Research partner

BearingPoint®

Independent research by

Chartis

Counting and Cutting the Cost of Compliance

How to accurately assess the cost of Risk Data Aggregation and Regulatory Reporting

April 2018

About Chartis

Chartis Research is the leading provider of research and analysis on the global market for risk technology. It is part of Infopro Digital, which owns market-leading brands such as Risk and Waters Technology. Chartis's goal is to support enterprises as they drive business performance through improved risk management, corporate governance and compliance and to help clients make informed technology and business decisions by providing in-depth analysis and actionable advice on virtually all aspects of risk technology. Areas of expertise include:

- Credit risk
- Operational risk and governance, risk and compliance (GRC)
- Market risk
- Asset and liability management (ALM) and liquidity risk
- Energy and commodity trading risk
- Financial crime including trader surveillance, anti-fraud and anti-money laundering
- Cyber risk management
- Insurance risk
- Regulatory requirements including Basel 2 and 3, Dodd-Frank, MiFID II and Solvency II

Chartis is solely focused on risk and compliance technology, which gives it a significant advantage over generic market analysts.

The firm has brought together a leading team of analysts and advisors from the risk management and financial services industries. This team has hands-on experience of implementing and developing risk management systems and programs for Fortune 500 companies and leading consulting houses.

Visit ***www.chartis-research.com*** for more information.

Join our global online community at ***www.risktech-forum.com***.

About BearingPoint

BearingPoint®

With its RegTech product line, BearingPoint is a leading international provider of innovative regulatory and risk technology solutions (RegTech and RiskTech) and services across the entire Regulatory Value Chain for Financial Services. Customers representing 6,000 firms worldwide, among them large international banks, a major part of the largest European banks, leading insurance companies as well as supervisory authorities and central banks, trust BearingPoint's RegTech products and services. We work closely with regulators and as a member of standardization bodies like XBRL consortium, we actively contribute to the process of standard setting. We combine our regulatory expertise with our proven, reliable and future-oriented RegTech product line and expert consulting capabilities as well as training seminars and managed services.

About the BearingPoint contributor

Maciej Piechocki

For the last 10 years, Maciej has specialized in the areas of digitalization and regulation, especially in the financial services sector. In his role, he is responsible for delivering services and solutions to regulatory clients such as banks, insurance companies, central banks and supervisory authorities in the areas of regulatory reporting, regulatory management and regulatory analytics. He covers regulations such as Basel 3, Solvency 2, IFRS and MiFID but also implements standards such as XBRL or SDMX.

During his career Maciej has worked with several regulators worldwide, including Deutsche Bundesbank, the European Banking Authority, the European Central Bank, the Polish Central Bank, the SEC in the US, Japan's FSA, and the Chinese Ministry of Finance. He has also worked with a number of large banks, insurers and listed companies, and in consulting, software development, accounting standard setting and academia.

Table of contents

List of figures and tables

1. Overview and goals

A costly business

For Financial Institutions (FIs), the cost of complying with regulation can be heavy. Since the onset of the financial crisis FIs worldwide have been fined $270 billion[1], and counting. Their profits have also taken a hit – thanks largely to changes in the regulatory environment[2].

These changes are numerous and varied, from the introduction of new regulations and codes of conduct to greater demands for compliance and new approaches to governance. They have had an effect on most aspects of FIs' day-to-day operations. Alongside the financial penalties themselves, FIs have had to hire more staff to handle compliance with evolving regulations, and implement new, expensive and often unfamiliar technology.

The big problem for FIs is that many of these factors are ultimately beyond their control. What's more, responding to the challenges is costly. Coping with changes in derivatives market structures, for example, requires fundamental, wide-ranging organizational change. We believe that the industry as a whole spends close to $70 billion each year on risk, risk data and regulatory reporting, *excluding* any related spend on operations.

Yet FIs have no reliable way to assess just how much they are spending, or where their investment is having most impact. Some will be employing cost-reduction strategies, but in many cases without a reliable measure of their benefits. They urgently need a way to:

- Attribute the cost of regulatory compliance accurately across their organizations: people, processes, technology, outsourcing relationships and data standards.

- Adjust the key elements that affect their cost of compliance, according to the type of institution they are, their size, their client base, their organizational structure, the nature of their technology architecture, and their operational framework. Crucially, an FI's technology and operational framework will be much easier to change than its type or size, making these prime candidates for action.

Counting the cost of compliance for Risk Data Aggregation and Regulatory Reporting

This is the first of two reports that will explain how FIs can allocate, control and ultimately reduce their cost of compliance for Risk Data Aggregation and Regulatory Reporting (RDAR) activities. We have selected RDAR because:

- It accounts for the biggest proportion of an FI's compliance costs. Preliminary analysis[3] suggests that the industry-wide cost of RDAR operations and technology is about $70 billion.

- It is part of an FI's operations. It can be assessed and controlled more easily than nebulous strategic and business-model elements – leading to real, positive change.

[1] *This figure was arrived at by Chartis analysts, using data from several major published studies. Taking three separate sources as the base, we added estimates of the cost of market infrastructure changes, making the end value comfortably above $270bn.*
[2] *These include additional regulations around the structure of derivatives markets, for example, or restrictions on proprietary trading and new capital charges.*
[3] *Based on our global risk IT expenditure database and early data from a survey carried out for this research.*

Chartis has developed a robust, scenario-based maturity model and cost-attribution framework that FIs can use to analyze both their cost of compliance and the factors that influence it. In this paper we consider the key challenges FIs face in assessing their cost of compliance, define our areas of focus, and outline the central questions and hypotheses we will explore. We also briefly summarize the nature and methodology of the model itself. In the second paper we will provide a more detailed methodology and, using our own data and data from a survey of FIs, run the model and analyze its results. The second paper will also define the steps FIs can take to benchmark their cost of compliance, understand it in more detail, and cut it.

A unique approach

The cost-of-compliance model developed by Chartis Research focuses on the levers and mechanisms of cost in FIs' RDAR operations and IT. The scope of our research, which broadly corresponds to the process of regulatory reporting, is shown in Figure 1. We started our research by conducting a thorough review of published material on the theme of compliance costs. Many of these studies analyzed and quantified the overall cost of compliance and its associated system-wide impacts (such as a more risk-averse culture and a drop in profitability[4]).

But simply knowing the system-wide or average cost of compliance doesn't necessarily give you the means to control it. What's more, system-wide impacts – the focus of most of the studies we analyzed – do not generally map to individuals or specific operating processes and technology[5].

Our study focuses on the deep, granular characteristics of FIs' operational and technological processes. It links these to costs, but it also provides benchmarks and a mechanism to evaluate how specific managerial actions[6] can impact costs.

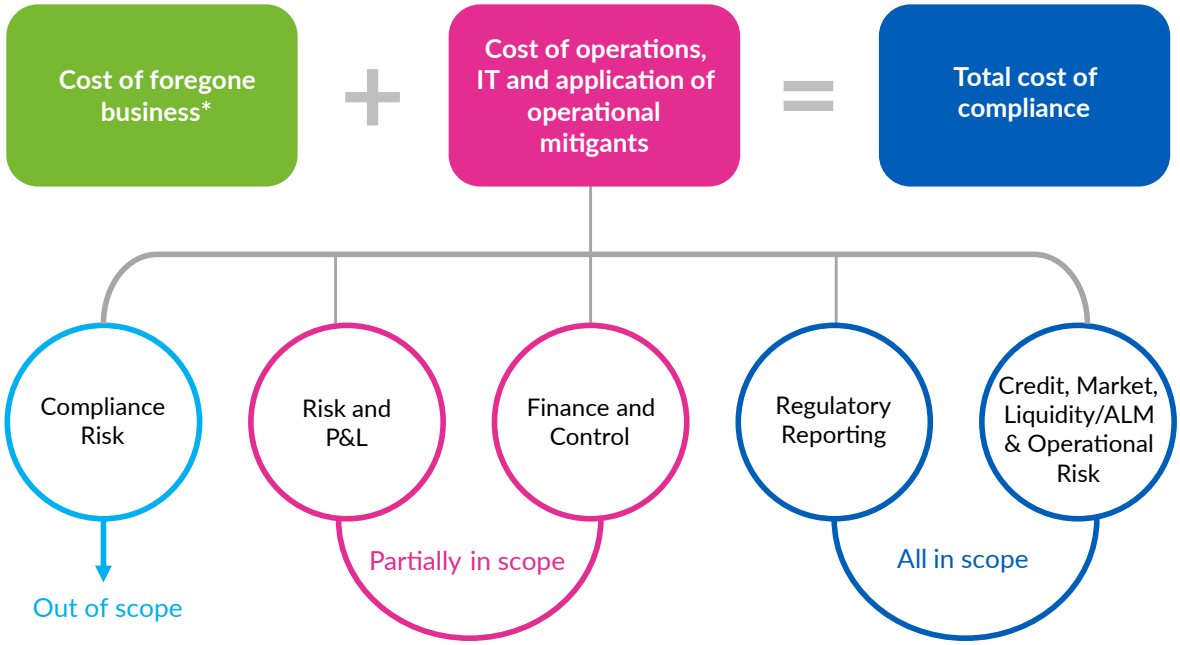
We intend our approach to be both *meaningful* and *actionable*, by clearly delineating the characteristics in FIs – the organizational 'levers' – that drive higher costs. These include:

- Data architecture.
- The size and nature of an institution.
- The type of regulation affecting it.
- The jurisdictions in which it operates.

Our approach is unique because it develops a granular and detailed mechanism of cost attribution. This in turn allows FIs to benchmark and analyze their costs and determine whether they are appropriate for their type of institution. It also creates a framework for comparing different classes of FI.

[4] *We analyzed studies carried out by the US Federal Reserve on banks in its systems, as well as studies by the International Monetary Fund (IMF). We found more than 75 studies covering system-wide impacts, written by academics and central bank representatives. A full bibliography will be provided in the second report.*
[5] *These are nevertheless very useful – we will include some key data points from selected studies in our model.*
[6] *Such as changing the messaging architecture, or adding internal or external utilities for specific or macro processes.*

Figure 1: The scope of the research: Risk Data Aggregation and Regulatory Reporting



** Measured by declining price-earnings ratio and profitability analysis*
Source: Chartis Research

Why bother?

Many FIs continue to face intense cost pressure – on their capital, from the cost of regulatory enforcement, and from crushed margins. Having a number for the overall cost of compliance is useful. But FIs must be able to drill down into the key elements of cost, quantify them, and then adjust the levers that influence them.

Understanding the *dynamics* of cost is also crucial. Is a centralized data warehousing strategy the right and most cost-effective approach to the data issue, for example? Or will a model-free framework work better? Equally, as utilities become more important in some geographies, what is the relative impact of employing them?

This research and its associated models and tools will enable FIs to understand a significant area of their technology and operational costs. It will:

- Help FIs define the structure of their operations, and benchmark the ideal risk operations for their size and structure.
- Benchmark their costs to their peers and understand where different elements of their costs come from.
- Define the impact of key architectural and operational decisions[7].

Our overall goal is to create a model that enables FIs to allocate and analyze exactly what their RDAR IT and operations cost. Within that, we have two key aims:

[7] *Such as having a centralized data management structure or a distributed point-to-point structure; or employing a shared-service internal utility or business-line-specific operations; or the impact of incorporating external utilities.*

- First, to quantify the impact of communications/feed-management architecture on overall RDAR costs (both the cost itself *and* its dynamics).

- Second, to quantify the impact of other factors, such as centralization of the data model (as opposed to a distributed model), the size of the institution (e.g. examining economies [or 'dis-economies'] of scale), and the use of reporting and aggregation utilities across different jurisdictions.

In the process of our research, we will also answer some important questions about the parameters affecting the cost of compliance, such as:

- Does cost vary by institutional type? And if so, by how much?

- Does cost vary by the type of regulation affecting the FI?

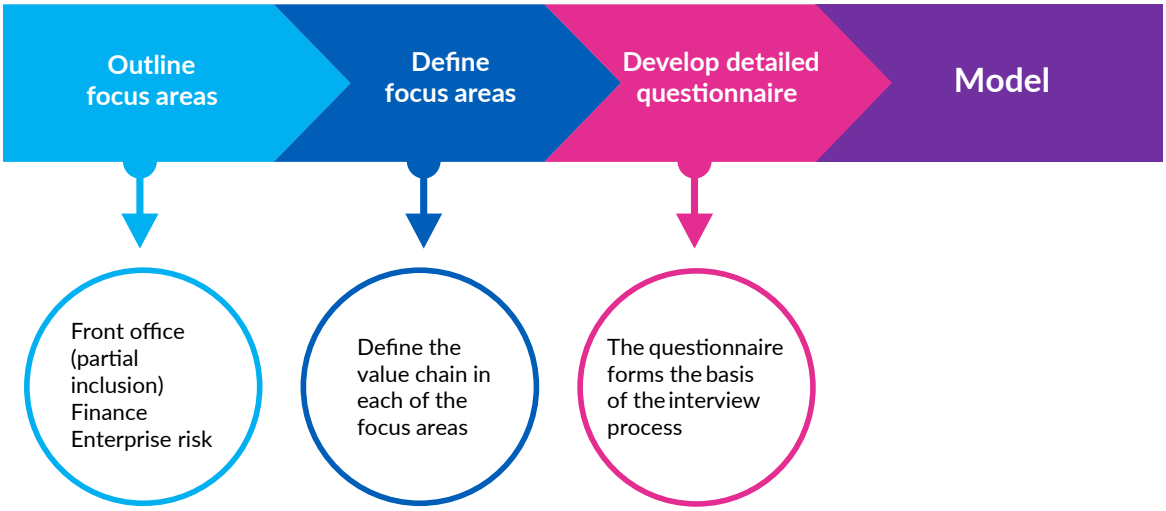
- Does cost vary by the types of client the institution serves?

2. Methodology and approach

Our methodology has four key steps (see Figure 2):

- Outline the focus areas.
- Define the focus areas.
- Develop a detailed questionnaire.
- Develop the model.

Figure 2: Simplified methodology for the Chartis Research cost-of-compliance model



Source: Chartis Research

Outline the focus

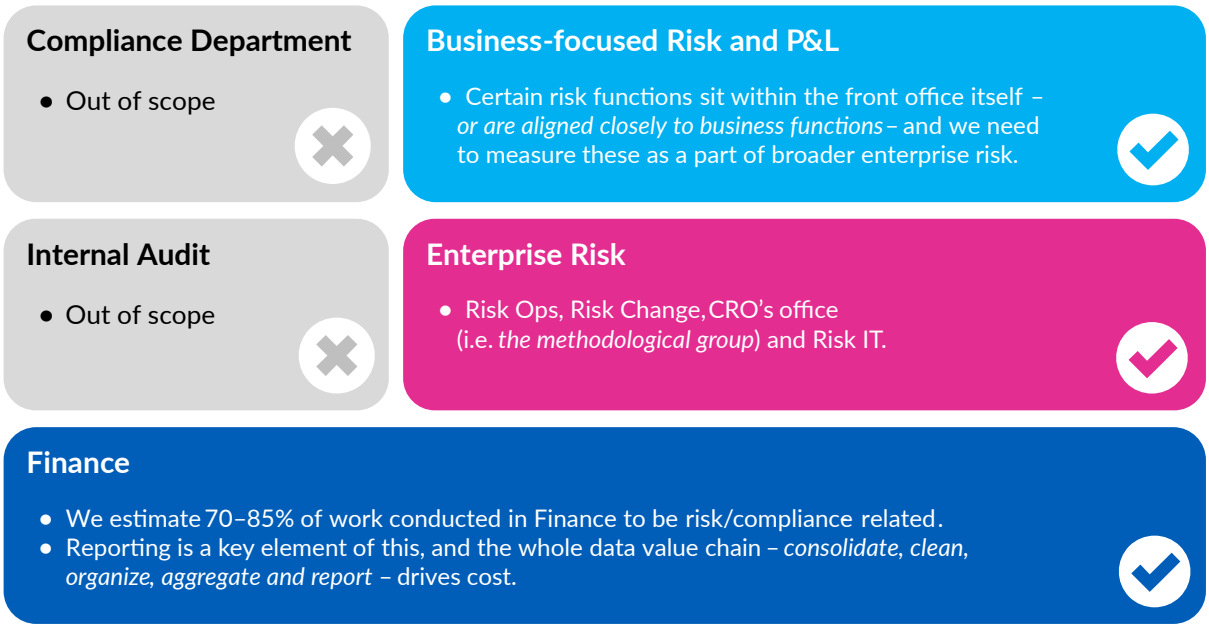
First, we need to drill down into the discrete business units and operational and technology areas we will include in our analysis, and which we focused on during the survey for the model.

The focus of our research is the costs arising from the IT and operational units that are closely associated with FIs' RDAR. The broad divisions and verticals we considered in our analysis were (see Figure 3):

- Enterprise risk.
- Finance.
- Business-focused risk and Profit and Loss (P&L) groups.

We did not include audit and compliance departments in our scope. There are clear inputs from the compliance group into areas of management reporting, and Anti-Money Laundering (AML) is reported to regulators. But the overall impact of these groups on the RDAR value chain is marginal. They make up only a small component of systems and, therefore, overall operational spend.

Figure 3: Defining our scope – business divisions and verticals covered in this study



Note 1: key drivers of cost are Full-Time Employees (e.g. business, ops, IT); software (e.g. internal/external); Infrastructure (e.g. direct/indirect).
Note 2: software costs and infrastructure (excluding the front-office) will be derived from latest Chartis Risk IT Expenditure data.
Source: Chartis Research

Next we outlined the key activities in each of these selected groups that we will analyze, and the key processes we will examine when calculating costs (see Table 1).

Table 1: The key functional areas of the RDAR value chain

Functional areas	Value chain segments	Regulatory drivers
Enterprise risk	• Data collection – transaction data, market data, CSA • Pre-risk data warehouse • Pricing valuations and P&L support • Risk engines (covering market, counterparty, credit and liquidity risk) • Risk attribution • Data distribution (to finance department and front office)	• Basel 1/2/3 • MiFID II • FRTB • BCBS 239
Finance	• Data collection across different departments • Data quality, consolidation and integration • Internal audit • Model validation	• Basel 1/2/3 • MiFID II • FRTB • BCBS 239 • SOX
Business-focused Risk & P&L	• KYC and counterparty risk • xVA • Balance sheet optimization • Accounting standards • Trader surveillance • P&L attribution • Limits management	• MiFID II • MAD/MAR • FRTB
Compliance & Internal Audit	• Transaction surveillance • KYC/AML • Data management • Cyber risk • Internal audit	• Money Laundering Regulation 2007 • Patriot Act • Solvency II

For definitions of the acronyms used in this table, see Appendix B.
Source: Chartis Research

Define focus areas

By clearly identifying the relevant business lines and functional areas we want to cover in the research, we can outline the structure of the research itself. This begins with the value chain, which passes through five stages (see Figure 4):

- **Organizational structures**. The structure within the FI, as well as its business lines. Whether a bank is retail- or wholesale-focused, for example, will be directly relevant.

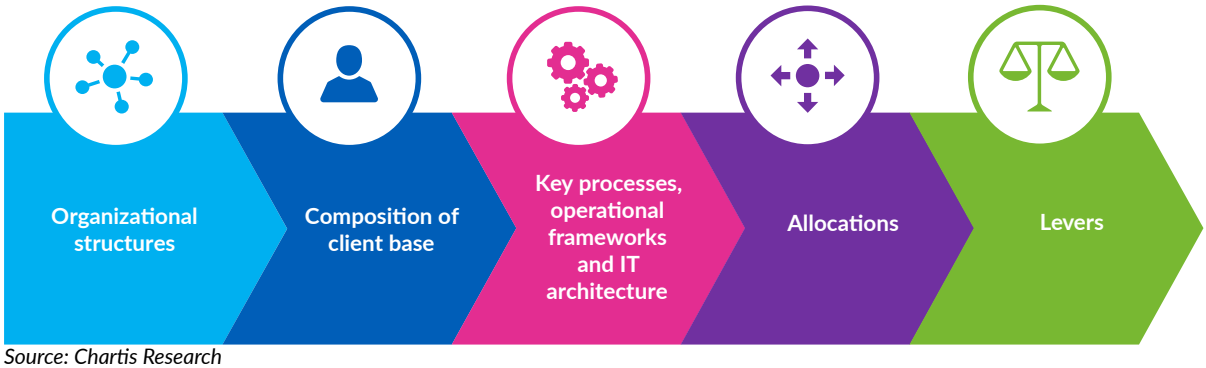
- **Composition of client base**. The nature and size of the client base. Our observation, based on the institutions analyzed, is that the nature of the client base hugely impacts the IT infrastructure. Those servicing a predominantly brokerage client base, for example, will have a relatively lower cost of RDAR because of their more simplified IT architecture.

- **Key processes**. The detailed processes and architectural components we identified will be covered in the context of three organizational units – Business-aligned risk and P&L, Enterprise risk and Regulatory reporting.

- **Allocations**. Having developed the overall cost model, we will then allocate costs back to the specific operations and processes identified.

- **Levers**. The levers are the mechanisms that institutions can adjust to make changes to their existing organization, technology or people, ultimately changing their overarching cost of RDAR compliance. Levers considered in this study include:
    - Centralized data warehouses vs. decentralized data sources.
    - Availability of Application Programming Interfaces (APIs).
    - Feed-handler environments.
    - The variety and diversity of supported reports.
    - The utilization of shared services and utilities.

Figure 4: Defining the value chain for RDAR compliance cost



Source: Chartis Research

One critical lever: the feed-handler environment

As highlighted above, the operational levers that FIs can adjust include: the use of utilities; the availability of APIs; and the variety and diversity of supported reports. One important lever that affects the overall cost of compliance is the feed-handler environment. It's important because it influences not only the overall cost of compliance but also the way that costs scale up and down against other parameters.

Based on a sample of banks we surveyed as part of our initial research, we observed that different institutions had highly variable architectures, reflected in the structure of their feed-handler environments. Some had a consistent and coherent internal utility-like framework, whereas others employed point-to-point architectures. Similarly, some firms had a fully message-oriented platform across all their lines of business, whereas others employed ad hoc structures.

Questionnaire and data collection

To power our methodology we collected a range of key data items from a variety of FIs, from global Tier 1 institutions to supra-regionals and narrowly-focused local firms. In many instances – particularly for the Tier 1 firms interviewed – we had several contacts within the institution, enabling us to develop a broad understanding of the overarching organizational structure.

In addition to these primary inputs, we also used data from the Chartis Research Global Risk IT (GRIT) expenditure analysis, to supply cost data for a broad set of FIs, including regional banks, universal banks[8] and retail-focused banks. (For more information on our GRIT expenditure analysis, and how we employed it in our research, see Appendix A.)

RDAR-specific discussions

We asked our sample of FIs a comprehensive set of questions and cross-referenced the answers against the GRIT expenditure database. Key areas of insight included:

- **Organizational definition**, across several dimensions:
    - A high-level functional definition (e.g. retail, capital markets-oriented, universal, etc.).
    - Jurisdictional coverage. Institutions operating in hundreds of jurisdictions, for example, tended to be universal banks with complex organizational processes and substantial regulatory reporting costs.
    - Regulatory focus. An institutional focus on MiFID, for example, tended to create more costs for capital markets-oriented institutions.

We also approximated the FIs' current operational costs and analyzed the structure of their existing regulatory reporting processes.

- **Client base**. One of our assumptions was that the size and nature of an FI's client base has a significant impact on the type and volume of the data passing through the regulatory reporting process. We profiled the clients that FIs service in each of their business lines.
- **Infrastructure**. Key elements of an FI's infrastructure include:
    - Workflow.
    - Aggregation architecture.
    - Supporting operations for workflow and aggregation architecture.
    - Potential use of utilities.
    - Nature of supporting personnel.
    - Availability of external support, either IT support or systems support (via utilities) or outsourcing.
- **Nature of regulatory reporting**. To define and outline the regulatory reporting process we examined key issues such as:
    - The personnel handling the bank's regulatory reporting needs.

[8] *Including institutions with large brokerage units.*

- The level of standardization.
- The approach to and impact framework for new regulation.
- Data quality processes and standards.
- New product approval processes and systems.
- The overreaching data management process.
- The use of statistical methods[9] or Artificial Intelligence (AI) to support risk and compliance data management processes, and the potential use of automation.

[9] *Such as factor or cluster analysis.*

3. Conclusion

FIs need a reliable way to assess – and control – their risk- and regulatory-related costs. Broad cost-compliance studies are very useful and impactful, particularly for interested parties such as regulators and investors. But they are less useful for banks that want to benchmark their costs against their peers, decide how to reduce the cost of their IT and operational infrastructures, and fine-tune their organizational frameworks. Broader macro-level studies do not help FIs identify weaknesses in their feed architecture, data warehousing or strategy, or decide which levers to adjust to streamline their regulatory reporting processes.

We believe our study will add a new and valuable dimension to the ongoing debate around compliance costs, at a time of intense cost pressure on FIs. Our approach will produce a detailed model to quantify, allocate and control risk RDAR costs. Our follow-up report will explore the key questions and issues in more detail, specifying details of the model and providing results. We will also show how FIs can use our framework to benchmark and analyze RDAR costs across a range of institutions.

'Regulatory projects have so far operated on a "whatever needs to be done" basis. However, we need to treat this as one of the elements of doing business – like having a trading system or a bank branch.' – Program manager at a large universal American bank.

Key findings from the interviews

Several themes and findings have emerged from the interviews and research we have done so far. These focus on the big concerns among FIs when it comes to the cost of compliance: what is driving costs, dealing with data, and the challenge of integration.

Costs – the big drivers

For the FIs we spoke to, the significant components of overall compliance costs were:

- The cost of analyzing and managing change.
- The internal/external communication framework.
- The feed architecture. Flexible feed architectures increased upfront (capital) costs but decreased variable costs.
- Data architecture and data flow architecture (see below).

Data is a big challenge

- *Data preparation and validation* across the reporting pipeline are expensive, difficult and error-prone.
- All of the FIs we surveyed were keen to automate these processes, despite the huge challenges involved.
- All were using statistical and AI techniques to try and control their costs, with some success. But they all conceded that there was a long road ahead.

- *Data integration* was another significant area of cost.
    - Its complexity and challenges differed across business lines.
- For investment banks, complex data and varying production timescales were important issues.
    - A number of standards in this area helped to mitigate these issues.
    - Despite complex data sets and human-resource structures, a standardized adapter framework simplified the problem, making integration with new systems less of a challenge.
- Retail and banking-book FIs, despite having relatively simpler data sets, had fewer standards.
- The variability and variety of data types and sources meant that running costs were often high, despite a greater availability of human resources and lower upfront costs.

'Flexibility and control is not just an organization issue – it is something you have to enforce through the technology architecture.' – Head of the market risk program at a large European bank.

Integration pain – outsourcing relief

- The biggest headache for FIs is integrating across silos.
- Broad, general utilities have little value for FIs.
    - They prefer utilities for operational niches or specific jurisdictions.
- For FIs in certain markets, outsourcing a very significant part of the workflow was appropriate – especially specific activities such as reporting and data management for certain verticals.
    - These were seen as very good candidates for utilities and powerful mechanisms of cost-control.
- All FIs would consider outsourcing significant elements of their value chain for jurisdictions outside their home base.
- All believed that while they would remain 'system integrators' for their regulatory reporting, many parts of the value chain are already heavily outsourced.
- FIs would welcome utilities in specific areas of data management.

'The biggest benefit of offshoring, outsourcing or using external entities like utilities is not the cost reduction but the standardization of processes that it imposes on the organization.' – Head of a risk management program at a large European bank.

4. Appendix A: Leveraging the global risk IT expenditure database

Using insights from the GRIT expenditure report, we augmented our findings with useful insights and observations. The resources provided by the GRIT expenditure analysis give us a valuable input into the overall project, helping to ensure that our final analysis reaches meaningful, actionable conclusions.

The database on which the report is based contains data from a broad array of sources, and is used to produce our annual expenditure forecasts. These sources include:

- Risk technology buyers and senior decision makers from financial institutions.
- Risk technology vendors.
- Risk technology consultants and system integrators.

We base our forecast methodology on the specific market characteristics of each major region and selected countries. The research uses financial industry data such as the overall number of banks, brokers/dealers and asset/fund managers, market concentration, and the overall IT expenditure per firm and vertical industry.

We also modeled FIs' expenditure on each type of risk solution by each vertical within each country. Risk IT spending is modeled from the FIs' perspective, and is then validated against vendors' and consulting firms' revenue data.

5. Appendix B: Glossary

Table 2 lists some of the common terms encountered during our research and in this report.

Table 2: Glossary of terms

Term	Definition
AML	Anti-Money Laundering
BCBS	Basel Committee on Banking Supervision
CSA	Commission Sharing Agreement
FRTB	Fundamental Review of the Trading Book
MAD	Market Abuse Directive
MAR	Market Abuse Regulation
MiFID	Markets in Financial Instruments Directive
KYC	Know Your Customer
P&L	Profit and Loss
SOX	Sarbanes-Oxley Act
xVA	Generic term for the family of valuation adjustments

Source: Chartis Research

6. How to use research and services from Chartis

In addition to our flagship industry reports, Chartis also offers customized information and consulting services. Our in-depth knowledge of the risk technology market and best practice allows us to provide high-quality and cost-effective advice to our clients. If you found this report informative and useful, you may be interested in the following services from Chartis.

For risk technology buyers

If you are purchasing risk management software, Chartis's vendor selection service is designed to help you find the most appropriate risk technology solution for your needs.

We monitor the market to identify the strengths and weaknesses of the different risk technology solutions, and track the post-sales performance of companies selling and implementing these systems. Our market intelligence includes key decision criteria such as TCO (total cost of ownership) comparisons and customer satisfaction ratings.

Our research and advisory services cover a range of risk and compliance management topics such as credit risk, market risk, operational risk, GRC, financial crime, liquidity risk, asset and liability management, collateral management, regulatory compliance, risk data aggregation, risk analytics and risk BI.

Our vendor selection services include:

- Buy vs. build decision support
- Business and functional requirements gathering
- Identification of suitable risk and compliance implementation partners
- Review of vendor proposals
- Assessment of vendor presentations and demonstrations
- Definition and execution of Proof-of-Concept (PoC) projects
- Due diligence activities.

For risk technology vendors

Strategy

Chartis can provide specific strategy advice for risk technology vendors and innovators, with a special focus on growth strategy, product direction, go-to-market plans, and more. Some of our specific offerings include:

- Market analysis, including market segmentation, market demands, buyer needs, and competitive forces
- Strategy sessions focused on aligning product and company direction based upon analyst data, research, and market intelligence
- Advice on go-to-market positioning, messaging, and lead generation
- Advice on pricing strategy, alliance strategy, and licensing/pricing models

Thought leadership

Risk technology vendors can also engage Chartis to provide thought leadership on industry trends in the form of in-person speeches and webinars, as well as custom research and thought-leadership reports. Target audiences and objectives range from internal teams to customer and user conferences. Some recent examples include:

- Participation on a 'Panel of Experts' at a global user conference for a leading Global ERM (Enterprise Risk Management) software vendor
- Custom research and thought-leadership paper on Basel 3 and implications for risk technology
- Webinar on Financial Crime Risk Management
- Internal education of sales team on key regulatory and business trends and engaging C-level decision makers

7. Further reading

- *RiskTech100® 2018*
- *Data Integrity and Control Solutions in Financial Services: Market Update 2018*
- *Enterprise GRC Solutions: Market Update 2017*
- *Spotlight: quantifying cyber risk in financial institutions*
- *Risk Data Aggregation & Reporting Solutions 2016*

For all these reports see ***www.chartis-research.com***.