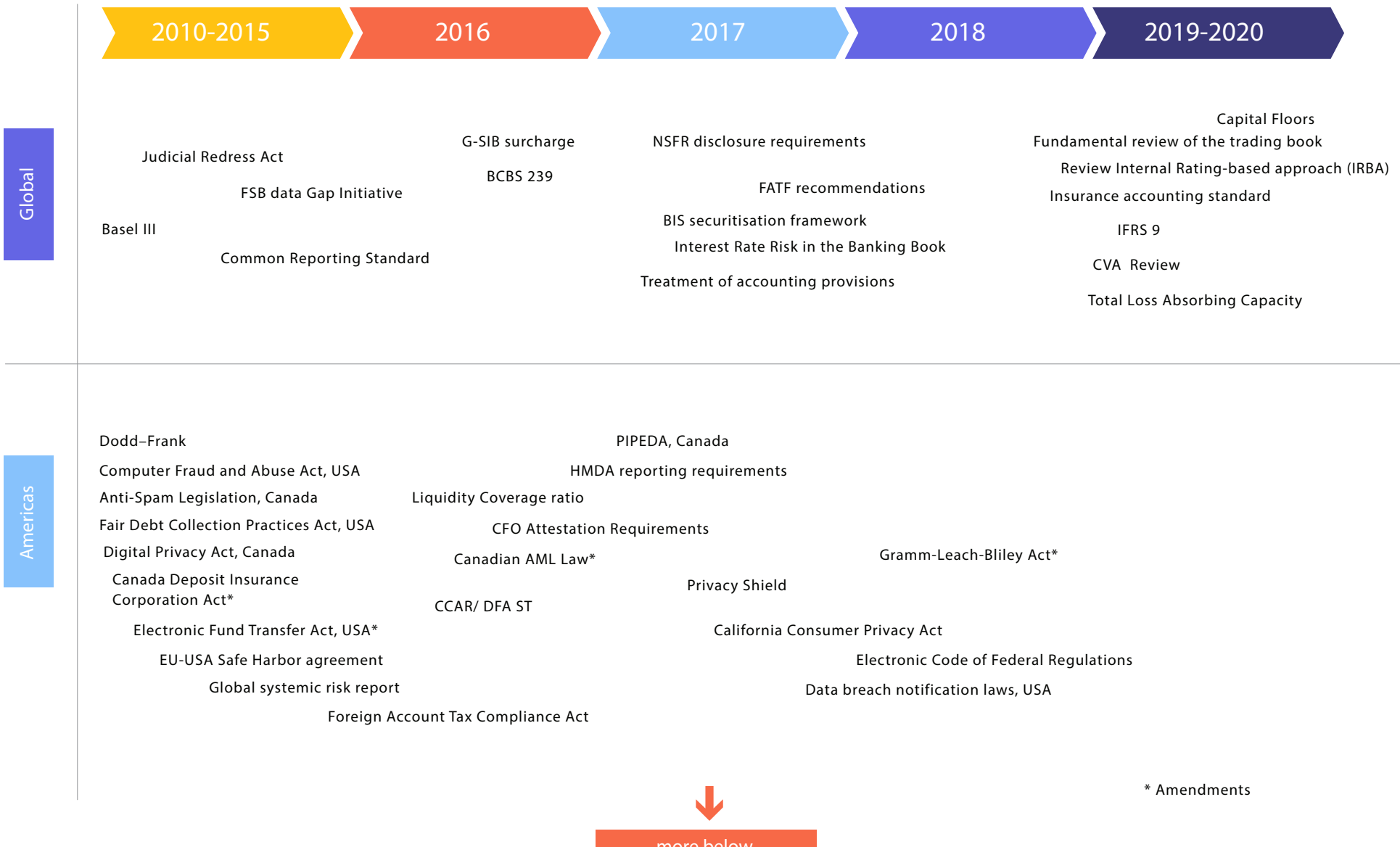
Since the global financial crisis, regulators in the US, Europe and Asia, often inspired by the G20 countries and the Financial Stability Board, have been racing against each other, and time, to implement many new regulations targeted at managing systemic risk, improving public revenue collection and enhancing transparency and investor protection. These regulations span global OTC derivative reforms (Dodd-Frank, EMIR), tax compliance regulations (FATCA, CRS), BCBS 239 and local and intra-block AML and KYC regulations (for example, the 4th EU Money Laundering Directive). However, KYC, AML and other regulations such as BCBS 239 that mandate the collection and sharing of data are often at odds with adherence to local data privacy obligations and potentially interfere with the right to privacy.

The data-driven regulatory era (2015-present)

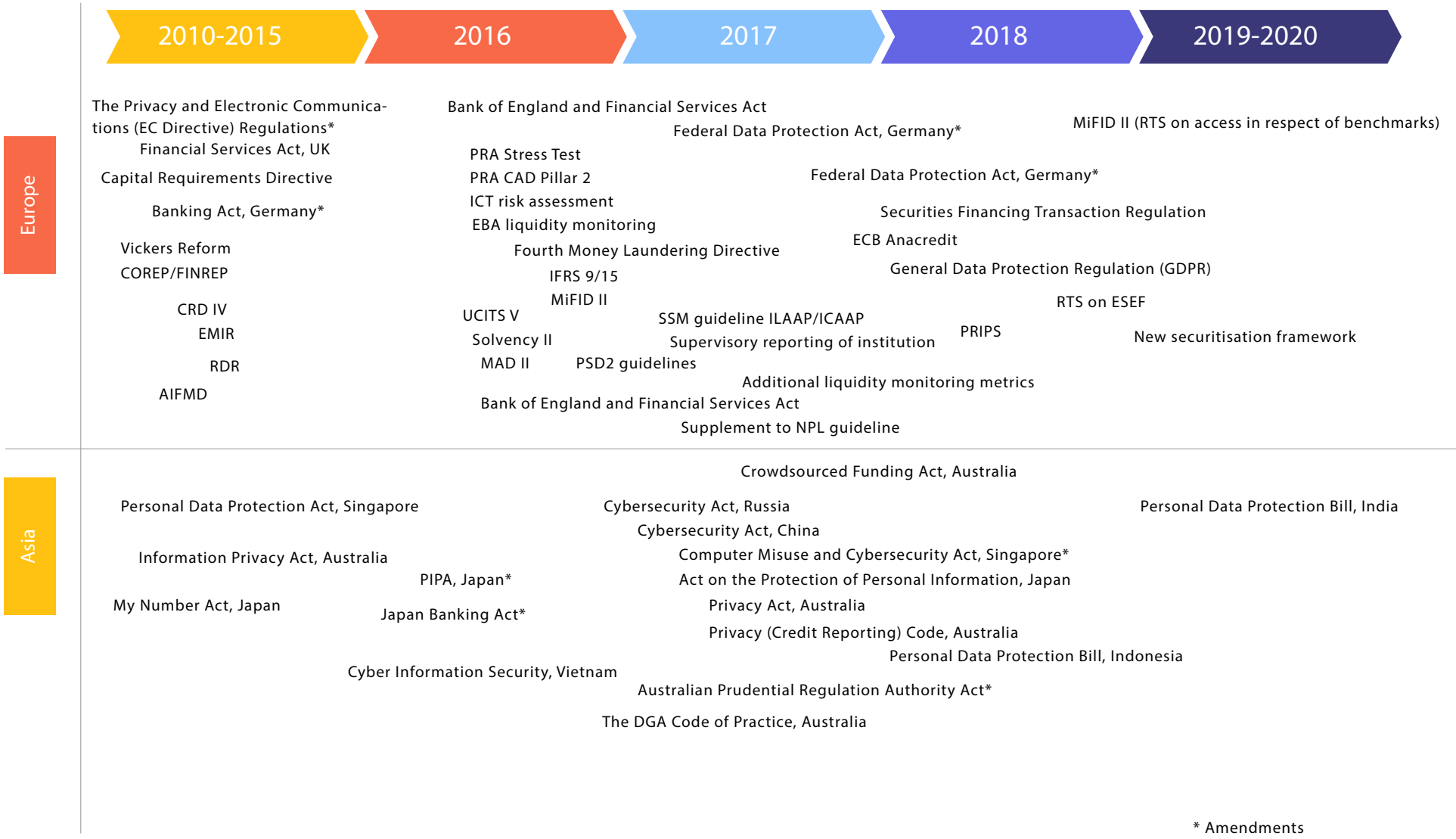
From domestic regulatory measures such as the Foreign Account Tax Compliance Act (FATCA), the Dodd-Frank Act in the US and the Retail Distribution Review (RDR) in the UK, to regional measures such as the Alternative Investment Fund Directive (AIFMD) and the European Market Infrastructure Regulation (EMIR) — as well as UCITS V/VI, the Markets in Financial Instruments Directive (MiFID) II, Market Abuse Directive (MAD) II, Solvency II and Packaged Retail Investment Products (PRIPs) proposal to come — each new regulation will carry with it a unique set of data requirements, reporting deadlines and compliance challenges.

In addition, there are specific regulations on data protection and privacy such as GDPR in Europe and cybersecurity laws in various countries that have emerged in the wake of frequent data breaches that have happened across industries.

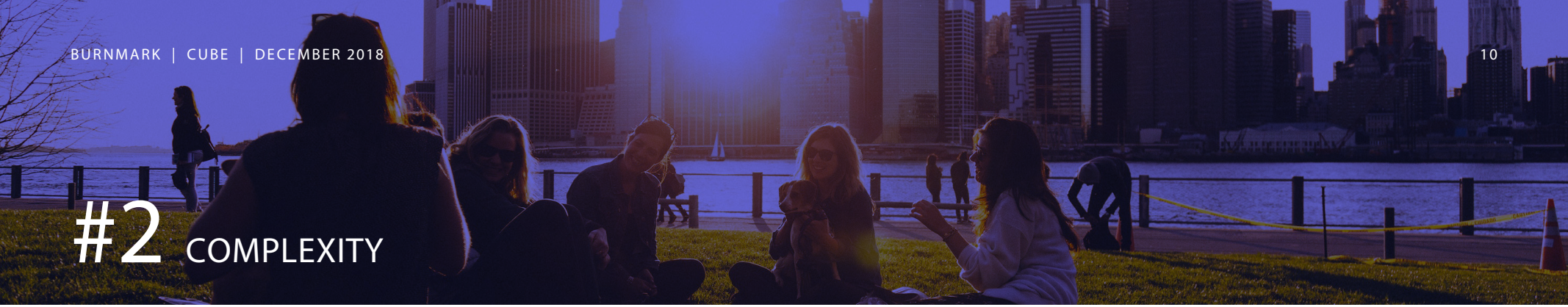
#1 COMPLEXITY /
Regulatory divergence in data protection and privacy laws across the world



#1 COMPLEXITY /
Regulatory divergence in data protection and privacy laws across the world



* Amendments



#2 COMPLEXITY

DATA PROTECTION IS A GLOBAL "PUSH" PHENOMENON

Data privacy and protection legislation is a multi-jurisdictional concern

According to the United Nations Conference on Trade and Development, 107 countries have enacted some form of data privacy and protection legislation and 138 countries have enacted cybercrime legislation.

A number of international privacy frameworks have emerged in various parts of the world which are influencing national policies on data privacy legislation in various countries. The three most prominent ones are: the Organisation for Economic Co-operation and Development (OECD) Privacy Guidelines, the Convention 108 of the Council of Europe, and the Asia Pacific Economic Cooperation (APEC) Privacy Framework. Out of these three, 'Convention 108' is the only existing legally binding international treaty with global relevance.

Due to the non-binding nature of other international privacy frameworks, the legal landscape in data legislation varies on several fronts, ranging from general differences on fundamental concepts (such as what constitutes personal data) to overarching philosophical differences on data collection and processing.

Europe: The mecca of legislation

Europe has had the largest amount of data-related legislation implemented, with 98% of countries currently holding active data legislation. In many EU countries, GDPR is emerging to be a valuable tool in strengthening national policies for improved data protection. However, with countries and regions approaching issues of privacy, security, data protection and 'rights' in different ways, interpreting and meeting GDPR requirements may not be so simple.

The Americas: Decisive steps towards data privacy

Across North America and Latin America, 51% of countries have data privacy legislation and 23% are in the process of drafting. As of March 2018, all 50 US states have enacted breach notification laws that require businesses to notify consumers if their personal information is compromised. In 2018, Canada and Brazil became the latest countries to unveil data protection legislation. The US Senate has also recently held a series of hearings where major technology firms were asked for inputs on data privay legislation and their mode of implementation.

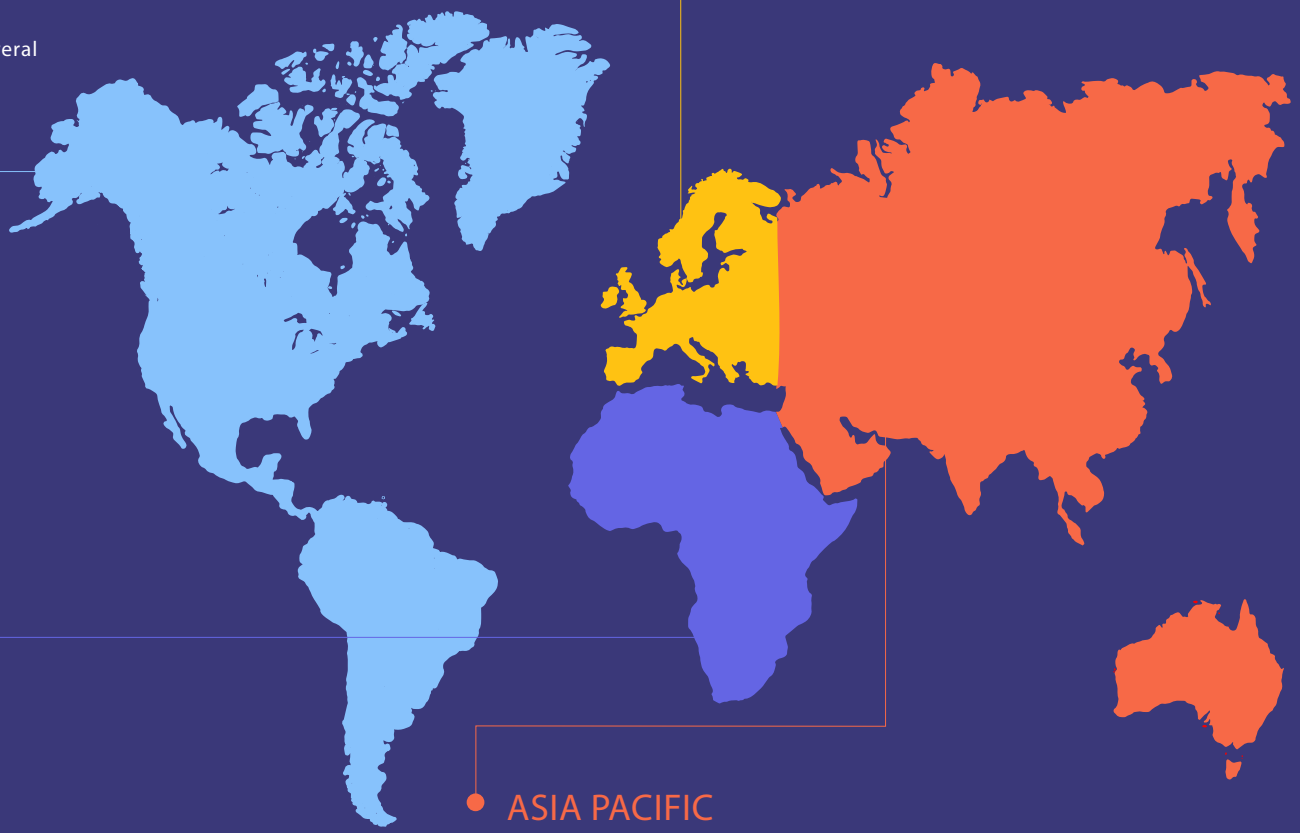
Asia Pacific and Africa: Encouraging signs

Asia and Africa show a similar level of adoption with around 40% of countries having data legislation in place. While there is considerable awareness around data security and privacy, governments in Africa are still very restrictive in establishing data classification policies that over-classify data in terms of confidentiality.

In Asia, 45% of countries have data-related legislation, while 7% of them including Iraq, Jordan, Pakistan and Thailand are in the process of drafting them. Regionally, the continent has the APEC Privacy Framework which aims to develop a uniform standard of data protection law across the region. Only China, Hong Kong, Indonesia, Japan, Korea, Malaysia, Philippines, Singapore and Vietnam are a part of this regional bloc. Unlike GDPR, the Cross Border Privacy Rules (CBPR) system does not displace or change a country's domestic laws and regulations.

#2 COMPLEXITY /
The state of data protection and cybercrime legislation around the world

The enforcement of GDPR in Europe along with some of the high profile data breaches by internet giants is setting the tone for several regional variants of data protection and cybersecurity legislation around the world.



AMERICAS
(35 countries)

Data Protection and Privacy Regulation
- Legislation: 18 (51%)
- Draft Legislation: 8 (23%)

Cybercrime Regulation
- Legislation: 26 (74%)
- Draft Legislation: 3 (9%)

AFRICA
(54 countries)

Data Protection and Privacy Regulation
- Legislation: 22 (41%)
- Draft Legislation: 7 (13%)

Cybercrime Regulation
- Legislation: 28 (52%)
- Draft Legislation: 11 (20%)

EUROPE
(45 countries)

Data Protection and Privacy Regulation
- Legislation: 44 (98%)
- Draft Legislation: 0 (0%)

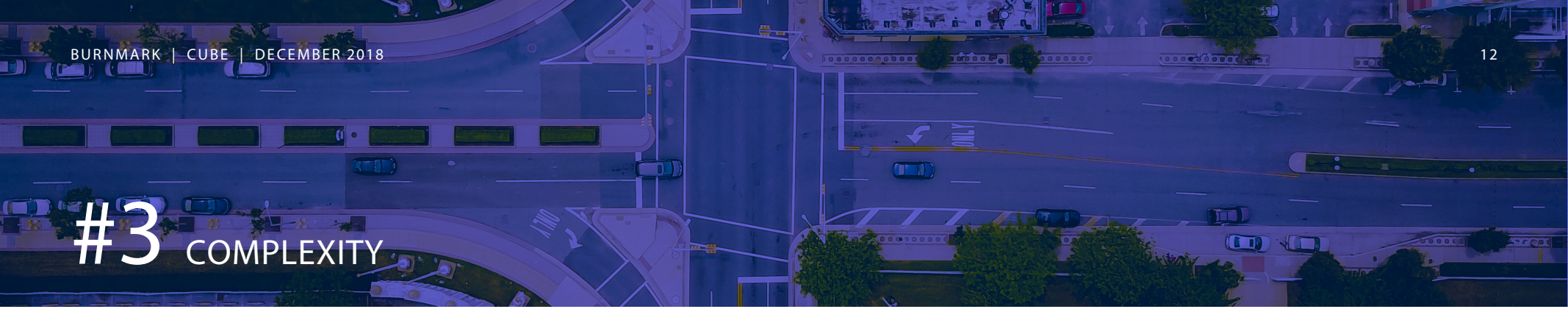
Cybercrime Regulation
- Legislation: 44 (98%)
- Draft Legislation: 0 (0%)

ASIA PACIFIC
(60 countries)

Data Protection and Privacy Regulation
- Legislation: 27 (45%)
- Draft Legislation: 4 (7%)

Cybercrime Regulation
- Legislation: 42 (70%)
- Draft Legislation: 4 (7%)

The % figures denote the proportion of countries,in the respective geographic region, where data protection and cybercrime regulations are either live or in draft status



#3 COMPLEXITY

THERE IS NOW A WIDER SCOPE FOR INFORMATION GOVERNANCE

Manage information throughout the lifecycle

FIs are now moving towards a compelling new operating model, which places customer engagement and retention firmly in mind. Consequently, there is a need to consider the specific elements of customer data privacy risks that must be addressed.

There are various regulations that impact one or more stages of the information lifecycle. GDPR gives customers unprecedented rights across different stages of the information lifecycle. Privacy regulations introduce a trend in granting new customer rights when it comes to the collection, processing, retention and distribution of their data.

Data collection and retention

Privacy laws now ask that FIs only collect data in which they have a legitimate interest and that they have a justified reason for requesting or collecting the client/counterparty data. This may clash with the compliance teams' need for additional data for financial crime, AML and risk purposes.

FIs must also address the conflict between lengthy retention requirements (regulatory or business-driven) and data privacy regulation, which mandates disposal of data once it is no longer needed for the purpose it was originally collected.

Data processing

GDPR gives customers the right to restrict processing. Individuals have the right to request restriction or suppression of their personal data. However, this is not an absolute right and only applies in certain circumstances.

When processing is restricted, you are permitted to store the personal data, but not use it. An individual can make a request for a restriction verbally or in writing.

Data sharing

While GDPR warrants FIs to take consent before sharing, PSD2 and Open Banking regulations mandate FIs to share customer data with other firms upon a customer's request.

The challenge to retail banks will be to assimilate this data for both client experience and also traction of client longevity. However, the antithesis of collecting these rich levels of data exposes the organisation, its executives, employees and other agencies to intentional and unintentional data disclosure, breach and theft for which mitigation is required.

#3 COMPLEXITY /

The impact of regulatory requirements on information governance stages

NO	Regulatory initiative	Region of Origin	Data Collection	Data Processing	Data Sharing	Data Security
1	BCBS 239	Global				
2	FSB Data Gaps Initiative	Global				
3	Legal Entity Identifier initiative	Global				
4	BCBS review of pillar 3 disclosure requirements	Global				
5	Privacy Shield	EU-USA				
6	Recovery and Resolution Directive	EU				
7	CRD 4	EU				
8	COREP	EU				
9	FINREP	EU				
10	MiFID II	EU				
11	EMIR	EU				
12	MAD II	EU				
13	GDPR	EU				
14	SEPA Regulation	EU				
15	Solvency II	EU				
16	European Institute of Financial Regulation	EU				
17	PSD2	EU				
18	Wheatley Review of LIBOR	UK				
19	Open Banking	UK				
20	FATCA	United States				
21	The California Consumer Privacy Act	United States				
22	Canadian Privacy Statutes	Canada				
23	Privacy Act	Australia				
24	Personal Information Security Specification	China				
25	Data Protection Act	Russia				
26	Act on the Protection of Personal Information	Japan				
27	Data Privacy Act	Phillipines				
28	Data protection law	Qatar				
29	Personal Data Protection Act	Singapore				
30	Law on the Protection of Personal Data	Turkey				

Significant Impact

Moderate Impact

Low Impact

The information governance process is impacted by almost every regulation today

#4 COMPLEXITY

THERE ARE EMERGING DATA LOCALISATION IMPERATIVES AND CONSEQUENCES

Variations in cross-border data flow restrictions

While the economic and trade opportunity from connectivity and data flows are significant, governments are increasingly introducing measures which restrict data flows. Consequently, multi-jurisdictional FIs are confronted by a patchwork of disparate data transfer laws, many of which place restrictions on the transfer of personal data from one jurisdiction to another. Even countries that do not impose specific cross-border data transfer restrictions may, nevertheless, regulate certain data transfers through limitations on data sharing or disclosure.

While some countries enact blanket bans on data transfers, many are sector-specific, covering personal, health, accounting, tax, gambling, financial, mapping, government, telecommunications, e-commerce, and online publishing data. Other national laws, particularly those aimed at the financial services sector, also may impact whether and how personal data can be transferred.

Data transfer legislation varies significantly across regions

- Under Canada's PIPEDA, data transfers are not restricted, but organisations remain responsible for the protection of personal data in their control even after transfer outside of the jurisdiction.
- Mexico has adopted an accountability model containing multiple exceptions to the requirement to obtain consent which includes cross-border transfers between affiliated companies, transfers necessary by virtue of a contract that is in the individual's interest and transfers to cloud computing service providers, subject to specific safeguards.
- In Latin America, EU-style omnibus laws often contain requirements that are similar to those found in GDPR.
- Macau and Malaysia have implemented EU-style transfer restrictions, prohibiting cross-border transfers except (1) with consent; (2) if the recipient country is an approved jurisdiction, or (3) if another exemption applies.
- Some APEC nations, including Australia, New Zealand, and the Philippines, have adopted accountability models for cross-border data transfers.

Mechanisms to facilitate data transfer across borders

One way forward is being developed by the APEC forum through its CBPR system, serving as a mechanism that fosters trust and facilitates data flows among participants. South Korea has become the fifth member economy to join the CBPR system.

On 17 July, 2018, the European Union and Japan successfully concluded negotiations on a reciprocal finding of an adequate level of data protection, thereby agreeing to recognise each other's data protection systems as "equivalent". This will allow personal data to flow safely between the EU and Japan, without being subject to any further safeguards or authorisations.

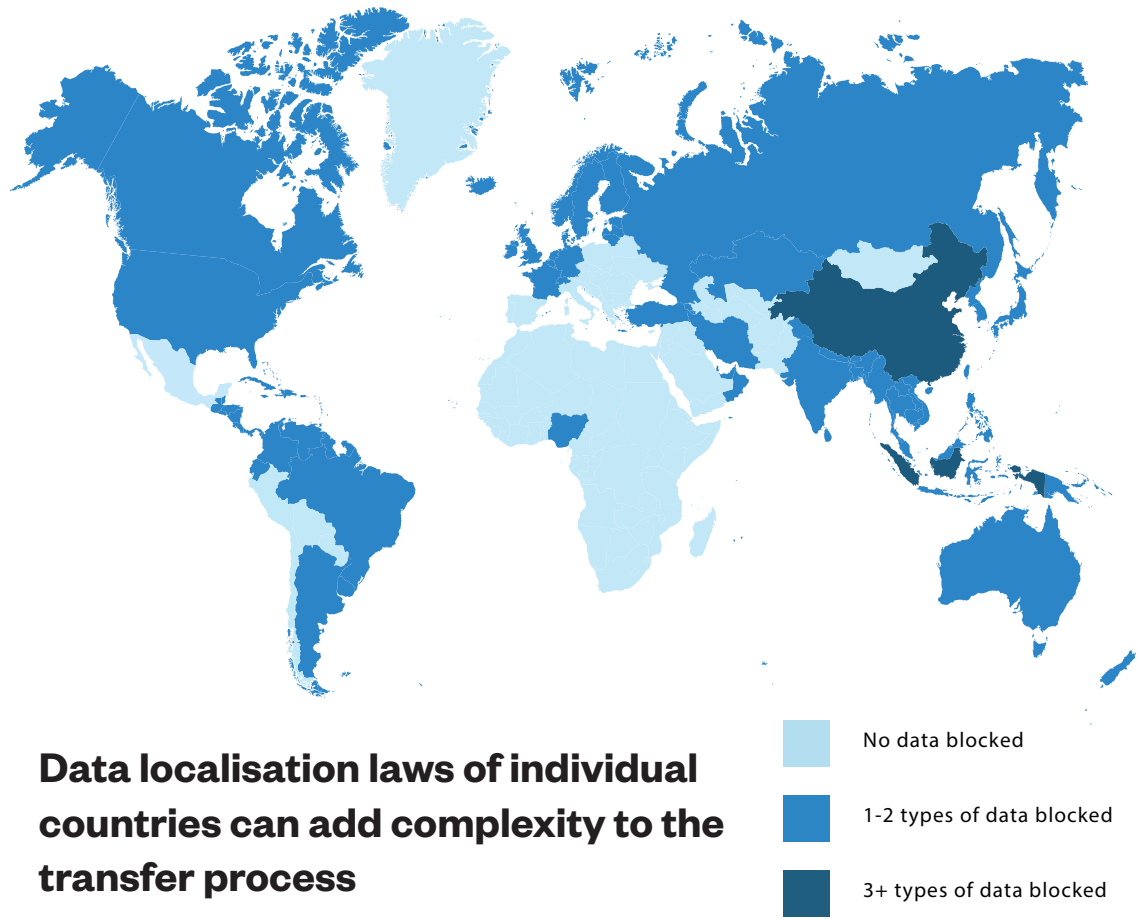
#4 COMPLEXITY /

Cross-border data flow restrictions vary significantly across jurisdictions.

What type of data is blocked by various countries?

Country	Financial Data	Personal Data	Government Data
China	Y	Y	
Germany	Y	Y	
India	Y		Y
Nigeria	Y		
UK	Y		
USA	Y		Y

Note: Data sourced from an ITIF analysis of laws and regulations (as of April 2017). The above table provides a sample of countries where data flows are blocked. The types of data blocked according to ITIF are financial, personal, government, digital, telecom and other.



Data localisation laws of individual countries can add complexity to the transfer process

#5 COMPLEXITY

INFORMATION ASSET OWNERSHIP AND VALUE FOR BUSINESS LEADERS HAS SEEN MAJOR CHANGES

Get customer data and information governance to serve multiple masters

Banks of every size are more focused than ever on rebuilding relationships based on trust and loyalty. To achieve this objective, banks must meet the modern customer's expectations and deliver services that are convenient, integrated and accessible. To do that profitably and consistently, banks need to be much more connected. Over the past few decades, banks have become adept at gathering data but are not yet fully capable of (or comfortable with) sharing this information effectively across their organisations. Moreover, many institutions are struggling with legacy systems that are not able to interact or communicate with each other.

Where there is a reluctance to share this important data, due to traditional fiefdoms, lack of trust or because management fails to support its own directives to share, the cost can be lost revenue.

In the quest to monetise data by creating business value and fostering a data-driven culture, data and analytics leaders, especially the Chief Data Officers (CDOs), must come to terms with the ever-increasing quantity and complexity of information assets and their use. Traditional cost-based, control-oriented and internally focused approaches to data and analytics inhibit innovation, creativity and responsiveness. Silos are maintained, opportunity benefits are missed, while experimentation and entrepreneurialism are potentially stifled by the need for certainty and consistency.

- The top tier of a client-centric business model is the "client modern experience." This is about creating modern, relevant services and it is the outbound interface (channels) banks have with their clients that drives loyalty and new service adoption.
- Below this is the"operational transformation layer," that enables the client experience and creates the ability to deliver new client-centric products and services with greater speed.
- The third layer, reinforcing operational transformation, is the "operational risk and regulatory compliance layer." Intended to be an all-encompassing approach to digital risk mitigation, it involves infrastructure and endpoint security; regulatory compliance and audit; and proactive threat mitigation.

#5 COMPLEXITY /
Enterprise information governance stakeholders - and their wide-ranging objectives

Chief Marketing Officer
Demonstrate customer-centric brand leadership and distinction in the digital economy

Chief Technology Officer
Deliver agility through digital transformation initiatives by leveraging new technologies like big data, AI and NLP

Chief Data Officer
Enhance data quality and data-driven business growth by exploiting internal and external data

Chief Financial Officer
Reduce the cost of operations while balancing effectiveness, efficiency and risk

Chief Compliance Officer
Monitor and comply with global regulations governing information assets, including record-keeping and data privacy and protection law

Chief Operating Officer
Explore new sources of revenue and profit growth, monetise data and improve operational efficiency

Data ownership and utilisation is diverse for the group of executives in large global banks

#6 COMPLEXITY

THERE IS A HEAVY COST TO REGULATORY FRAGMENTATION

Fragmented data protection regulatory framework in the US

As an example of regulatory fragmentation, the United States follows what is referred to as a 'sectoral' approach to data protection legislation. Under this approach, the governance of data protection and privacy rely on a combination of legislation, regulation and self-regulation rather than governmental control alone.

There are many laws at the state level that regulate the collection and use of personal data; and the number grows each year. Some federal privacy laws pre-empt state privacy laws on the same topic. For example, the federal law regulating commercial e-mail and the sharing of e-mail addresses pre-empts most state laws regulating the same activities.

Conversely, there are many federal privacy laws that do not pre-empt state laws, which means that a company can find itself in the position of trying to comply with federal and state privacy laws that regulate the same types of data (for example, medical or health records) or types of activity.

Most states have enacted some form of privacy legislation, however, California leads the way in the privacy area, having enacted multiple privacy laws, some of which have far-reaching effects at a national level.

In the US, there is no single, comprehensive federal (national) law regulating the collection and use of personal data. Each Congressional term brings proposals to standardise laws at a federal level. Instead, the US has a patchwork system of federal and state laws and regulations that can sometimes overlap, dovetail and contradict one another.

Financial regulators in the US

- The Federal Reserve, which sets the nation's monetary policy and regulates banks
- Office of the Comptroller of the Currency, which supervises all national banks and federal savings associations
- National Credit Union Administration, which regulates credit unions
- The Federal Deposit Insurance Corp., which insures money deposited with banks
- The Securities and Exchange Commission, which oversees publicly held companies and US securities markets
- The Financial Industry Regulatory Authority that acts as a self-regulatory organisation
- The Office of Thrift Supervision, which, until 2011, oversaw savings and loan associations
- The Federal Communications Commission, that regulates interstate and international communications
- The Commodity Futures Trading Commission, that oversees the derivatives and futures markets
- The Consumer Financial Protection Bureau, which regulates consumer financial products and services

#6 COMPLEXITY /
Complex and fragmented data protection regulatory framework in the US

Sectoral regulations	MY DATA Act Email Privacy Act	The Health Insurance Portability and Accountability Act Family Educational Rights and Privacy act	BROWSER Act
Cross-border data transfer regulations	EU-USA Safe Harbour framework (now defunct)	Privacy Shield	Judicial Re-dress Act
Federal privacy laws	The Fair Credit Reporting Act The Federal Trade Commission Act	CAN-SPAM Act Wiretap Act Gramm-Leach-Bliley Act	The FCC Privacy Rule (*now repealed*) Department of Homeland Security Data Framework Act The Financial Services Modernisation Act
State data protection regulations	The California Security Breach Notification Law Massachusetts Data Protection Law New York SHIELD Act	The California Electronic Communications Privacy Act Data Breach notification regulation in all 50 states Chicago Personal Data Collection and Protection Ordinance	Georgia, Personal Data Protection Ohio Senate Bill 220 Minnesota Plastic Card Security Act

The US approach to data protection involves complexities due to application of both state and federal laws

INTERVIEW

HOW ARE GLOBAL BANKS HANDLING THE NEW ERA OF DATA PRIVACY AND DATA PROTECTION?

Conversation with Lynn Molfetta, Global Head of Records Management, Deutsche Bank

What are some of the greatest challenges for large global banks dealing with the changing regulatory environment?

We are required to comply with all regulations that relate to our business. Over time, Deutsche Bank has implemented global standards for retention obligations across all jurisdictions; however, the standard established for some jurisdictions may conflict with new retention obligations. With GDPR, as an example, this has required us to adjust or make exceptions to some rules in order to address privacy issues. It is also challenging to apply rules throughout the organisation, given the inordinate amount of data that banks the size of Deutsche Bank create. This challenge is escalating, as the regulatory world is changing.

How has this contradictory nature of regulation made record-keeping more complex?

In the past, records management was purely based on rules that stipulated how long you needed to retain records, and as soon as the retention obligations were met you could dispose of them. When you add privacy regulations on top, which in some cases can overrule the retention schedule, it gets complicated. A former customer might request their data back, and it's difficult to know how we resolve that when our regulatory retention obligation is outstanding. That's a complication that all banks are dealing with right now.

Legal teams are heavily involved in Deutsche Bank's GDPR program, because they must be able to prove that any information kept beyond retention has an identifiable, ongoing litigation or regulatory requirement. Previously, Legal teams have preferred to retain records beyond the regulatory requirement 'just in case'. This was the safety net, but with GDPR, retaining the data could get a bank into more trouble than deleting it. This new requirement to destroy more information, under specific conditions, has created both cultural and technological challenges.

Some systems within large banks have very long retentions on them, because they house prospective data that is analysed to help understand our business models. Some data has limitations of action, requiring it to be kept longer than the retention obligation stipulates, and figuring out how to apply retention when Personally Identifiable Information (PII) is involved is challenging. At Deutsche Bank, we're working to get ahead of these situations, because we want to keep focus on using these systems for their original purpose, rather than working on solving retention issues. Every system must be re-tested for examples like this, which are arising more often because of new, conflicting regulations.

What are some of the multi-jurisdictional challenges you encounter?

Our systems are global, and our processes need to be global, so that we can ensure we have the right governance and controls in place to safeguard compliance. For us to apply a rule for each country, without any global standard application, is very hard. Deutsche Bank operates in more than seventy jurisdictions, so cross-border transfer of records and data adds a lot of complexity. We have to know where the information

POINT OF VIEW

originated, where it is stored, and which jurisdictions it passes through. Every instance must be evaluated, and then have a specific rule put on top of it, which is difficult to control for large global banks transferring data from one jurisdiction to another. Even though GDPR is a European rule, for Deutsche Bank it is a global concern.

How are your processes set up to manage these challenges?

Like all banks, we build technological rules on top of an application to ensure we are compliant. First, you must understand what data is being stored in that application, then you need to apply the retention, and then you have to examine the PII data that sits within that application. In practice, the retention obligation is the primary driver. In some instances, if there's PII data that absolutely has to be deleted at the time it meets its retention deadline, and it co-exists alongside other information that's not PII, we have to move that data elsewhere in order to meet all regulatory obligations. In other instances, we're looking at applying those rules right on the system. We have multiple businesses and processes, so it's never a 'one size fits all'. It's difficult for banks of our size to put global rules in place and then provide those rules to the businesses to operationalise, fully knowing that the complexity of their regional operations conflicts with the general rule. So, you have to dig deeper, and work with your businesses on the end-to-end process.

How does the organisation come together in the process, to become compliance-ready?

Speaking with colleagues across the industry there is only one effective approach. It requires a governing body at the top, which brings the businesses and the infrastructure groups to the table, to have their say on how best they can apply the agreed, consistent set of rules. Policies and procedures are put in place and we work with our businesses to ensure that they can both adopt and adjust them to fit their needs. The policy stipulates that the businesses must comply with the rules, but they remain responsible for execution in their own region. We help to ensure that the technology is available, the right people are watching the data correctly, and they have the right controls in place. The regulator can see that there is consistent leadership from the top down, in support of compliance.

How do you plan to use technology within records management?

As the incoming Head of Records Management, nearly four years ago, I knew that for Deutsche Bank to implement a program we could stand behind we needed an authoritative source of regulatory information. I worked with the CIO Group to choose a tool that would enable me to manage the retention obligations for records management at a global level. We also needed to be sure that the tool I was implementing for records management was applicable for other groups within Deutsche Bank. For instance, when the regulatory technology team looks for a solution that monitors upcoming regulations, and enables them to push them out on a timely basis, we needed a tool suited to that function also. The privacy group and other stakeholders provided their requirements, and then we relied on the technology group to source the right solution.

What do you look for in a technology solution?

I look at many factors, including scope, breadth, agility, time to market, and responsiveness. I look at my criteria for records management, and then I evaluate the technology accordingly. The true test is whether it can do everything it claims, and whether it can be implemented into the pre-existing infrastructure, which is a big challenge for large banks. Connecting the pipes is an extraordinarily difficult thing to do because we have well-established internal processes for information security and so on, and a lot of providers underestimate the challenge of bringing their solution in-house. A cloud solution is much easier to implement than bringing a system in-house and trying to build it out internally, if you can make sure that the security and the controls are in place to ensure that your data is secure.

What are your top priorities for the next five years?

Our focus is on ensuring that the lifecycle of data and information at Deutsche Bank is absolutely ironclad. From the creation to the disposition of data, the processes, governance and accountability surrounding that must be airtight. You have to look at it from the beginning to the end, front to back, and make sure that all of those controls and checkpoints are rock solid. Otherwise, when you can't see the full process, you

POINT OF VIEW

can't see the breaks along the way. This is an approach that our CEO fully supports, from the top of the house, which is essential because it is a long-term initiative that requires a cultural shift. You can't just throw a strategic plan out there and assume it will be executed throughout the business. We are working alongside the businesses, through execution, and prioritising programs based on risk and tolerance levels.

And your short-term priorities?

Our number one priority right now is to continue implementing our new tool. Once the businesses are on-boarded and trained, and we've got the right governance and controls in place within the system, our processes will be managed automatically from within the tool. An ongoing priority is to mature the program, and to adapt as the regulatory environment changes. New ways of working – the increasing use of social media, for example – present new and different challenges for record-keeping.

How do you ensure your position with the regulators is defensible?

Regulations are not black and white, they are open to interpretation, and this can lead to vulnerabilities. The businesses, and even the control functions, often challenge us because the interpretation of a regulation can be quite generic. We apply the principle of 'reasonableness', interpreting every regulation to the best of our ability within the processes that we're managing, which might fit one business but not necessarily another. We can't prescribe what every business must do to comply, because we don't know their systems and processes as well as they do, but we can offer a point of view and help remediate.

It's easy to focus on making a regulatory deadline, but in my experience, Regulators are there to work with you. They want to see your plan, understand what you think is reasonable to comply with, and be transparent and honest. If you commit to a plan, follow through with it and demonstrate progress, that goes a long way towards maintaining a defensible position. Building honesty and trust is key.

Where technology comes into play, as an important defence tool at Deutsche Bank, is to provide an auditable methodology, which greatly reduces the risk of breaching critical retention obligations and enables us to prove that the action we are taking is supporting compliance.

INTERVIEW

HOW ARE CHIEF DATA OFFICERS NAVIGATING THE MAZE OF DATA PRIVACY AND DATA PROTECTION?

Conversation with Tom Mavroudis, Chief Data Officer, Scotiabank

How has changing regulation impacted your role as Chief Data Officer? Has this altered your view of data from a strategic perspective, or your work with other stakeholders, like the CCO, to ensure compliance?

It has, dramatically. Regulations have forced transformative changes in managing how data is captured by producing systems and functions. Typically, front office businesses were accountable and responsible for producing the data that is required to drive revenue and execute their core business functions. Now, the CDO role is focused on expanding the responsibilities of Data Producers and holding them accountable for meeting the needs of more of the bank's Consumer requirements, including capturing data that is critical for Compliance, Risk and Financial Management.

How do you ensure the quality and security of data coming into the bank, given the number and variety of sources it is now coming from? What regulatory challenges are associated with the flow of data throughout your organisation, from data collection through to data sharing?

Instrumentation and tooling for executing data quality rules and controls is a necessity. The traditional approach has been to work back to front – identify the data sources that are being used for compliance, risk and financial management functions and measure the quality. Then identify root causes of data quality issues using data lineage, and then remediate the systems as close to the front that is accountable for producing the offending data. Lately, we have been exploring using data lakes, where we ingest data from a variety of sources front to back into an environment where we can run quality checks and reconcile data front to back in one place. The data lake process is effective only within jurisdictional borders; there are still cross-border data privacy issues that impact the ability of data from many countries from being copied over to a single central lake.

How has the process of transferring records and data internationally changed, what impact has new data privacy and protection regulation had on this process, and how are you managing this?

Data sharing agreements and cross-border data privacy controls are now an inherent feature of the data and records movement process. For new data interfaces being registered, where data is being transferred from one system to another, we require cross-border data privacy approval (which is reviewed by global and local country compliance teams), as well as technical contracts and SLAs captured in data sharing agreements that codify exactly what data is being moved from where to where.

With regulators pushing for the 'democratisation of data' with open API legislation, data governance now includes managing external or syndicated data from partners, as well as managing data shared with third parties. How does this affect your records and data management practices?

Regulations and rules vary globally and there is still some conflicting guidance on how much customer information to make available for sharing with third parties, especially in

POINT OF VIEW

light of breaches and mis-use of data by third parties. I think there is still some conservatism in adopting open APIs and information exchanges, and legal teams cautiously review efforts to share customer data (even with explicit consent) via open APIs.

Technology has expanded both the scale and scope of information assets. How are you utilising technology to manage these assets, given the above challenges? Can you share some examples or use cases of any cost, de-risking or compliance (speed) advantages using technology?

Because of the speed with which data is being created, use of traditional tools and techniques for building information warehouses are becoming more and more unviable. We see adoption of AI/machine learning and low-cost storage + elastic compute on cloud as being two technologies that are vital for maintaining information assets. The machine learning and AI can be used to support data discovery (classification + tagging) for entire ecosystems of databases with Natural Language Processing for more robust document meta-tagging, and cloud compute can be used for executing transformations, reconciliations, clustering, de-duping and other processes that require multiple scanning of databases and document repositories. Two examples:

First, on the structured data side, automated classification and clustering models are being deployed to find and master customer records so that we can link customer records across databases and create a holistic picture of the customer's behaviour which can be used in anti-financial crime profiling (e.g., AML, anti-bribery, anti-fraud).

Second, on the unstructured side, NLP tools are being used to classify and extract key data elements from documents, such as trade or credit service agreements, ISDAs, corporate loan agreements, in order to compare the information retained within the documents to structured data records being used in financial reporting. This would typically be a manual process, hiring temps to read through thousands of documents; this is now being done on a sustainable basis through deployment of NLP tools.

With organisations turning to multiple data governance tools and cloud vendors for critical operations, what are the challenges of maintaining information security in a hybrid records management environment?

Meta-data management and inventory management are critical. We must have enterprise data inventories and data dictionaries along with a view of where those data assets lie, and what are the minimum controls that are in place within each host. To the extent that information is highly distributed and federated in multiple environments of varying control, that is creating significant risk to organisations. Being able to agree on a common data glossary and putting logical to physical maps within a single data or document modelling or management tool is critical.

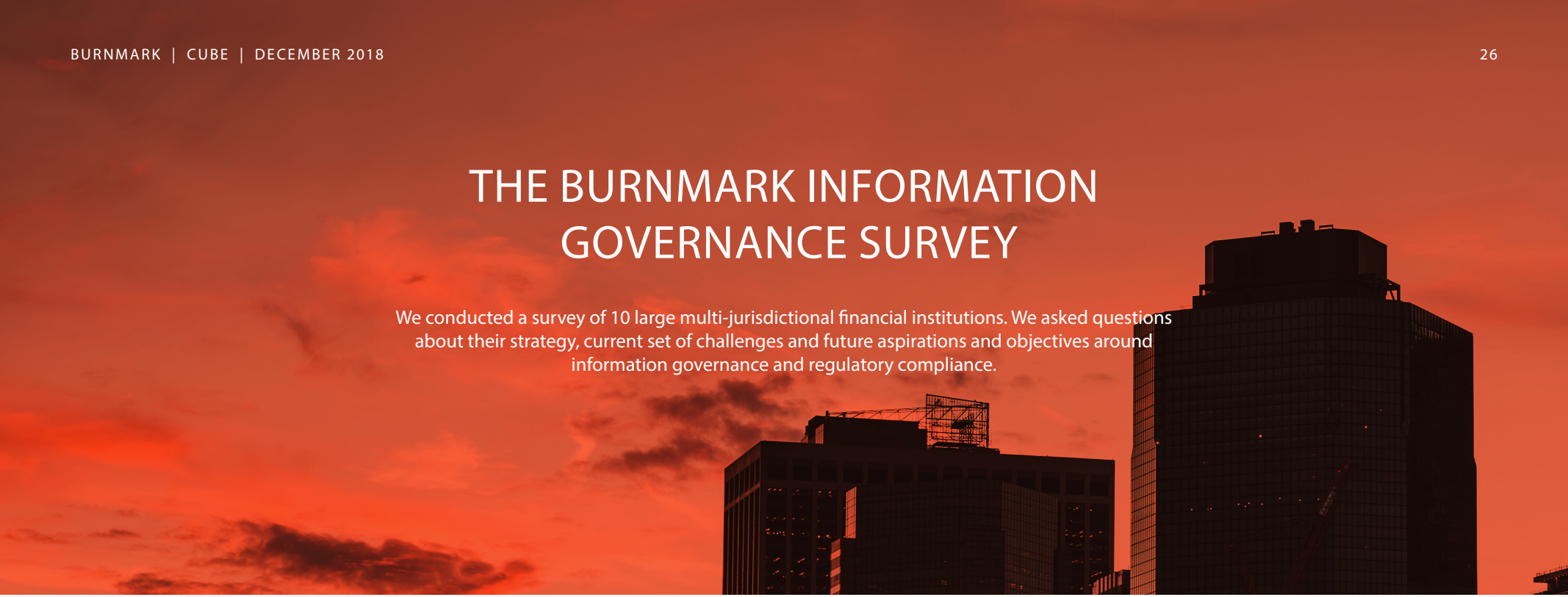
What metrics are being used to measure data governance ROI today in large organisations?

Business KPIs typically tend to revolve around improved RWA (risk-weighted assets) because of less punitive capital requirements required for bad data (or data not processed straight through), reduced false positives and cost of AML compliance, and reduced reported operational risks and losses due to lack of reconciled data between trade capture and settlement platforms.

What does the future look like? Do you think technology will play a significant role in handling aspects like privacy and security?

Yes. The ideal environment is one where data assets are catalogued, inventoried and tied to a set of required data protection and management controls. Systems that host data are assessed against their control requirements and we can assess the effectiveness of each system in implementing the set of controls based on the type of information held within the system. There is full transparency up to senior management as to which controls overall are strong and in line with expectations and which systems have weak controls in place.

The Survey



THE BURNMARK INFORMATION GOVERNANCE SURVEY

We conducted a survey of 10 large multi-jurisdictional financial institutions. We asked questions about their strategy, current set of challenges and future aspirations and objectives around information governance and regulatory compliance.

SURVEY PARTICIPANTS

BARCLAYS

Deutsche Bank

BNP PARIBAS

Standard Life

RAIFFEISEN

Freddie Mac

AVIVA

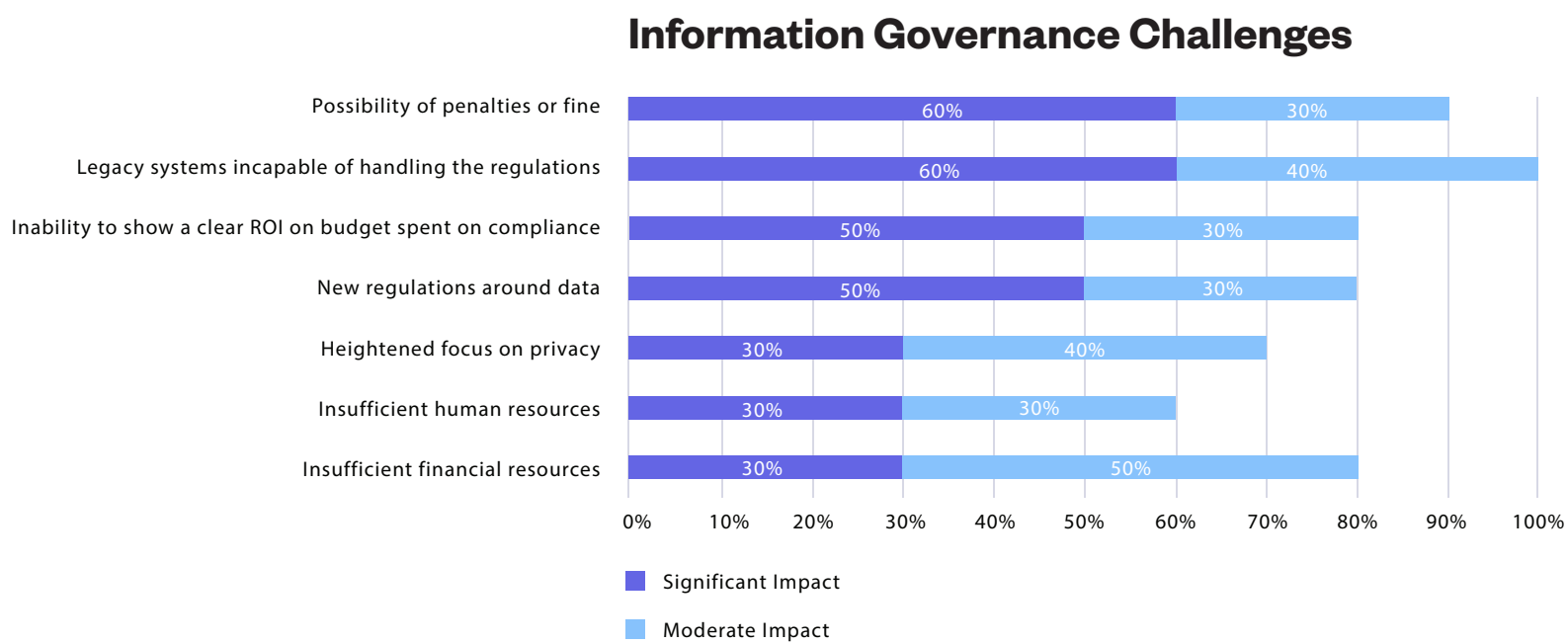
Aberdeen

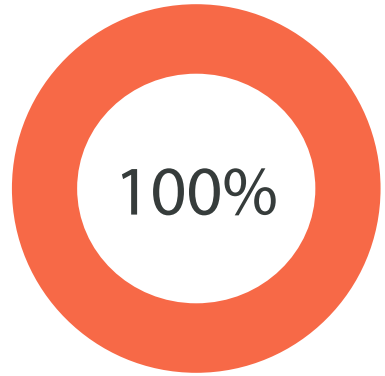
Danske Bank

Scotiabank

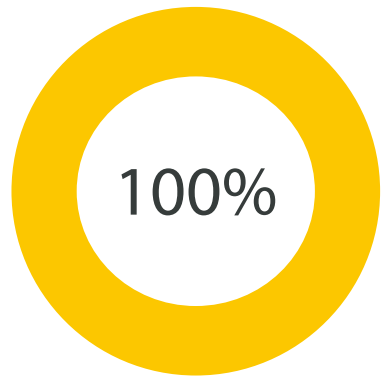
THE BURNMARK INFORMATION GOVERNANCE SURVEY

How much impact do the below challenges have on your ability to manage data and information governance?



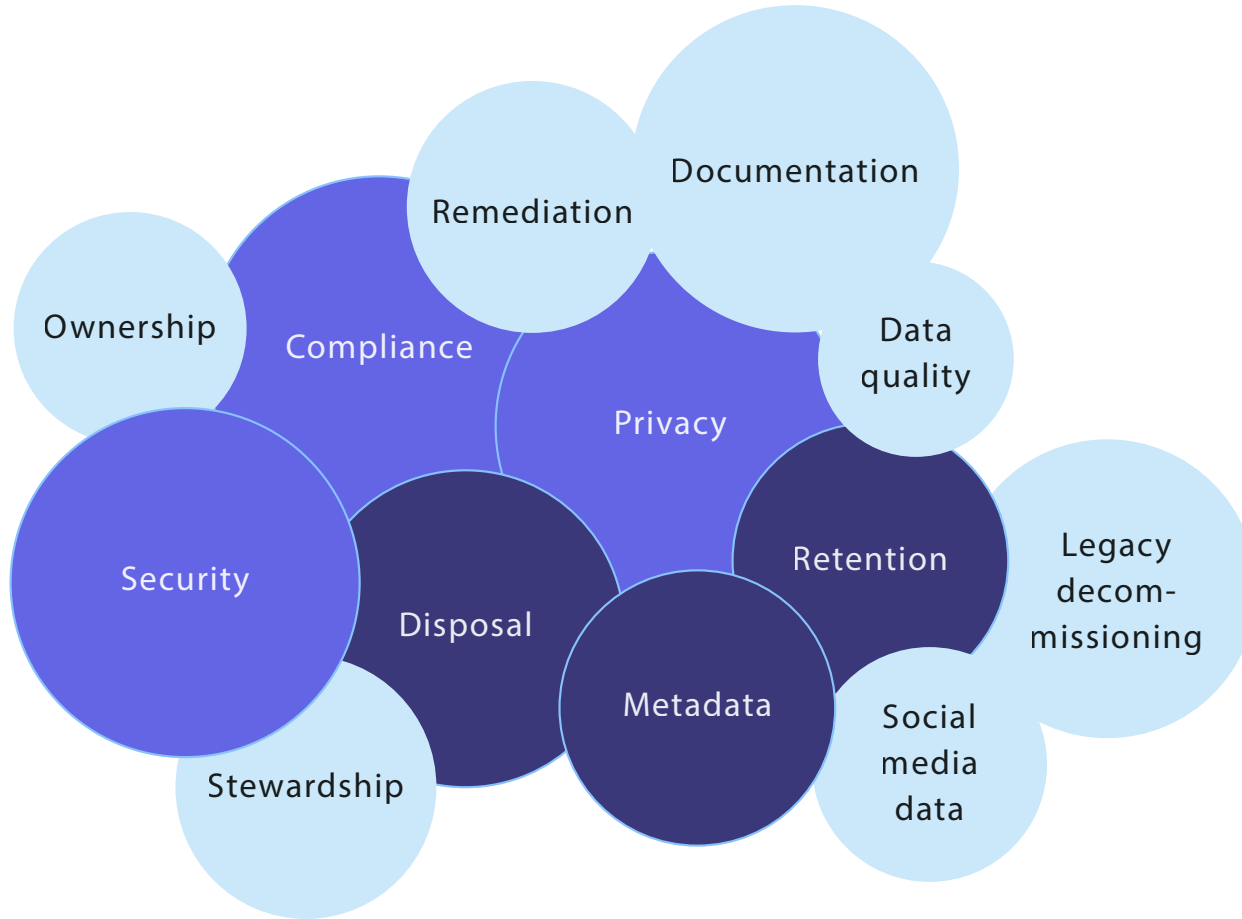


100% respondents agree that cross border and multi jurisdictional operations add complexity to data and information governance in organisations

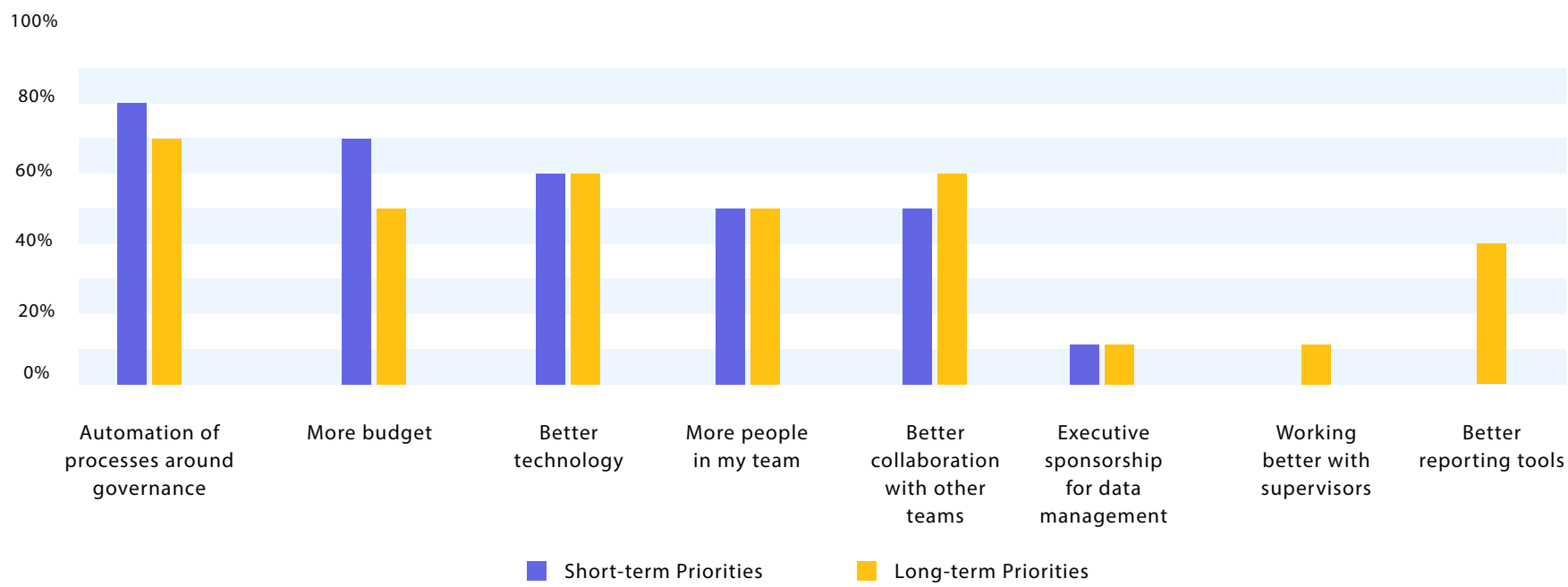


100% respondents say that complex and often contradictory nature of rules and regulations make data and information assets compliance more difficult

What are some of your key priorities (around data and information governance) for 2018-19?



What can help fulfill your key priorities in the short term (1-3 years) and long term (3-5 years)?



POINT OF VIEW

HOW IS THE WORLD OF INFORMATION GOVERNANCE EVOLVING IN A TIME OF EXTREME REGULATORY CHANGE?

Conversation with Matthew Bernstein, Information Management Strategist, MC Bernstein Data

What is your view on how the regulatory landscape is changing, and the challenges that are emerging, in what seems like a time of extreme regulatory change globally?

Information governance has been greatly affected by changes in regulatory focus. When I think of information governance, I think of information security and cyber risk, as well as data governance and records management. Regulators around the globe want to know what is being done to secure information and reduce risk.

Secondly, heightened focus on the handling of personal data, encompassing data privacy and protection, has led to a more scrupulous approach to regulation. Record managers now need to deliver governance at a far more granular level. When a record contains PII, for example, it opens the requirement to follow a whole different set of rules.

Finally, new regulations like MiFID II have extended records retention requirements into areas of the business where it has not been seen before. There is a heavy focus on electronic communications – email, chat systems, voice and social media predominantly – which the regulator needs to see recorded and monitored both retrospectively, and in real time.

In the wake of the financial crisis, initially we saw a lot of convergence of regulator supervision, but now we're seeing regionalisation of information governance, which is challenging from a compliance perspective. With GDPR, while everybody is following the same regulation, there are differences of interpretation across EU states, and we're also seeing jurisdictions outside the EU piggybacking on GDPR, which is introducing some interesting twists. This is leading to greater diversity in requirements, which is adding complexity to the regulatory intelligence and change management process.

How are financial institutions responding to this?

These challenges are best solved through technology that aligns with business functions and use cases, consuming vast quantities of regulatory intelligence, and communicating it to the right people, in a form that can be absorbed in an efficient way.

In the past, large financial institutions have tended towards over-retention of records and data, because it gave a sense of security and data storage was relatively cheap. That is all set to change, now that new regulations like GDPR have brought disposition into the spotlight.

Compliance and Legal teams responsible for maintaining regulatory intelligence are better-suited to advisory work than business-as-usual processes. They deal with a vast number of global regulators, huge volume of regulations, and diversity of data from a multitude of sources. Any attempt by these teams to maintain regulatory compliance in a cost-effective or risk-reducing manner, when the process remains reliant on human intelligence and manpower, has become unscalable, unreliable and unsustainable.

POINT OF VIEW

Technologically, there have been great advances in the management of structured data held in applications, databases, and trading systems. It's become easier to retain it, search it and archive these. The most challenging information to manage from a regulatory perspective is unstructured data, including communications, like email and social media. Documents are especially difficult to govern across the enterprise, because they live everywhere, and duplication is rife.

With so much regional variation in regulation, are multi-jurisdictional complexities being managed effectively today?

In Europe, country-specific regulations sit alongside pan-European regulations, and in the US we have federal versus state regulations to contend with. Historically, multi-jurisdictional financial institutions have struggled to maintain a central point of regulatory intelligence and governance. It is not unusual for regional compliance officers to make autonomous decisions concerning retention. But without enterprise-wide oversight across all jurisdictions, governed by one overarching centre of competence, business operations involving cross-border data usage are risky.

Multi-jurisdictional operations need technology that captures global rules automatically, aligns them with the organisation, and makes them available for people in a way that is oriented towards the business and that is accessible to everyone in the business. This enables a culture of compliance, which can be achieved easily, repeatably, reliably and dynamically.

What are banks prioritising from a technology perspective, in information governance?

There is a big drive within large global banks to use fewer systems and manage fewer vendor relationships. This drive towards simplified implementation and infrastructure is also encouraging banks to build out private or hybrid cloud environments. Compliance is far more achievable when information and data are consolidated across one platform, giving a unified view across the enterprise of all systems and data, rather than deploying point solutions across the business that solve just one aspect of compliance.

It is also much easier now to consolidate storage, or to create a consolidated data management layer where the metadata or indexing of different data types enables information to be stored in different locations, yet retrievable from a single access point. This is a popular approach in compliance and surveillance.

How do you measure the success of implementing technology, and proving Return on Investment (ROI)?

ROI used to be oriented towards storage costs. However, the storage cost now is relatively small, so the return we're looking for today is risk reduction, which is achieved by a robust, auditable position when you are approached by a regulator or litigant.

When you can clearly demonstrate the policies and processes you have in place, show how you test whether they are being executed correctly or not, and how you remediate any gaps, you are most likely to avoid multi-million dollar enforcement actions. The smart approach is to have a centre of competence, which can respond quickly and knowledgeably to regulator enquiries.

Another significant saving is time. For far too long, financial institutions have left their business lines to figure out information governance on their own. With advances in technology – most notably "infrastructure as a service", process automation and artificial intelligence – there is no reason why they cannot be supported by a central compliance management platform that is faster, more consistent and reliable, and way more prescriptive.

The Trends

INFORMATION GOVERNANCE - THE TRENDS

What does the future look like?

#1

Information governance is expected to thrive as a shared utility.

A shared utility model for RegTech is emerging to help FIs lower costs and gain quicker access to the latest technology and developments. Rather than each FI managing its own solution, they can subscribe to shared utility services managed by third parties.

By identifying data synergies between global reporting regulations, enterprises can leverage centralised information governance platforms to promote data quality and operational efficiency. Where similar rules exist for different regulations (FMIA, MiFID II, EMIR, etc.), a rules engine can be built and subscribed to as a shared utility. Many asset managers and smaller intermediaries who lack the scale to invest in systems, may look toward new outsourcing service providers as a way to meet increasingly complex and pervasive compliance requirements.

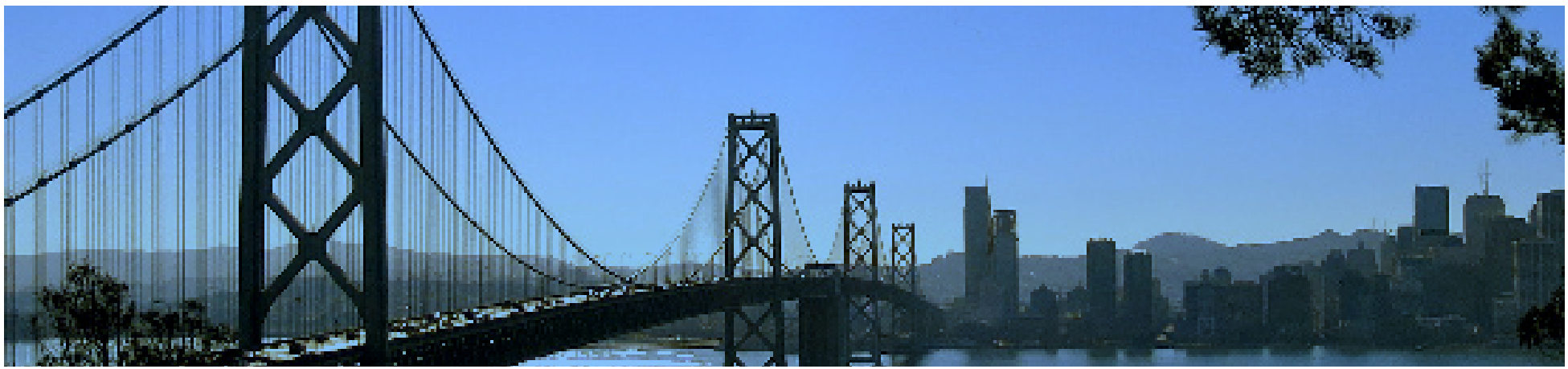
#2

Information governance will be comprehensive, pervasive and federated.

Next-gen information governance platforms promise to bring a common framework for managing records based on all types of content from revisable documents to scanned images to voice and video recordings, email, texts and comments on online forums. A common framework would ensure that the rules specifying records retention, security or other records management policies would be applied regardless of type and location of the document.

Secondly, the information governance platform will be pervasive across the enterprise touching content creators, business leaders and not just information and records administrators. Records management policies need to be expressed in rules that get applied automatically rather than allowing or expecting individuals to declare each content item as a record.

Finally, as cloud-based repositories grow in popularity, federated records management will continue to make more sense than the centralised approach in terms of relieving the burden of responsibility on end-users to move content from one repository to the other.



#3

Advanced technologies will drive the future of information governance.

While adding headcount has been the way to solve compliance challenges in the past, the rise of RegTech has provided an alternative route to streamline and optimise existing compliance departments to handle the increased workload. With innovative big data technologies, it is now possible to scale up the computing power for risk management in a cost-effective manner.

Artificial intelligence and cognitive analytics are enabling enterprises to automate analysis, classification and retention of structured and unstructured documents against different record-keeping regulations. OCR, coupled with NLP, is helping derive structured templates from unstructured records. The application of machine learning is helping firms understand the records' context and automatically assign applicable retention policies. Furthermore, it is possible to trace every record throughout the lifecycle, which is critical for meeting demands for data retention and data disposal requirements embedded in the data protection laws referenced previously in this report.

#4

API-based integrations will become essential for enterprise-wide information governance.

Financial services firms are increasing their transition to open API-based technology architectures that are conducive to integrating RegTech solutions to establish a comprehensive information governance practice.

RegTech solutions are increasingly getting designed to bring forth enterprise-wide information governance to banks by enabling data integration across all their legacy systems, data warehouses, front, middle and back office applications. A number of these applications are running on legacy systems like on-premise ERPs or mainframes. These legacy applications contain mission-critical data, like customer or transaction history repositories, which need to be classified and tagged for the information governance process. Cluttered and intertwined data sets can be unbundled and organised through Extract, Transfer and Load (ETL) technologies in an increasingly effective and all-pervasive way.

POINT OF VIEW

WHAT VALUE CAN REGTECH BRING TO INFORMATION GOVERNANCE?

Conversation with Ben Richmond
Founder and CEO, CUBE

What are the catalysts that have turned the industry's focus towards new technologies for information governance?

Digital transformation has brought countless benefits to financial services firms, however the result has been a significant increase in information and data being generated and ingested, all of which is governed by a regulatory universe that is growing exponentially. Faced with billions of individual rules, regulations, handbooks and citations to analyse and apply, Records Managers are finding that the labour-intensive manual processes they have relied on in the past to ensure compliance are neither reliable nor cost-effective at scale.

Heightened focus on data protection and privacy has triggered a complex intersection of records, data, privacy and security. Rather than simply managing where information assets are produced and maintained, defining retention rules and ensuring effective enforcement, records must now be managed at a far more granular level, with understanding of who owns each piece of data, how it must be protected, and what systems must be put in place to govern this. Regulatory technology (RegTech) is the only way forward, to ensure that the data within each record is protected in transit as well as at rest, and that retention policies are adhered to, given that disposal is now as important to the regulator as retention.

Which technologies are having the biggest impact on information governance?

Huge advances in Artificial Intelligence (AI) are enabling financial institutions to reduce compliance costs and minimise exposure to compliance risk.

Underpinned by AI, we are seeing many large financial institutions deploying holistic technology platforms that encompass regulatory intelligence, the governance of information assets, and automation of complex compliance processes. AI tools including Machine Learning (ML) and Natural Language Processing (NLP) can be used to track global regulatory change, across jurisdictions and in many different languages, and then identify which rules apply to specific information assets. As a result, financial institutions can automatically pinpoint, in real time, any compliance gaps in their policies and procedures, and then take effective remedial action.

Robotic process automation can also be used to extract machine-executable rules from regulatory data. Rules relating to information assets can be applied in a fully automated, end-to-end process. If, for example, you are required to retain trading information for six years, then destroy the information at the end of this period, the entire process can be automated.

What value, do you think, are financial institutions gaining from RegTechs today?

AI drives incredible business value for financial institutions, allowing far less time to be spent searching for regulatory intelligence and monitoring for change. Manually capturing data such as the format that each record must be stored in, how long it must be retained for, how it should be protected and made available,

and for how long, would be extremely time-consuming and labour-intensive. AI frees time to spend on the analysis and application of regulatory intelligence, which safeguards compliance.

Another key benefit is reputational risk mitigation. When financial institutions practice pro-active information and data governance, with a more joined-up information base, Chief Data Officers (CDOs) can demonstrate greater control over data and improve standards across the enterprise. In doing so, they are diminishing compliance risk and reducing the likelihood of costly fines, which avoids publicity surrounding enforcement breaches. In turn, this bolsters customer confidence and fosters more trusting relationships, which is always good for business.

Finally, AI allows risk assessments to be conducted more effectively. If you are looking to launch a product in a new jurisdiction, using AI you can quickly discover which records and data are relevant, what data needs to be created and maintained to meet regulatory requirements in the new jurisdiction, and the type of governance framework required.

It is no longer feasible for financial services firms to manage their information assets without the use of technology, especially when operating cross-border. As the regulatory environment continues to grow more complex, we will undoubtedly see RegTech become mission-critical in information governance.

USE CASES FOR ARTIFICIAL INTELLIGENCE IN INFORMATION GOVERNANCE

- Paragraphs from regulatory statements can be broken down into sentences, and then analysed by Machine Learning (ML) models that identify themes and recognise all information assets to which they relate.
- Once regulations are classified and aligned to information assets, these assets can be linked to regulatory fines and events, enabling customers to pinpoint risk exposure and define controls that must be put in place to mitigate risk.
- Business function owners (records management or data privacy, for example) must ensure that all policies and controls are mapped to relevant regulations. When applied to each policy, ML can suggest regulations that refer to the same topic and must be enforced. ML can be trained to look for a combination of terms, not only data privacy, for example, but all content that refers to both data privacy and an enforcement fine.
- When ML models look for a specific regulatory term such as 'KYC', they can be trained to apply a weighting to related terms like 'client/customer' or 'identification'; the weighting determines the ranking of results from a search.
- For horizon scanning, ML can be applied to identify upcoming regulations (not only formal published regulations) and filter out from the global mass only those that are relevant to a financial institution's specific jurisdictions and lines of business.
- The Financial Conduct Authority (FCA) handbook is vast. For a financial institution wanting to identify all elements and obligations that are relevant to information or data governance, Natural Language Processing can be used to locate relevant sentences, narrow the search and determine which sections of the Handbook the team should act on.

INFORMATION GOVERNANCE DATA FROM BURNMARK

Burnmark has data on 100+ regulations directly relevant to information governance in financial services, across the Americas, Europe, Asia and Australia - please reach out if you'd like to get the list!

info@burnmark.com

#	Regulation	Info	Geography	Year	Link
11	The FATF Recommendations	These are the internationally endorsed global standards against money laundering and terrorist financing. These require States, among other things, to implement relevant international conventions, criminalise money laundering and enable authorities to confiscate the proceeds of money laundering, implement customer due diligence, record keeping and suspicious transaction reporting requirements for financial institutions	Global	2017	http://www.fatf-gafi.org/publications/fatfrecommendations/?hf=10&b=0&s=desc(fatf_releasedate)
12	Digital Privacy Act	This amends the Personal Information Protection and Electronic Documents Act, most notably called Bill S-4 or the Digital Privacy Act	Canada	2015	https://laws-lois.justice.gc.ca/eng/annualstatutes/2015_32/page-1.html
13	The California Consumer Privacy Act	This is a bill passed by the state of California legislature and is officially called AB-375. The bill, in part, would grant a consumer the right to request a business to disclose the categories and specific pieces of personal information that it collects about the consumer, the categories of sources from which that information is collected, the business purposes for collecting or selling the information and the categories of third parties with which the information is shared	USA	2018	https://www.cmswire.com/customer-experience/what-is-the-california-consumer-privacy-act-of-2018-and-how-does-it-affect-marketers
14	MiFID II & MiFIR	This contains a number of provisions under which non-EU firms may provide investment services to EU-based clients.	UK	2018	https://www.globallegalinsights.com/practice-areas/banking-and-finance-laws-and-regulations/united-kingdom
15	Common Reporting (COREP) Financial Reporting (FINREP)	In the UK, all BIPRU firms including banks, building societies and investment firms will be required to report under COREP. All credit institutions applying IFRS (International Financial Reporting Standards) will report under FINREP.	UK	2014	https://www.accenture.com/t20150714T065457__w__/ae-/en/_acnmedia/Accenture/Conversion-Assets/DotCom/Documents/Global-PDF/Industries_3/Accenture-COREP-FINREP-Implementation
16	Fourth Money Laundering Directive	The Directive includes some fundamental changes to anti-money laundering procedures, including changes to CDD, a central register for beneficial owners and a focus on risk assessments	Europe	2017	https://vinciworks.com/blog/4th-money-laundering-directive-what-you-need-to-know
17	Personal Data Protection Act	The PDPA establishes a data protection law in Singapore that comprises rules governing the collection, use, disclosure and care of personal data. It recognises both the rights of individuals to protect their personal data, including rights of access and correction, and the needs of organisations to collect, use or disclose personal data for legitimate and reasonable purposes	Singapore	2012	https://www.pdpc.gov.sg/Legislation-and-Guidelines/Personal-Data-Protection-Act-Overview
18	Information Privacy Act	The Privacy Act 1988 (Privacy Act) regulates how personal information is handled such as common examples are an individual's name, signature, address, telephone number, date of birth, medical records, bank account details and commentary or opinion about a person	Australia	1988	https://www.oaic.gov.au/privacy-law/privacy-act
		This revised market risk framework will go live in 2019 and banks are expected to adhere by 2020, seeks to bring greater consist-			

Conclusion

Information governance is nothing new for financial institutions. Nor are the regulatory challenges associated with dealing with the complexities of information governance. The processes and baseline of information governance was set decades ago - however, we find ourselves in a unique period in regulatory compliance history where banks, insurance firms and large financial institutions are dealing with several multi-jurisdictional and global regulations at the same time; and dealing with enormous impact of careless behaviour and lack of action.

The hidden costs of not managing information governance effectively and ethically have also risen in an unprecedented way in the past couple of years.

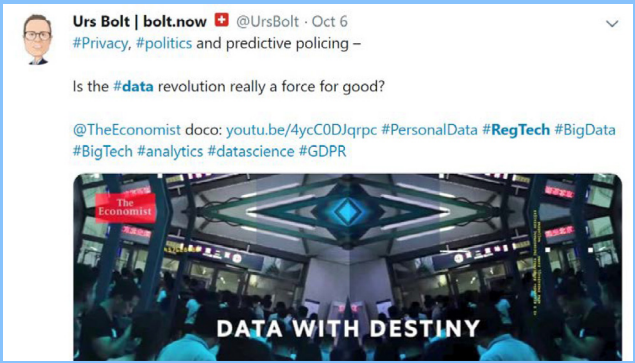
Technology is an answer to a lot of the problems caused by legacy and it's as good a solution as any to the enormous complexities faced by financial institutions around new regulations, increased focus on data privacy and security, as well as the uneven pace of geographic adoption of standards. Burnmark published a RegTech report earlier in 2018, dealing with some of the possibilities of regulatory technology in detail, and in this report, we look at the other side of the landscape - what kind of complexities exist around data management, information management and records management even when you keep technology completely out of the picture?

AI and blockchain, to a large extent, help find solutions to some of these problems quite effectively. Singular platforms dealing with all processes within information governance, with the capability to manage any types of rules and data, are hard to come by, and Burnmark has looked at CUBE's ambitions and capabilities to do just that, with a lot of interest.

At the end of the day, as we reiterated in our RegTech 2.0 report, it's not about a single solution to the problem. Or one RegTech provider that offers the perfect product. The change will happen when the ecosystem is built, and it starts to function effectively and collaboratively with all solutions available in the market. There is also a need to develop the skillset needed to manage the challenges of the digital world within banks and partner firms. The technology and resource stack that can effectively manage these complexities in a dynamic, future-proof manner will definitely win the world! And, of course, survive to see the future.

- Devie Mohan, Burnmark

ON TWITTER



CUBE @CUBEGlobal Aug 14

Interesting stats on how #FinancialServices firms manage regulatory #data. Top concern is keeping up to date with the pace of regulatory change (55.8%), followed by keeping compliant with changing #regulations & adhering to deadlines (54.0%) http://bit.ly/2w4gdu9 #RegTech

burnmark @burnmark_ Oct 25

The #RegTech sector powers on with nearly $9bn raised since 2014 via @Fintech_Global https://buff.ly/2RbdXua

burnmark @burnmark_ Oct 8

Great to see IRTA use its discussions in our #RegTech report to launch its open standard principles

https://buff.ly/2RA4Zrg

Lee Baker @BakerLJ May 16

#RegTech as a key driver of collaboration between banks and Fintechs - what's the abiding characteristic? Data! @devie_mohan of @burnmark_ at #MATech

CGOC @CGOC_Council Oct 31

Article 32 requires a strong information #governance (IG) foundation that enables organizations to identify where personal data exists and the risks associated with it: http://bit.ly/2IMqRvr #GDPR

DEFeND Project @DefendProject Oct 15

13 October 2018, #Milan: the DEFeND Project was introduced by The Observatory on Information Governance in Banks (@ABI_Lab Task Force on "Information Governance") to 100 bank industry experts.

Follow us on Twitter!
@burnmark_

This report has been published by Burnmark in association with CUBE.

CUBE leverages Artificial Intelligence (AI) to automatically capture all global financial services regulations, extract regulatory obligations and map them onto policies, procedures, controls, and records. CUBE highlights information assets that are at risk of non-compliance and enables timely remediation. Two million financial services staff are consuming regulatory intelligence across 180 countries, in 60 languages, powered by CUBE.

For any questions or comments, please write to
info@burnmark.com
contact@cube.global

December 2018 @burnmark_ @CUBEGlobal