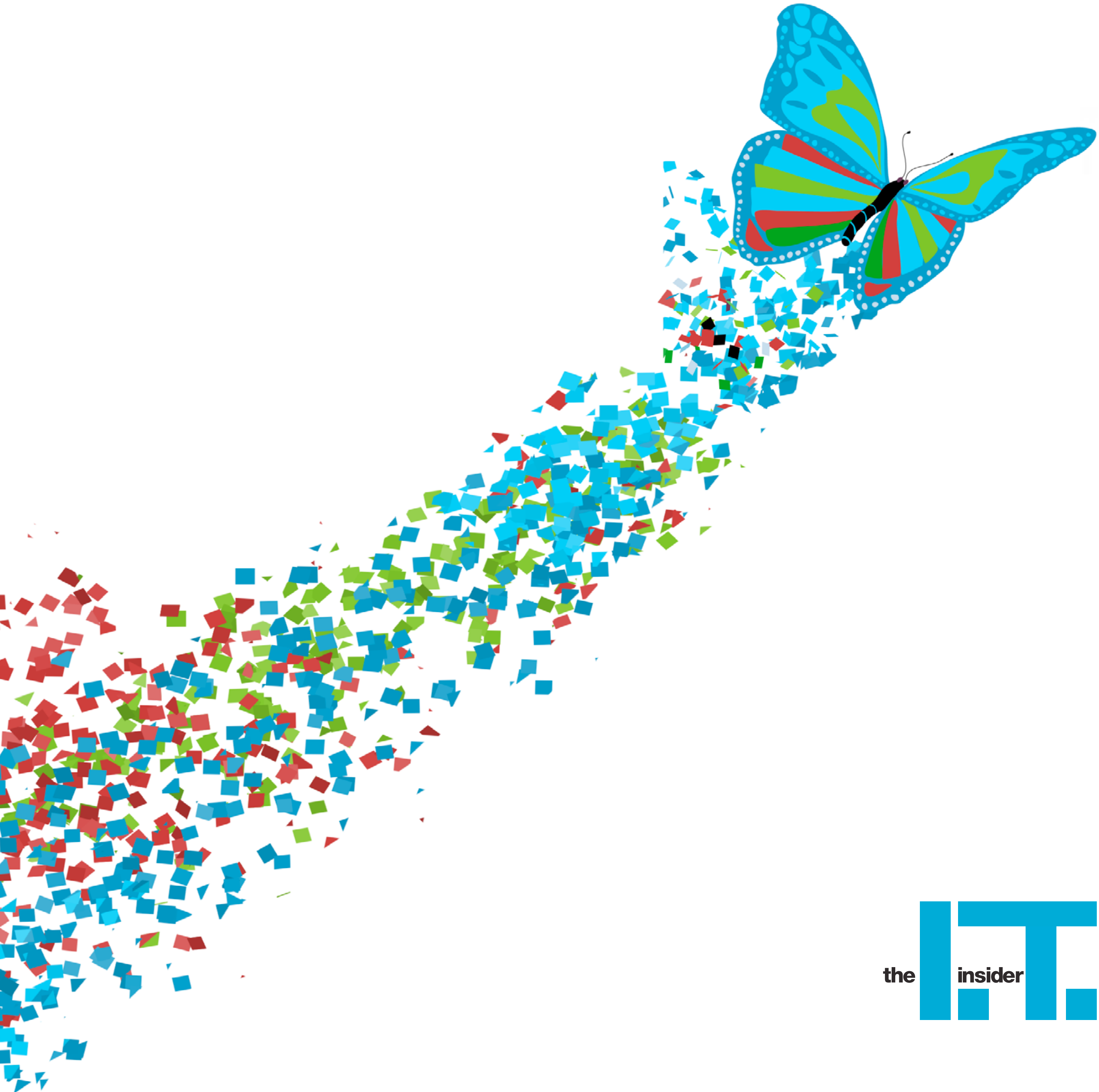
Digital Transformation in the Financial Services Sector

Turning data from challenge to opportunity



the insider I.T.

Contents

Introduction

There's no ignoring the fact that we now live and work in a digital world, where virtual trumps physical and data is king. This is particularly true when it comes to the financial services sector.

With the majority of both businesses and consumers now managing their finances online – from banking, to insurance, pension and shareholdings – **the physical distance between financial service organisations and their customers is greater than ever.**

As a result, customer service has become a deciding factor in the choices we all make. It's easier than ever to explore, compare and access different service providers, and with their triumphs and failures clearly visible, the margin for error is shrinking all the time. The need to understand our customers and provide a personalised service is essential to gaining and retaining their loyalty.

Yet a February 2017 survey by The IT Insider amongst business leaders in the financial services sector found that **only 22% of organisations are confident that they have complete visibility across their data sources**.

Our research also found that **40% of business leaders are concerned about the impact of digital disruption,** with start-ups making significant headway within the financial services sector. Their ability to deliver highly-targeted applications – often more effectively and less expensively than traditional companies – means they are quickly entering the mainstream. Across online lending, money transfer, banking, insurance and credit ratings, these digital innovators are breaking the dominance of established players, giving them no choice but to sit up and take notice.

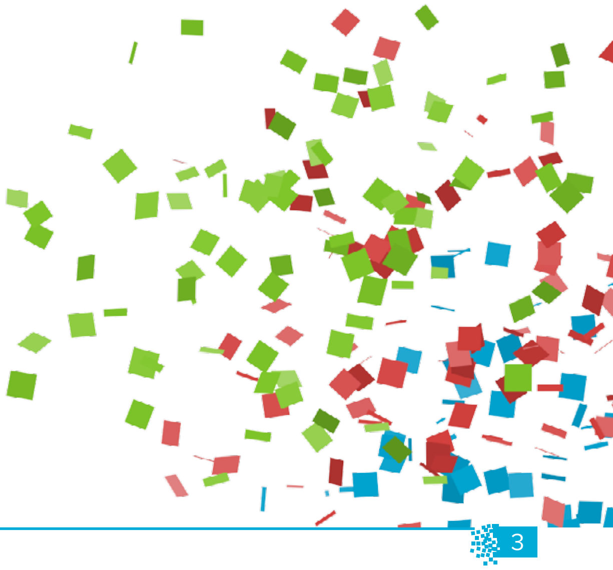
At a time when Financial Services organisations are facing unprecedented levels of public and regulatory scrutiny, growing data volumes and increasingly stringent rules around data protection can prove a major challenge. The IT Insider survey suggests that organisations have a long way to go in addressing these issues, with **only 28% feeling confident that they can comply with the new General Data Protection Regulation (GDPR),** and only 29% having a satisfactory solution in place to help combat fraud effectively.

'Big data' can be viewed as a major opportunity or a huge threat, depending on who you're talking to, so the pressure to unlock business value without causing business risk is on the rise.

There are a number of simple solutions that could help you to transform your business processes – staying competitive in this digital, data-driven age.

Bringing together in-depth insight and real-world examples from a number of specialists within the financial services sector, this White Paper explores how you can:

1. **Tackle digital disruption – driving deeper customer engagement and innovating to stay competitive:**
   - Bridge the gap between the data you have and the information you need
   - Plan to succeed, with a single version of the truth
2. **Create value for shareholders by focusing on areas that offer profitable growth at low cost and risk:**
   - Take an integrated, hybrid approach to transforming legacy applications and undertaking new, digital-led initiatives
   - Secure your digital transformation with a cloud-based approach to data backup and recovery
3. **Meet risk and regulatory compliance challenges head on:**
   - Combat fraudulent activity, taking a proactive approach to managing data and risk



1. Tackling digital transformation with data management

The finance sector has undoubtedly been revolutionised by digital transformation. When was the last time you went to your local bank branch to ‘check your balance’ or sent a cheque through the post as a means of payment?

Because of this focus on making the customer’s life easier, the financial services sector has a pressing need for robust data management. Organisations often have a long-standing history of mergers, de-mergers and acquisitions, meaning that their systems are complex, with large volumes of disparate customer and product data.

It’s therefore no surprise that those behind the management of financial services data have been at the forefront of data management best practice for many years – particularly due to additional drivers such as regulatory compliance and risk management.

Complying with the requirements of Basel III regulations, as well as the data protection requirements of the new GDPR legislation would represent major data management challenges for any business (see Section 3: Meet risk and regulatory compliance challenges head on). However, these initiatives are just a small wave in the huge tide of digital transformation facing the financial services sector, as technology continues to have a major impact on the way that organisations and their customers do business.

A common theme amongst all organisations in the financial sector is the size and complexity of the challenge that digital transformation represents. Whilst data is undoubtedly a critical asset for any organisation that wants to compete effectively in today’s digital world, this is particularly the case for financial services companies, where business is built on a continuous stream of transactions – each of which adds yet another row to the industry’s immense and growing ocean of data. Never before has so much data been held in so many formats and across so many devices and platforms, so harvesting and leveraging this information to gain a competitive advantage is no easy task.

In a global business environment characterised by volatility, uncertainty and risk, decision making needs to be both fast and well informed. Organisations need to be able to react quickly to unforeseen events and seize opportunities as soon as they present themselves, since competitive advantage is often short-lived. However, with financial and operational risk a rising concern in today’s fast-paced digital world, business leaders also need to be circumspect. They need to look to the future, the past, and inside and outside their organisations for answers to important questions. They need to utilise both internal and external data sources and construct forward-looking scenarios with all the foresight that human and machine can deliver – assessing both the risks and rewards that lie ahead, dependent on the strategies and actions that are taken.

Key Data Management Challenges in the Financial Services Sector:

□ **Meet growing customer demand for digital services**

□ **Comply with data protection legislation and industry regulations**

□ **Gain a 360° view of customers to stay ahead of the competition**

□ **Undertake effective financial planning and budgeting in support of business growth**

□ **Mitigate business risk through secure access and analysis of 3rd party data**

□ **Enable and support real-time decision making through predictive analytics and BI**

Crossing the Data Delta

The obvious answer is to invest in data analytics and business intelligence (BI) solutions, but whilst the IT industry has been running this type of data project in various guises for many years, the rate of failure to deliver on the promised business benefits has been unacceptably high. Implementation programmes that have been devised by IT teams are often doomed to failure, as the rest of the business simply disengages from the project, which often drags on over many years.

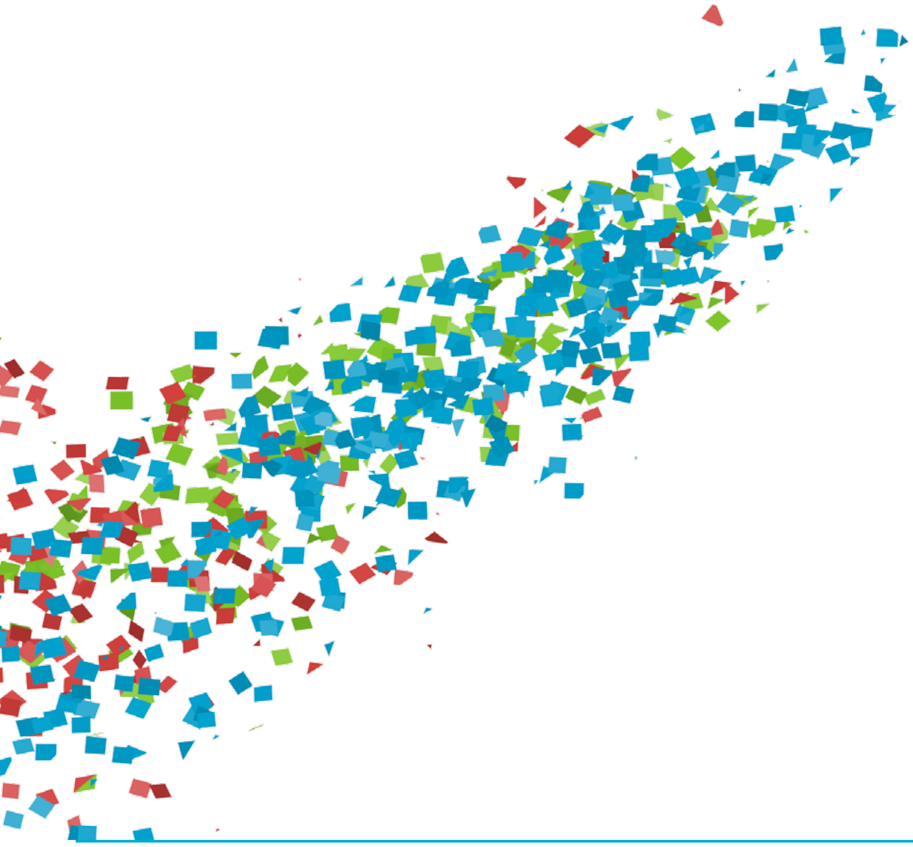
Once implemented, lack of confidence amongst senior executives in the figures they're presented with is also a major stumbling block, but rather than blaming the tools or the individuals that are running the reports, the problem lies in the data itself. **By trying to get by with incomplete or poor quality data when running data analytics, organisations are at risk of wasting a lot of time, effort and money.**

Data and information are different things and to unlock the value of data, it needs to be:

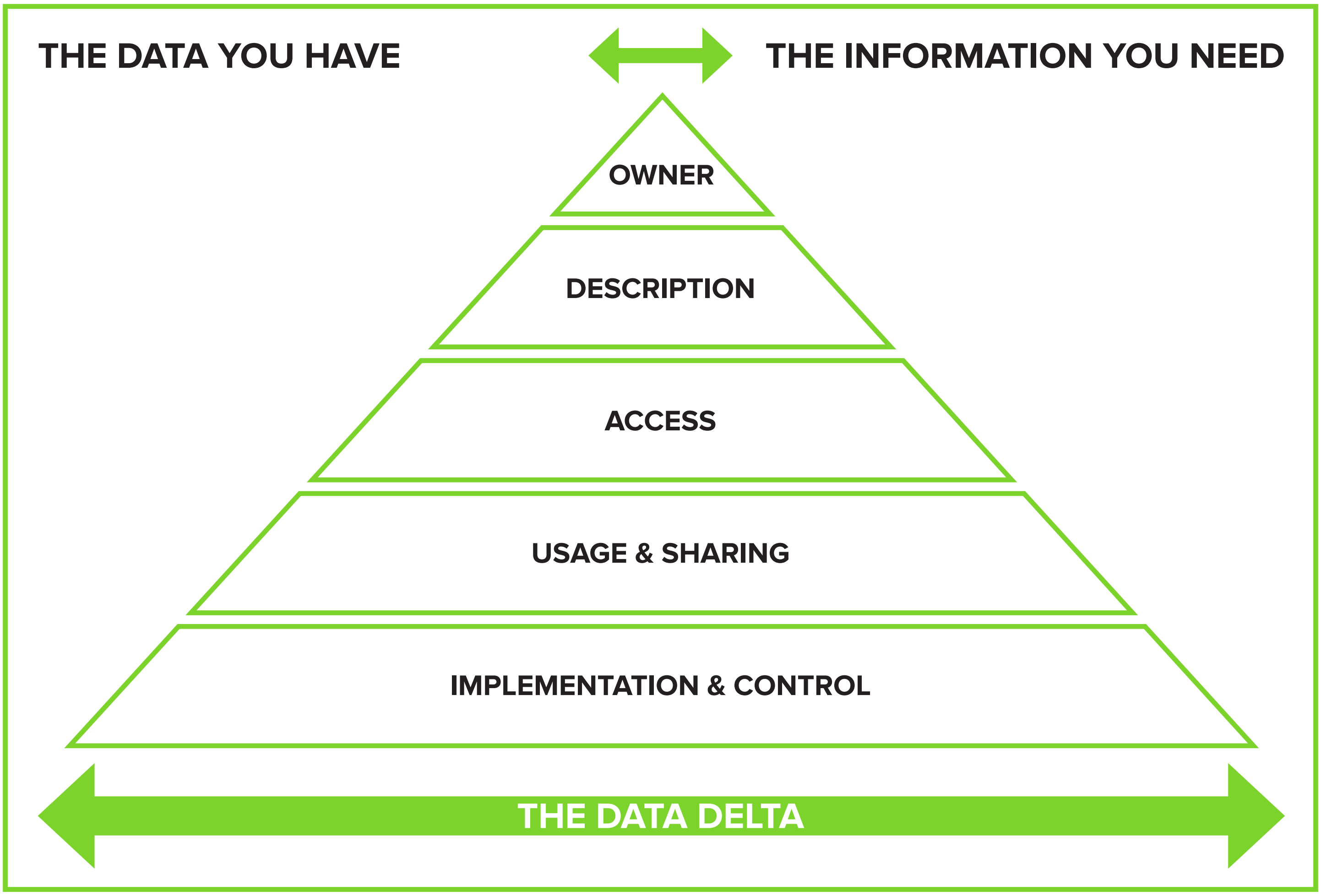
- **Properly defined: so that you know what you've got and where it lives**
- **Complete: ensuring that you can make accurate decisions and assumptions**
- **Sufficiently accurate/up-to-date: quality-controlled and if not 'real-time', at least not 'out-of-date'**
- **Meaningful: know the origin and context of the data**
- **Available: when it's needed, by those who need it and in a suitable format**

If your data doesn't meet those criteria, no matter who is undertaking the analysis and what tools they are using, they will never be able to produce the information that's needed.

In their recently published book – 'Crossing the Data Delta' – digital transformation experts, Entity Group, explained the process that they have developed for ensuring the data management, roadmaps and governance needed to avoid this pitfall – saving you a significant amount of time and cost. Address the underlying data issues before you invest in BI or data analytic solutions, and you will avoid the possibility of being presented with information that still doesn't add up – despite being more readily available and nicer to look at!



Data strategy and governance



1 Ownership

Determine who owns which pieces of data at the various levels within your organisation? Who in the management chain is accountable and who is responsible for taking action?

2 Description

To maximise data value, you need to gain clarity over what it actually is – describing it in a manner that's standardised and simplified. This will facilitate sharing and collaboration across the organisation to prevent duplicating data and 're-inventing the wheel', whilst also helping you to identify more easily what you're missing. It will ensure that future changes to data values can happen in a timely and straightforward manner.

3 Quality

Once data is properly described, it becomes possible to measure its quality more objectively – using different standards and targets for different classes of data, based on its importance to the business.

4 Access

Be sure to allow authorised people to access data securely and with the correct level of control and audit. You also need to adequately protect the privacy of the individual whose information is being accessed or shared.

5 Usage and Sharing

Reduce data complexity, ensuring that you only capture data that is necessary, reasonable and proportionate for your needs. This will make it easier to share data both within your organisation and with external parties, whilst ensuring compliance with data protection legislation.

6 Implementation and Control

If you have followed the first 5 principles correctly, this part of the process should be considerably more straightforward and carry a much greater chance of success. Attempt to address this stage in isolation by simply purchasing a BI or analytics solution and the ROI will be minimal.

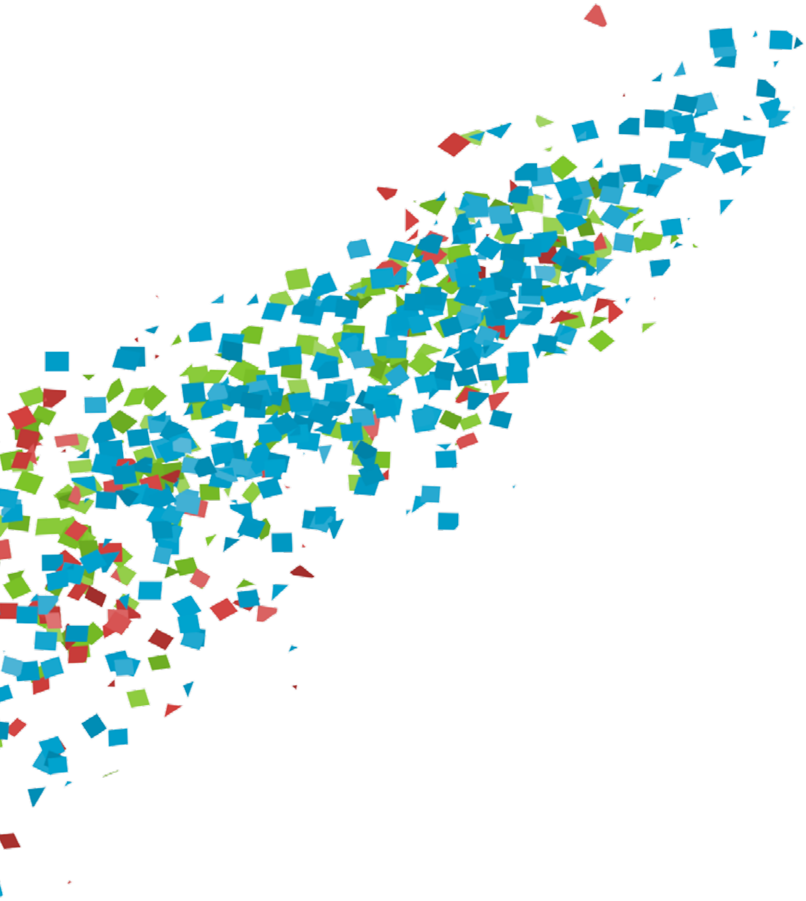
Unlocking your data value

The reality is that most finance teams still spend too much time in manual, spreadsheet-based processes – collecting, consolidating and validating data before they can even begin to analyse it. Because of that, finance professionals are often too slow in delivering the plans, budgets, forecasts, reports and value-added analysis that management requires.

So, how can you get from where you are now to where you need to be?

Industry research indicates that although the financial sector has a strong core of analytics capabilities – designed to address structured data, such as basic queries, predictive modelling and optimisation - it lags behind other industries when it comes to tackling unstructured data sets and taking advantage of advanced visualisation capabilities. With ‘big data’ sets too large for business or financial analysts to view through traditional reporting and mining tools, a different approach and more powerful analytics engine is needed if you want to gain the speed, agility and foresight needed to anticipate and react to changing market conditions.

- □ **Go beyond automating your planning, budgeting and forecasting** – embedding self-service analytics into everyday decision making to ensure that operational tactics and financial plans are inextricably linked.
- □ **Blend planning with predictive analytics** to enable deeper analysis and calculations to support the most challenging scenario and profitability-based decision making.
- □ **Include intuitive, natural language searching** to enable faster analysis and more accurate reporting across big data sets.
- □ **Ensure choice and flexibility** for business users with spreadsheet, web and mobile interfaces.
- □ **Enable visualisation capabilities** that will help users communicate and share their insights more quickly and effectively – highlighting what’s important with clear and compelling graphics.



2. Taking a hybrid approach to digital transformation

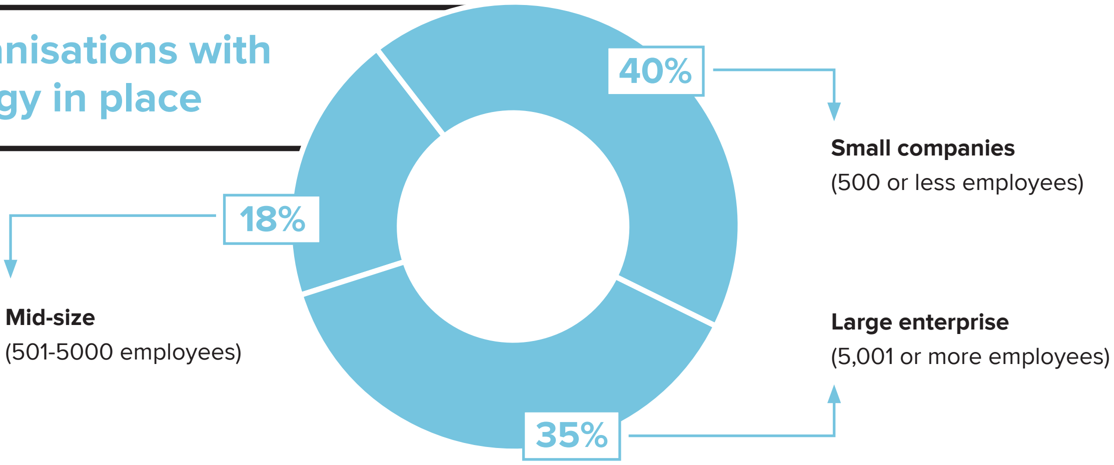
In this era of rapid digital transformation, where big data analytics, cloud and mobile rule the roost, there's no room for complacency. Fail to move with the times and invest in the emerging technologies that can enable business innovation and the competition will leave you behind – taking your customers with them. Move too quickly and without adequate strategic planning and you risk wasting a significant amount of time and money whilst trying to meet customer and end user requirements.

Is cloud a priority in the financial sector?

According to research conducted by the Cloud Security Alliance (CSA) – "How Cloud is Being Used in the Financial Sector" – most organisations do not have a concerted cloud migration strategy, although a hybrid approach – leveraging both private and public clouds – is fast becoming the norm.

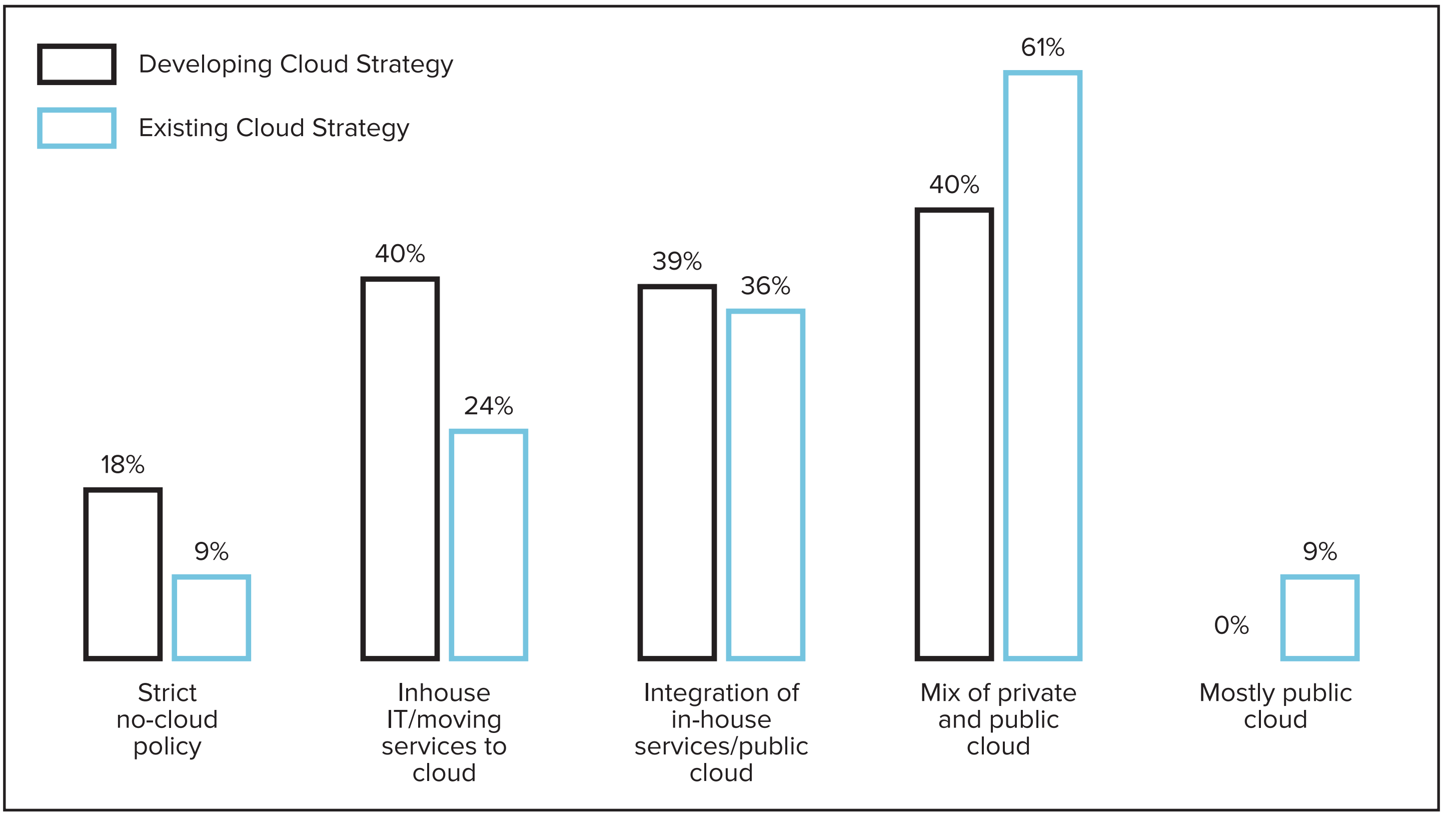
The study showed that the more digitalised an organisation's customer base is, the more likely they are to adopt a cloud strategy. And whilst you might expect the size of organisation to have a bearing, it's the the smallest and largest companies having the highest rate of cloud adoption, with mid-size organisations lagging some way behind.

Financial organisations with a cloud strategy in place



With a hybrid strategy proving the most popular approach to cloud, it's interesting to note that **70% of the companies with existing cloud strategies have chosen to adapt their strategy over time to include a greater percentage of public cloud services.** This is another sign of a growing confidence in adopting cloud services and relying less on in-house IT. Having a flexible infrastructure, reduced time for provisioning, reduced total cost of ownership, and shorter time to market are some of the primary reasons.

The changing approach to cloud adoption in the financial sector



From chaos to cloud

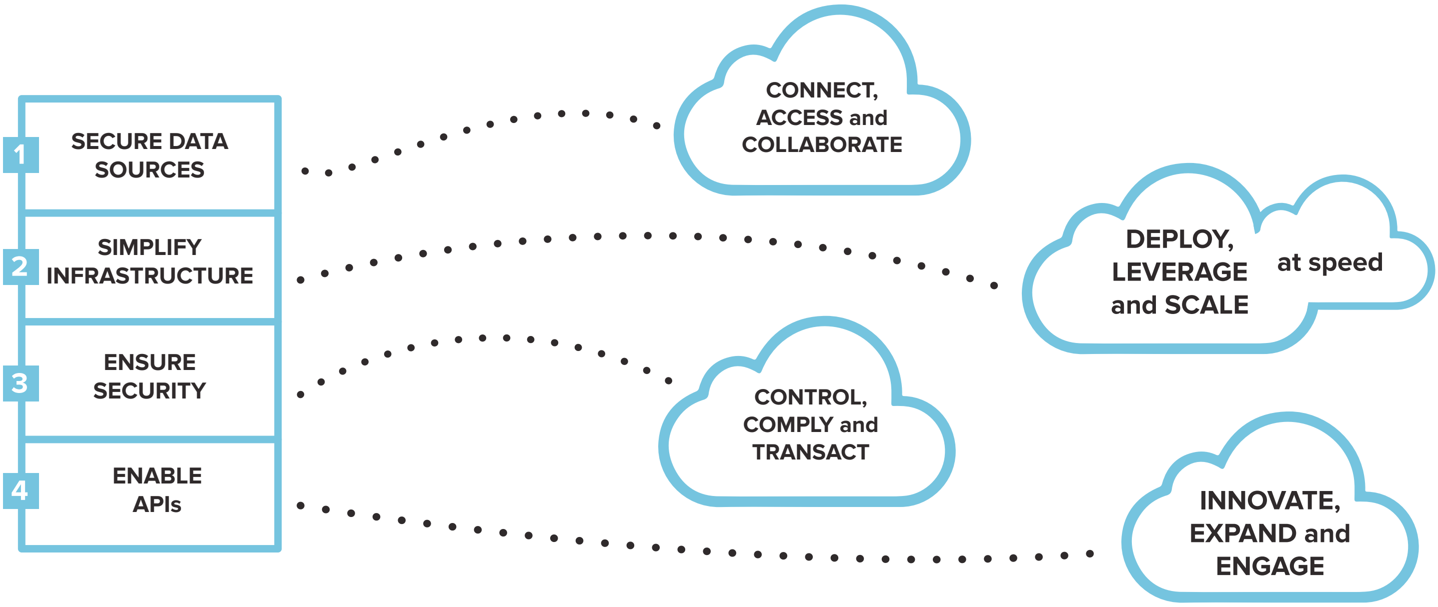
So the need for cloud is there and the will amongst financial services organisations is growing, but where should they start?

Whilst legacy IT environments are not sufficiently flexible, scalable or reliable enough to meet changing business needs, simply investing in a technology refresh is not the answer – leading to more complex environments, with more endpoints, data sources and integration requirements. Instead, a wholesale business transformation strategy is needed – re-architecting the business into a digital entity.

Start by mapping the current technology estate:

- **Which parts work well and need to be retained?**
- **Which elements have fundamental problems that are holding the business back?**
- **What do you want and need to change about the way the business operates and how can technology enable this?**

Then, consider how you can enable innovation, without sacrificing your existing IT investments. Essential to this, is avoiding a disconnect between cloud and on-premise systems. Hybrid integration provides the answer and global technology solutions provider, Prolifics, has developed a 4 pillar strategy for those organisations looking to ensure a best practice approach:


1 SECURE DATA SOURCES
2 SIMPLIFY INFRASTRUCTURE
3 ENSURE SECURITY
4 ENABLE APIs
CONNECT, ACCESS and COLLABORATE
DEPLOY, LEVERAGE and SCALE
at speed
CONTROL, COMPLY and TRANSACT
INNOVATE, EXPAND and ENGAGE

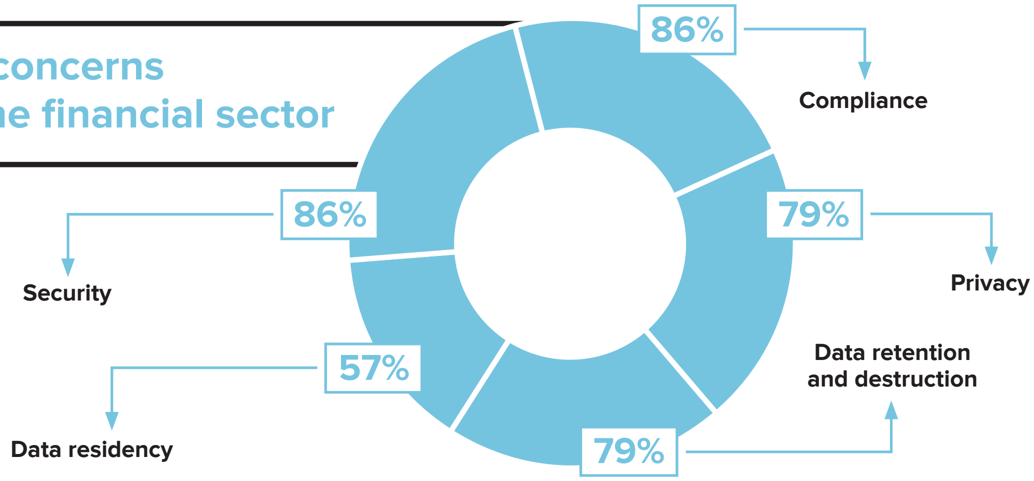
With these 4 pillars in place, you can confidently transform your legacy applications and undertake new digital-led initiatives through a world-class integration platform, such as IBM BlueMix. In this environment, cloud-based systems are integrated with existing apps quickly and securely – halving the cost and deliver time for new services to drive a significant competitive advantage. And because you've de-coupled the individual components from the physical architecture, they can then be linked tightly together or easily extracted in the future, enabling your business to:

- Make changes quickly
- React to what's going on in the market
- Gain commercial leverage over suppliers, with flexibility built in to your systems and processes

Managing risk in a digital world

The CSA survey amongst financial services organisations found that for those with a strict private cloud only policy, the main reasons were all related to data protection:

Key cloud concerns amongst the financial sector



With security topping the list of questions to be answered for most financial organisations, even those that feel confident that their data can be stored, transferred and accessed securely in the cloud, need to question whether they have the bandwidth and network capacity available to redirect all users to the cloud, should the need arise.

If the plan is to restore from the cloud to on-premises infrastructure, can you be sure that the restore will happen quickly enough to avoid significant business downtime? Incidents rarely happen at a 'convenient' time, so even if a data recovery process is tried and tested, would it still meet recovery time objectives should the need arise to call it into action in the middle of the night or on a bank holiday?

The rapid growth in data volumes and continuous change that is inevitable in today's digital world means that IT teams have less time to react to any back-up related incidents or problems. With the business increasingly reliant on 24x7 secure data access, the focus needs to be on recovering service levels, as opposed to simply recovering data. Traditional approaches to data backup and recovery are notoriously unpredictable and largely dependent on the level of time and resource dedicated to undertaking manual monitoring, maintenance and reporting. To support a digitally enabled financial services business, continuous and clear visibility over the utilisation and performance of data storage is essential.

Take the hybrid road to recovery

For those organisations that are serious about maintaining service levels in the event of unforeseen circumstances, a different strategy is needed. It's for this reason that an increasing number of organisations are choosing to take a 'hybrid' approach to data protection and disaster recovery – integrating the management of backup and DR services into core storage management tools and services. **In fact, according to a recent report by Gartner, by 2018, the number of enterprises using the cloud as a backup destination will double,** up from 11% at the beginning of 2016

By adding service management automation and orchestration to the data backup and recovery process, it's possible to combine the flexibility of the cloud with the security of local, on-premise control.

Recovery isn't just about data

Organisations going down the hybrid cloud route can gain a clear, single-pane-of-glass view of the performance and cost of data recovery – giving them a simple means of addressing any board-level or stakeholder concerns. Complexity is reduced throughout the management process, with quick-fix knowledge to help resolve administrative issues and easy access to historical data to enable trend analysis within the data protection environment. Essentially, this approach increases productivity, reduces costs and transforms an organisation's data backup and recovery platform into a hybrid cloud utility service. As a result, data protection is more transparent and predictable, more flexible and easier to manage.

By automating the monitoring, alerting, capacity and risk management process, any data-related issues can be identified and resolved before they become visible to business users or customers. The pressure is removed from data administrators and IT teams – ensuring that they have the right information available at the right time in order to manage and escalate potential problems – so they can focus on supporting business innovation, rather than simply maintaining the status quo.

Disaster Recovery: 10 Point Checklist

Whether you choose to work with a third party service provider, manage the process in-house, or take a hybrid approach to ensure the best of both worlds, the following checklist will help to support your decision making process:

1. How much data do I have?

Understanding how much data you have is important, but so is recognising how much of it is duplicated, out-of-date, or not needed as part of an immediate recovery strategy. Can the service provider help you to tier data and its recovery so that not all data is stored in the same place and at the same cost?

2. What's really important?

Which applications are the ones that are needed to ensure you can communicate & transact with your external customers and continue to interact with you internal customers? How can you ensure that all the right people can connect to the right applications at the right time, with minimal impact on system performance?

3. What can wait?

Starting at the bottom, which data & applications are the least important for your business to continue to operate 'as normal'

4. Where in my infrastructure is it?

Do you have data in cloud-based applications such as office365, google apps, salesforce.com etc. Is critical data hosted on mobile devices?

5. How much will downtime cost?

Every hour that your systems are down, revenue is lost and, in some cases your reputation and customers are lost for good. How long can the business survive and maintain reputation in a disaster without access to critical applications?

6. How do I access and secure my data?

Recovery of services in the cloud offers significant flexibility to access recovered applications, but how are your internal/external users going to connect? Do they have sufficient bandwidth coming in and do you have sufficient bandwidth going out? What about your websites? If these are currently part of your internal IT service portfolio, do you need to load balance web traffic for web services?

7. How quickly do I need to recover?

Once you have identified what is really important, you need to establish how quickly the business expects/needs these important services back online. This information will need IT & business working together to complete a business impact analysis (BIA) exercise. Will your disaster recovery as-a-service (DRaaS) provider offer a BIA prior to implementation?

8. Can I recover at all?

Is the data that is being transmitted off-site consistent and recoverable? What checks are in place to ensure that this is the case? Is it possible to test your solution bi-annually / annually without disrupting the DR solution that's protecting your production environment?

9. Who will be around to recover me?

Where does the responsibility for recovery lie – with you or the service provider? Either way, do you/they have all the skills necessary to recover not just the data but the applications? Are you/the service provider accredited or have proven expertise in all the areas you require?

10. When is data loss unacceptable?

Any regulated business knows that being able to recover data that may be deemed 'non-critical' by the business can nevertheless prove important in complying with data protection standards and legislation. Data governance should be a key part of your decision making process – ensuring that you can meet compliance and audit requirements on an ongoing basis.

3. Meeting the security challenges of digital transformation head on

The financial services sector is undoubtedly one of the most regulated industries in the UK today, meaning organisations are under a huge amount of pressure to ensure that the right controls are in place to protect their business and customer data. The negative impact associated with failing to ensure compliance has been well documented over the years, but the era of digital transformation has seen a significant shift in mindset from compliance simply being an obligation, to one of 'opportunity'.

Turning fraud from threat to opportunity

According to the Association of Fraud Examiners, a typical organisation loses approximately 5% of its annual revenues to fraudulent activity. Ensuring effective protection against fraud is therefore a primary concern for organisations in the finance sector, who are constantly challenged to balance opportunity with risk, whilst adhering to increasing regulatory demands. Any failure to address security risks is not only damaging to brand reputation and customer confidence – it can also have an immediate, adverse impact on shareholder value and the bottom line.

Increasingly sophisticated techniques are being used to defraud financial organisations and their customers – taking advantage of the relatively porous channels of the digital age, in which the majority of financial transactions are conducted online. At a time when both data volumes and the need to access and mine that data to extract the business value are growing, forward-thinking organisations are turning to new analytics capabilities. The aim is not only to help detect fraud attempts at the earliest opportunity, but also identify the culprits and gather the critical evidence that will be needed to ensure successful prosecution.

According to an IBM Institute for Business Value survey of 500 banking and financial markets executives, whilst for most institutions fraud is a serious problem, others (14%) have managed to turn it into a competitive differentiator – giving customers complete confidence that they have everything under control. So, how have they succeeded in transforming their fraud operations, when the majority have yet to even begin the process?

An integrated approach is key

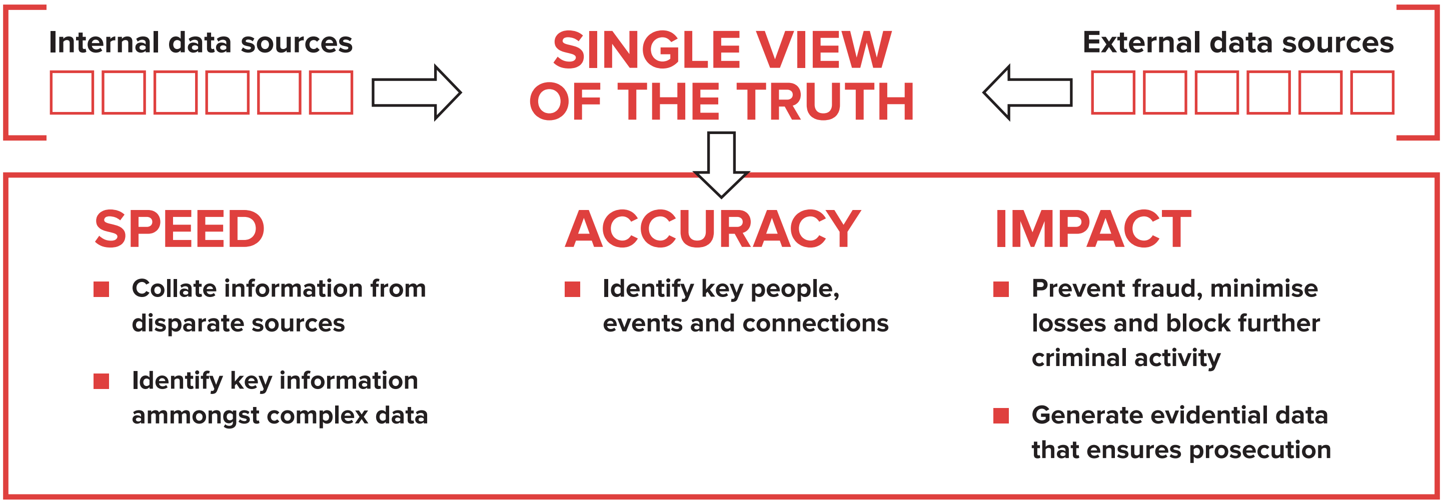
To combat fraud effectively, organisations need to find a way of integrating all the disparate internal and external data sources that are relevant and available, so that they are presented with a 'single view of the truth'. This will eliminate the time consuming and error-prone approach of spreadsheet-based analysis – presenting accurate data in a visual way that enables analysts to tackle complex investigations quickly, with minimal impact on day-to-day operations.

Having previously relied on individuals' instinct and hunches, many financial organisations have moved to automated decision making, using rules to standardise the process so that it becomes more consistent and reliable. However, in today's digital world where the available data and market conditions are in a constant state of flux, this approach is inflexible and limiting, with static rules quickly becoming obsolete.

The key is to combine business analytics with predictive models that are able to consider and adapt to new data as it becomes available – becoming smarter and more effective over time. Predictive analytics also enables personalisation, so that informed decisions can be made quickly, but on a unique, case-by-case basis.

This level of integration allows organisations to draw reliable conclusions about future events – making confident predictions that they can proactively act upon, rather than simply reacting and fire-fighting. It also makes the discovery of hidden data and connections possible, helping to provide clear evidence against fraudulent activity.

Integrate data sources to tackle fraud and corruption


Internal data sources

SINGLE VIEW OF THE TRUTH

External data sources

SPEED

- Collate information from disparate sources
- Identify key information ammongst complex data

ACCURACY

- Identify key people, events and connections

IMPACT

- Prevent fraud, minimise losses and block further criminal activity
- Generate evidential data that ensures prosecution

Cut costs and improve customer service through effective fraud management

Transformation initiatives require strong business cases to compete for a limited pot of funds, so whilst the direct cost savings in preventing fraud are substantial in their own right, it's the impact on customers that is proving the strongest pull for many organisations.

Integrated data analytics not only helps to combat fraud, but will also help to contain costs and deliver an enhanced customer experience. The deep insight that's uncovered through the variables and inter-relationships that define risk enables organisations to transform their processes and services to better fit customer needs, leading to happier and more profitable customers.

A good real-world example of this is Santam Insurance, South Africa's largest short-term insurance company. Their use of business analytics to improve their fraud detection capabilities also saw a significant improvement in customer service, with claims settled 70 times faster than before.

Santam also saw a dramatic reduction in operating costs, with a more efficient and integrated process enabling them to cut the number of in-depth claims investigations. Santam's business analytics solution automatically scores each claim according to its risk level, and then recommends the appropriate processing channel for settlement or further investigation.

> **"Within the first four months, we had saved R17 million on fraudulent claims, and R32 million in total repudiations – so the solution delivered a full return on investment almost instantly!"**
>
> Anesh Govender, Head of Finance, Reporting and Salvage, Santam Insurance

As part of a wider digital transformation strategy, the ability to integrate disparate systems and tap into unstructured data through BI and predictive analytics, will play a major role in mitigating the risk of multi-channel threats – securing customer loyalty and shareholder value.

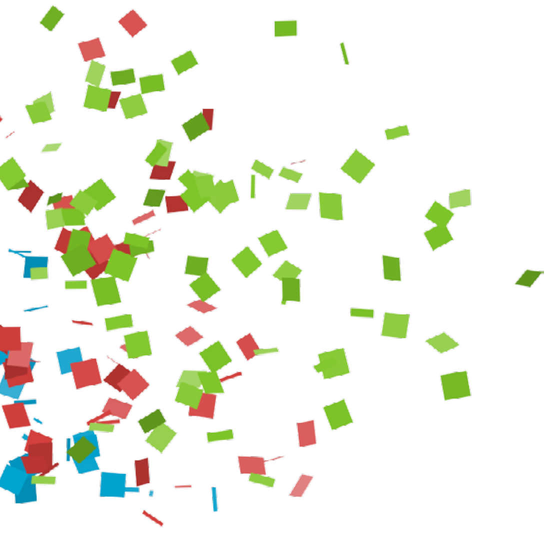
Compliance: Turning obligation into opportunity

Organisations in the financial services sector have always had to make ensuring compliance a priority, with legislation such as BCBS239 and Solvency 2. However, with the introduction of MIFID 2 and the new EU GDPR legislation, organisations need to move from viewing compliance as a tick-box exercise, to one that involves commitment from across the organisation. Do so, and the 'cost of compliance' can provide a many-fold return on your investment, driving significant business value.

The EU has approved the highly-publicised General Data Protection Regulation (GDPR) against the backdrop of global digital transformation – aiming to address the rapid increase in data volumes and dramatic change in use of personal data that's come about since the launch of the last EU Directive in 1995. The sheer scale of the wide ranging new requirements is compounded by a hard deadline of 25th May 2018 to ensure full compliance with the new regulations. Add to that the cost of non-compliance which could result in penalties of up to €20 million, or four percent of worldwide turnover (whichever is highest), and it is clear that organisations need to fully understand the requirements of the GDPR but also prepare well in advance of 2018.

Designed to protect personal information in an increasingly digital world, GDPR legislates that you can only collect personal data if:

1. **you have a statutory reason (e.g. employment)**
2. **you have a legitimate business interest**
3. **you have fully-informed and freely-given consent**



What action does the financial sector need to take?

Ensuring Consent

Before a customer can open an account, be credit checked or even receive direct communication from you, they must have first provided their consent for processing their personal data. For sensitive data of the sort held by banks and financial institutions, consent must be "explicit" – meaning that it is freely given, specific, informed and unambiguous.

Consider how your business currently collects, handles, stores and shares its customer data - comparing your current consent process with the requirements of GDPR. You can then begin a data cleansing exercise - deleting information you don't need, and building new consent management policies to protect the data you want to retain.

Ensuring Security

GDPR demands that any new system design incorporates data protection 'by design and default' and that a user's default settings must always maximise security. For financial service organisations going through a digital transformation process, this clearly needs to be taken into account at an early stage of any system design.

Reporting Data Breaches

GDPR demands that any data breaches likely to present a 'high risk' to individual rights and freedoms must be reported to the Data Protection Authority within 72 hours. Affected individuals should also be sent notification 'without undue delay'. Ensure that your organisation's data breach policies will comply with this requirement and update procedures as necessary.

Responding to Requests

Make sure you are prepared to handle data access or deletion requests within the new GDPR timescale of 1 month (extending to 3 months for complex requests).

However, whilst the focus of the GDPR is on protecting consumer and individual rights, there are significant business benefits to be gained by ensuring compliance, which are perhaps less obvious than avoiding the financial penalties and damage to brand reputation that are the usual business drivers.

Whilst the focus of the GDPR is on protecting consumer and individual rights, there are significant business benefits to be gained by ensuring compliance.

1 Driving digital transformation

Whilst financial organisations are collecting more data than ever, many lack the digital maturity needed to leverage it for business value. The need to comply with GDPR provides an opportunity to reconsider the data you collate, store and analyse – ensuring that it's properly understood, controlled and protected.

2 Understanding your customers

Whilst GDPR may limit the data that you are able to collate and store, the data that you can legitimately hold will significantly increase in value. In an industry that struggles to manage and make sense of the sheer volume of data, GDPR will filter out the relevant from the rest – providing a much clearer picture of who your customers are.

3 Attracting the next generation of customers

Once data is properly described, it becomes possible to measure its quality more objectively – using different standards and targets for different classes of data, based on its importance to the business.

Whilst most organisations will have a lot of work to do in transforming their processes and systems to ensure compliance, the GDPR is an opportunity for organisations to take a fresh approach to data - one where quality trumps quantity, and where consent, personalisation and privacy form the basis of a new relationship between financial institutions and their customers.

Summary

This White Paper brings together in-depth insight, real-world examples and best-practice thinking from leading specialists across the IT industry:

Entity Group: Digital transformation experts

ICit: Performance management solution specialists

Prolifics: Global technology solutions provider

Portal: Advanced analytics solution specialists

Silverstring: Hybrid cloud data protection solution and service provider

As a result of the insight and thought leadership provided by these organisations, along with direct research conducted by The IT Insider through a series of Twitter Polls, we can conclude that business leaders in the financial services sector:

□ **Have significant concerns about the impact of digital disruption within the finance industry**
With this in mind, organisations are generally willing, even if not yet able, to extend and enhance their digital services. Whilst some are very much focused on addressing the threat of disruption that 'big data' present in terms of both business cost and risk, a growing number of organisations are recognising the opportunities that the digital world delivers – getting closer to customers and enabling a productive workplace. Taking an integrated, hybrid approach to transforming legacy applications and introducing new solutions and services is key to success.

□ **Lack confidence in the visibility they have across growing volumes of different data sources**
Growing volumes and varieties of data mean that accessing a 'single version of the truth' can prove a major strain on time and resources. Key to minimising cost and maximising business benefits is to ensure that the right level of data governance is in place, prior to investing in technologies such as BI and predictive analytics.

□ **Feel under significant pressure to meet increasingly stringent rules around data protection**
Meeting new regulations such as the GDPR is a priority for business leaders today, but the majority of financial sector organisations are yet to put satisfactory processes in place to ensure compliance. Because of this, those organisations that are proactive in addressing security risks and protecting sensitive data have a great opportunity to gain a competitive advantage.

Whilst by no means exhaustive, this White Paper highlights a number of initiatives that could help to transform your business for the digital age.

To find out more or engage directly with our industry experts, please visit our website at:

https://theitinsider.co.uk/finance-heroes/