JULY 2020

RISK CONTROL FOR A DIGITIZED FINANCIAL SECTOR

RegTech's illumination of IT and data blind spots

JWG
Making sense of financial services regulation

CLOUDERA

Contents

About the research

JWG Is a pioneering market intelligence company working with firms, technologists, and regulators since 2006 to help the industry comply with the ever-changing regulatory landscape.

This research report draws conclusions from JWG's February 2020 RegTech 2.0 conference with 250 market experts who discussed forthcoming challenges and defined strategies on how to get ahead of the curve. An expert panel on Infrastructure debated the impact of new technology on the risk footprint of the financial system and how well current policies help mitigate these risks under Chatham house rule.

We are grateful for the time and effort from over a dozen policy and operational experts from both private and public sectors who helped shape this final paper.

1. Executive Summary

An explosion of advanced computing capability facilitated by **Cloud technology** has provided massive benefits to both regulated financial institutions and their regulators. However, it has also introduced new **Systemic Technology Risks (STRs)** to the financial sector.

Rapidly scalable technology and data enable powerful new business and supervisory models at far lower cost and faster deployment cycles. This enables supervisors to get hold of and interpret the **vast quantity of information** they receive daily on the safety of the system.

Since the Great Financial Crisis (GFC) policy makers have extended prudential risk and conduct regimes to create a more **holistic and detailed view of the system.** Now more than ever, this data is needed to **fight the economic crises** of the 2020s.

However, powerful distributed technology does not come without idiosyncratic and systemic risks. **Core data sets** are slowly being **concentrated in the hands of a few providers** who do not own the risk of failure. **RegTech is required to digitise compliance** and control these new risks.

STRs reside off balance sheet and there is **no way to quantify them** – leaving the market with a large **blind spot.** While regulators have created discrete tick boxes for a firm's data and IT management help understand STRs, there is **no prescribed method of aggregating the risk factors.**

We believe risk measures like **'G' in Environmental, Social and Governance (ESG)** can be used to quantify RegTech risks and **create the incentives** for firms to invest in safer technology. The size of the prize is significant, and the **benefits already proven** in collaboration with regulators.

The introduction of these standards will not be easy. For this approach to succeed, the risk experts will need to engage with the SMEs to establish **standards for 'good RegTech'.** These disparate communities do not naturally sit together but can be incentivised to do so if the **regulators take the lead and convene the discussion.**

As evidenced by COVID-19 BCP plans, STRs are real, and have been **building for decades.** The industry needs **to move quickly** to gather the right stakeholders and **fast-track this discussion** in advance of the Great Infrastructure Crisis (GIC).

2. IT infrastructure and data risk mitigation today

Summary:

- How a firm manages **data is now intrinsic to its value** and linked to other actors
- **Risk aggregation** is heavily dependent on the **integrity of information produced**
- There are **inconsistent standards** to measure **computational integrity** of this data today
- **This is a big problem: the scale** of the Banking infrastructure is measured in USD trillions
- **IT obsolescence and data integrity** are top risks for the regulator and regulated

Technology has moved financial services from risk intermediation, to risk information processing, to risk information production and distribution. This means that **data by which risk is measured is itself a critical asset.** Unfortunately, there is no standard approach to managing data in the industry as data is shaped by bespoke operating models, technology platforms, accounting rules, business practices and other practices.

To account for risks reported by multiple firms, the system needs to be able to **trust the integrity of the environment in which it was produced.** This means the integrity of the prudential and conduct controls stipulated by regulators as well as the integrity of the computational infrastructure (i.e., the machines, networks and applications that produced it). Unfortunately, there is **no risk measure to encapsulate computational integrity** which we define as a financial institution's ability to correctly produce the granular information required by many different sets of regulatory obligations.

There are many standards to judge 'how' a firm manages its obligations, but nowhere do these come together to **value the firm's capabilities as a risk information provider.** A firm's ability to provide information to the market and the regulator will, in turn, be dependent on their trading partners and suppliers. This means that any one firm's **capabilities are linked to those that are close to them on the value chain** and that the regulator's view of these actors will need to be taken together to have a **view of that system.**

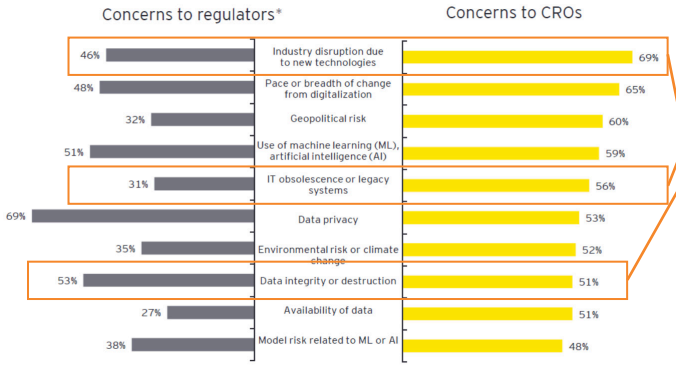
The Financial Services sector is **increasingly digital** and heavily reliant on technology. The European Expert Group on Regulatory Obstacles to Financial Innovation (ROFEIG) report estimates that the **total spend by the largest financial institutions globally is approximately $535 billion**, with approximately €192 billion of this spent in Europe. However, given that they put the number of licensed banks globally at 25,000, with another circa 60,000 'quasi' banks, they were right to conclude that "total spend on digital technology may be breath-takingly large" compared to the global annual expenditure on digital technology by the insurance sector which they put at $185 billion.

Legacy systems which contain institutional memory were paid for long ago, but they now carry a risk of not **being enterprise ready** in a digital world. A survey by the Bank of England in January 2020 revealed that the top 30 banks they supervise have over 1,500 applications in the cloud. The Future of Finance report concluded that "up to a quarter of the activities of largest global banks may already be on the public cloud or software hosted on the cloud." Looking forward the report concurred with a McKinsey & Company conclusion that up to 40%–90% of banks' workloads globally could be hosted on public cloud or software as a service in a decade.

Across the globe, regulators have established new Data Strategies like that in the UK which sets targets to become a **data-driven regulator.** Advanced data **analytics, simulations and predictive models** will deepen regulatory understanding of markets and consumers while Firms automatically supply data through digital regulatory reporting.

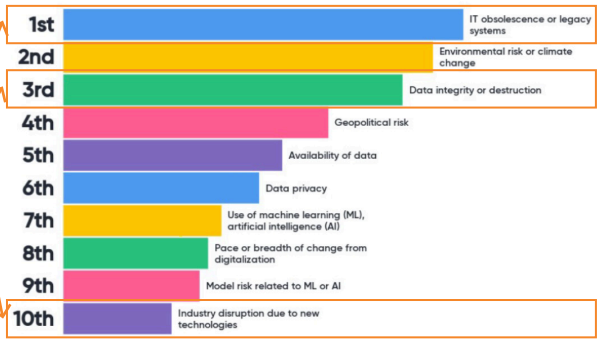
This means that as we collect more, granular information at high volume and lower costs, Financial Services is taking on ever increasing levels of risk. This fact has not escaped senior risk managers who **see IT obsolescence, legacy systems** and **data integrity** among the **top risks** over the next 5 years as revealed in a joint EY and JWG survey in as shown in Exhibit 1.

Emerging risks over the next five years
Industry vs regulator perspective



* CROs' views of regulators' concerns
Source: Tenth annual EY/IIF global bank risk management survey

Top 3 risks for regulators, compliance, operations and technology



Source: JWG RegTech 2.0 survey, Feb 2020, 64 respondents

Exhibit 1: 2020-2025 emerging risk rankings

Regulators have also recognised this year that that **no systemically important bank is fully compliant with the principles of risk data aggregation established in 2013**, according to the 2019 BCBS 239 assessment. This downgrade from the 2017 report cites **changes in cloud technologies**, which have affected banks' rate of progress "by **increasing complexities** and presenting other **business and technical challenges.**" Not least amongst these complexities is that businesses are now able to bypass IT and data policies within the bank and set up their own fiefdoms which then compete with the rest of the bank's infrastructure.

RegTech is required to **digitise compliance and reduce the levels of technology and data risk.**

3. Shining light on the blind spot

Summary:

- **Pre crisis analogue regulations** have become **data-centric** since the GFC
- **New regulations for technology and data** have been introduced since the GFC
- These standards are being used to **test firms' response to today's economic crises**
- However, a **large amount of risk remains off balance sheet** and cannot be evaluated
- The sector needs to **move quickly** to address **Systemic Technology Risks** (STRs)

A new regulatory demand for data in pre-GFC rules

Today's prudential and conduct oversight is built on four regulatory principles: Liquidity, Efficiency, Transparency, and Consumer Protection. We have **many standards for 'what good risk information looks like' for these analogue regulatory regimes** that were defined before the GFC.

As JWG 2019 analysis showed[1], the **regulatory perimeter has expanded in both breadth and depth since** the GFC. The **'how' is becoming as important as the 'what'** and the 'ad-hoc' requests are becoming more frequent. In sum, regulations are becoming more data centric and demanding transparency. Policy has shifted from a narrow focus on single data points on counterparties, algorithms, traders, to **a more contextual and holistic view of the whole system.**

As noted in the previous section, this has led regulators such as CFTC Commissioner Giancarlo to state: "The right path, indeed, the only path is to **combine robust data collection, automated data analysis and state-of-the-art artificial intelligence capability** to transform the CFTC into a highly effective, big data math shop – what I call a **"Quantitative Regulator."**

Post GFC infrastructure rules

Alongside this thirst for better information on the system, regulators have introduced **new rules** since the global financial crisis which raise the **standard of care for technology and data.** These controls include:

- **Data:** Privacy/ Encryption / data quality / data anonymity/ PET/ DRR
- **Processing:** Machine readable/ Machine Learning/Artificial Intelligence/ Blockchain
- **Sharing:** Identity/ API's / data exchange with the market/ regulator/ Interoperability
- **Dependencies:** 3rd party risk management / Cloud / Platform Design
- **Risk practices:** Operational resilience plans/ KRIs/ governance/ tests

Each of these obligations has defined risks in the infrastructure and put in place **new control frameworks** to manage them.

The fashionable new risk question of late is how we **identify concentration risks** like cloud in the technology supply chain. Driven by political scrutiny of recent system failures, The Bank of England, FCA and PRA issued a consultation to Building operational resilience: Impact tolerances for important business services. It proposes an outsourcing register and **tick list of**

[1]Ready for Digital Regulation? Rethinking your approach to enterprise data management for capital markets in the new age of quantitative regulation, JWG March 2019

obligations to have in suppliers' contracts which could even be validated by third parties and the subject of audits organised by groups of firms sharing service providers. Though still in consultation, some SMEs note that it is already part of the dialogue with firms about how well they are managing their infrastructure.

UK policies are broadly aligned with **Europe's** which introduced ICT & Security risk management guidelines last year which require IT strategies to be documented and risk inventories to be created with independent oversight functions. New EBA Guidelines on outsourcing create a common framework for all financial institutions to remain responsible for their supply chains at all times. Critically, they ask the **Competent Authorities to monitor risk concentrations on individual service providers** and identifying whether they pose a risk to the financial system.

On cue, ESMA noted in March 2020 that it considers Credit Rating Agency outsourcing to cloud service providers is a risk that is not yet managing appropriately. In June, France and Germany established the GAIA-X cloud non-profit which aims to ensure member companies abide by its goals of data sovereignty, data availability, interoperability, portability, transparency and fair participation. An ominous sign of things to come.

Off-balance sheet systemic technology risks

One of the key conclusions from an expert RegTech group which JWG convened in February 2020[2] was that **a large amount of risk is off balance sheet today and cannot be evaluated.** At the level of a single firm this is the underlying risk of legacy systems which have been long paid for but now carry a risk of not being enterprise ready. To put these idiosyncratic risks in a systemic perspective, if the sector has 220 Billion lines of code at $10 per line of code this would be the equivalent of 20% of tier 1 and tier 2 capital of all global banks.

Whether or not one agrees with this method of quantifying the risk, the **cost and complexity of overhauling** a firm's infrastructure is high in terms of actual spend and disruption. Thus, banks (and regulators) have historically put **minimal funds into rebuilding systems**, opting to patch old technologies and graft on new ones creating what some describe as 'spaghetti junction'. Eliminating known risk like those inherent in remaining on COBOL **could take decades**.

One panellist noted, "Even with great RegTech we run the risk of 'garbage in, gospel out' - we need to move out of rabbit holes and think big about concepts like ultimate beneficial ownership data." SMEs called on policy leaders to **recognize the pace and scale of the change and move quickly to address risks inherent in both the astronomical deployment of new technology, and the failure to address systemic technology risks (STRs).**

One key area of attention was **data policy**. Although standards on risk data aggregation (BCBS 239) and risk models (ECB's TRIM) have been introduced, they do not provide a mechanism to understand the risk profile of a firm, or a system's data. One panellist noted "Capital has convexity, but data has no convexity which means it has a 'jump to default risk' which should be insurable."

As banks have shared stakeholder responsibility to provide embedded cost of service to support regulatory requirements. This means they are **tying up regulatory capital** and cannot deal with important issues like serving the unbanked. This also creates an **uneven playing field** and gives an uncompetitive advantage to new FinTech entrants when they are not required to maintain similar capital levels.

In summary, the risk of data and the infrastructure which supports it is now too large to remain off-balance sheet. In volatile markets like we have seen in 2020, the rapidity of market prices going against positions crystallises the risk of data as an absolute risk.

[2]RegTech 2.0 conference Winning in the decade ahead

4. A path towards a safe, digitized financial system

Summary:

- RegTech standards can **provide measures for idiosyncratic and systemic technical risks**
- 88% already feel **RegTech should be a component** of their firm's **ESG** risk assessment
- **New RegTech standards** can be developed to satisfy ESG and SM&CR obligations
- Implemented correctly, a **new incentive system can spark innovation** across the sector
- This innovation will dramatically **lower the cost structure** and enhance **safety**
- **Examples** of real RegTech shifts have already been **proven and validated** by regulators

RegTech measures

"RegTech" became a hot topic with Financial Services regulators five years ago, to describe the **adoption of technology innovation** that can help **achieve the complex and challenging policy objectives set for the regulators and regulated.**

It is focused on enabling compliance processes to be better, either through digitising existing processes, (e.g. producing regulatory reports), or the redefinition of how the controls are applied. As described in a recent report from Fujitsu "a common suite of metrics needs to be developed that tie the performance of individual initiatives to long-term strategic aims of firms and the Financial Sector thereby making it **possible for a RegTech firm to tangibly demonstrate the value they bring.**

We believe that we can take this value argument further. By defining **"Good RegTech standards"** not only will the RegTech firms be able to prove themselves, but financial institutions and regulators can measure the quality of a firm's operational governance. In other words, **the 'G' of ESG** can become a measure of a firm's IT and data estate for compliance purposes.

This would mean that the firm's internal governance can be proven, and the market can rely on it. From an internal perspective senior management can evidence that they are **upholding their SM&CR obligations**.

For the market and the regulators, RegTech standards can **provide measures for idiosyncratic and systemic technical risks**. Exhibit 2 illustrates the impact that the introduction of these standards could have.

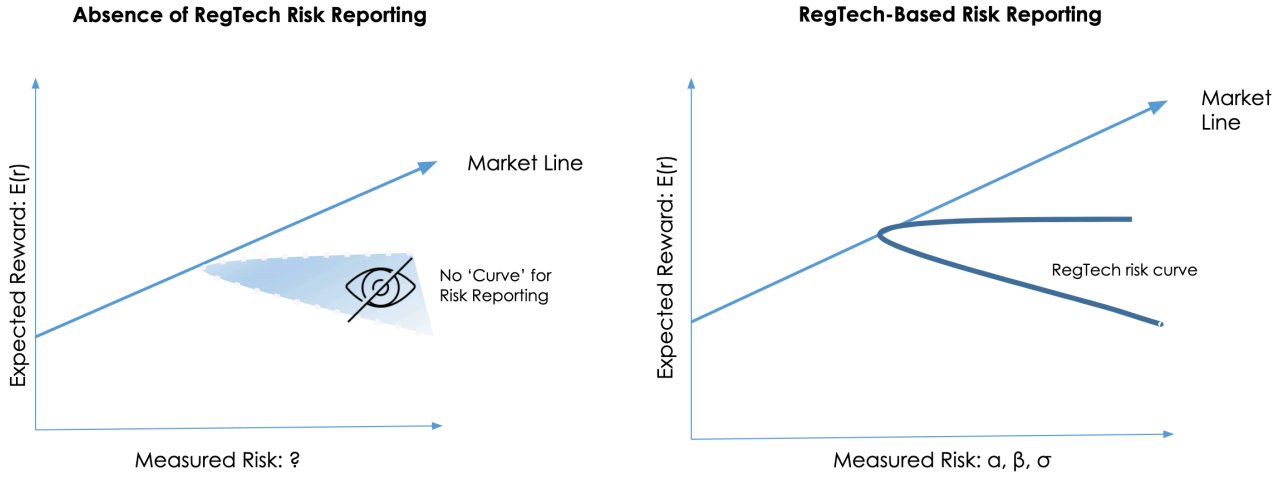


Exhibit 2: Defined vs. undefined infrastructure risk

Currently, market analysts and regulators are effectively guessing about the enterprise risk carried by the quality of the data and infrastructure as the **value of the enterprise is indeterminate** without a formal mechanism to evaluate the enterprise risks of the infrastructure and data.

Were market analysts or regulators able to capture a defined RegTech-based risk reporting measure, **standard risk management practices could be deployed** like excess return (α - alpha), correlated return (β - beta), mean variance of return (σ -sigma) could be applied. This would serve to **improve governance** and improve the **cost of capital** as per ESG mandates.

Though we have not yet defined RegTech standards, **the market believes** in them. As shown in Exhibit 3, **88% of respondents at JWG's 2020 RegTech conference felt that RegTech is a component of their firm's ESG** or SM&CR model. Three quarters of those which agreed with the assertion were in support of RegTech becoming a part of their CCAR Stress Tests. An overwhelming endorsement in the fact that the risk equation can be improved through RegTech measures.

Should ESG or SM&CR control frameworks incorporate RegTech quality?

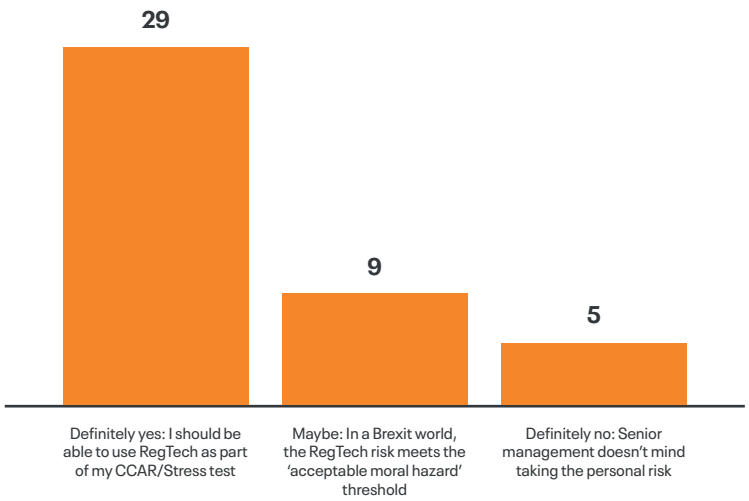


Exhibit 3: Where does Infrastructure and data risk belong?

Source: JWG RegTech 2.0 survey, Feb 2020, 38 respondents; asked to pick one answer to the question 'Is quality RegTech a component for my firm's governance equation (e.g., under ESG or SM&CR)?'

The great news is that **ESG regulation could already have established a mechanism to consider RegTech**. Under IFR the "K-Factor Requirement" defines a ration of the value of deferrable expenses to the value of estimated gross profits. This measure of externality costs relative to expected return could provide a basis for rewarding the reduction of RegTech risk.

Tech expense (e. g. legacy system amortization beyond useful life like COBOL) is an example. To the extent the K ratio grows it begins to affect K (capital adequacy) as the duration of expected value against deferred costs diminishes.

The recognition of this kind of risk control framework could have exciting consequences. For example, were **market analysts able to see the results** and amortize the risk to get DVAR on a daily basis, firms should be able to **get capital relief** for moving code into a trusted environment which produces more accurate and timely results.

In Europe, the EBA and ESMA have been asked to assess whether any ESG risk should be considered for an investment firm's internal governance and included in the **supervisory review** and evaluation process **by June 26, 2024**[3].

[3]EU Environmental Social Governance (ESG) Regulations Guide, Barrie Ingman, FactSet, April 2020

Establishing the governance

Defining standards for the many facets of RegTech will not be a straightforward exercise and cannot simply be handed over to academia or a consultancy. As described earlier in this paper, there is a broad patchwork of pre GFC regulation and a deep thirst for new data required to deal with current economic crises.

SMEs will need to **engage in a 'safe space'** which facilitates the constructive dialogue about the current challenges and how RegTech and SupTech standards can mitigate them.

A new **engagement model** and **plan** is required, with transparent **governance** to ensure appropriate checks and balances are applied to avoid conflicts of interest. The problem is **global**, but the solution may well need to **allow for jurisdictional differences**.

This may seem like a big ask, but it is one we feel the **industry is ready** for. After a decade of coming together to manage regulatory reporting, cyber risks, operational resilience, and the plethora of initiatives, we believe that **with regulatory engagement, the industry is ready to take a more proactive approach.**

Regulatory groups like GFIN and the FinTech Hub can help obtain consensus from the public sector while groups like the **RegTech Council can be engaged to support the public and private sector dialogue.**

The size of the prize

Our inability to account for systemic technology risk **stifles the incentives today** to move away from legacy code and to new technology with higher safety standards. This means that the prize from getting to a better control framework for a digitized financial system is worth **hundreds of billions** of annual spend on **IT which could be harnessed to make the system safer, at dramatically lower cost** if the industry had financial incentives to move to better technical platforms.

The definition of RegTech standards will have **benefits far beyond the mitigation of unchecked data and infrastructure risks**. For example, were each firm to be incentivised to hold and treat ultimate beneficial ownership information in better, more effective ways that are also shared with supervisors, this would **enable data vendors and RegTech firms to invest in new infrastructure**. This would reduce the cost each firm carries to manage that data today and provide incentives for third party investment in new cloud-based infrastructure which enables sharing and fuzzy matching of quality reference information. Though this kind of use case might sound far-fetched it is in fact precisely the reason project Citadel was awarded the top prize at the FCA's global AML and Financial Crime TechSprint in 2019.

Far from being a lone example, RegTech efforts in Machine Readable and Executable Reporting and Market Surveillance have also been **proven and validated by regulators**.

5. Getting ahead of the Great Infrastructure Crisis

Summary:

- Economic crises will accelerate demand for for **idiosyncratic and systemic risk measurement**
- **Discussion and consensus** on the use of the ESG framework is required
- A 5-10-year **implementation plan** is required to get to where the puck is going to be

The challenges in this paper were discussed at a conference which took place a full month before Italy went into lockdown and the implications of COVID-19 were not yet clear.

Since the conference, economic conditions have **shown that now more than ever, the sector needs a coherent way to measure idiosyncratic and systemic risk of the infrastructure**. The ESG framework suggested in this paper is an excellent starting point, but there is much more **discussion and debate required** to achieve **consensus** on the way forward.

These data and technology challenges are **neither new nor easy to solve**. Taking the UK as an example, it has been six years since concern over the safety of the financial infrastructure reached public consciousness and at the forthcoming policy statement addressing the matter.

The number of **infrastructure issues are becoming more prevalent**. According to Thomson Reuters, in the 12-month period between October 1, 2018 and September 30, 2019, UK banks reported 455 operational and security incidents for personal and business current accounts to the Financial Conduct Authority (FCA). Service outages, ransomware attacks and other technical problems have plagued high-street banks and irritated their customers which, in turn have raised political pressure for something to be done. The new **Operational Resilience regime is a step in the right direction**, but only a small one.

The scale and complexity of the technical challenges discussed in this paper will require many firms and many regulators to step-up quickly. Risk professionals will need to take a view on the **suitability of ESG as a framework** to control RegTech infrastructure risk. Massive rule books will need to be revisited and **new standards agreed**. Ultimately, the **implementation strategy** will need to be thought through in what is likely to be **5-10-year horizon**. Many legacy infrastructure that are hard to change, and even harder to test when changes are made.

All this means that **collaboration between public and private sector** is required. We need to frame this debate, engage the key stakeholders and define a path for action **quickly** as we engage with economic crises this decade.

As one regulator encouraged us throughout our conference, for the FS sector to **get ahead of RegTech infrastructure risks** we need to act like the famous hockey player, Wayne Gretzky who advised: "Skate to where the puck is going, not where it has been."

[4]Rachel Wolcott, Thomson Reuters Regulatory Intelligence, After six years from problem to policy statement, will 2020 start the operational resilience decade?, January 2020

6. Recap (#ICYMI)

Risk control for a digitized financial sector: RegTech's illumination of IT and data blind spots

CHAPTER	PITHY SUMMARY
2. IT infrastructure and data risk mitigation today	• How a firm manages **data is now intrinsic to its value** and linked to other actors • **Risk aggregation** is heavily dependent on the **integrity of information produced** • There are **inconsistent standards** to measure **computational integrity** of this data today • **This is a big problem - the scale** of the Banking infrastructure is measured in USD trillions • **IT obsolescence and data integrity** are top risks for the regulator and regulated
3. Shining light on the blind spot	• Pre crisis **analogue regulations** have **become data-centric** since the GFC • **New regulations for technology and data** have been introduced since the GFC • These standards are being used to **test firms' response to today's crises** • However, **a large amount of risk remains off balance sheet** and cannot be evaluated • The sector needs to **move quickly** to address **Systemic Technology Risks** (STRs)
4. A path towards a safe, digitized financial system	• RegTech standards can **provide measures for idiosyncratic and systemic technical risks** • 88% already feel **RegTech should be a component** of their firm's **ESG** risk assessment • **New RegTech standards** can be developed to satisfy ESG and SM&CR obligations • Implemented correctly, **a new incentive system can spark innovation** across the sector • This innovation will dramatically **lower the cost structure** and **enhance safety** • **Examples** of real RegTech shifts have already been **proven and validated** by regulators
5. Getting ahead of the Great Infrastructure Crisis	• Economic crises this decade will accelerate demand for **idiosyncratic and systemic risk measurement** • **Discussion and consensus** on the use of the ESG framework is required • A **5-10-year implementation plan** is required to get to where the puck is going to be