Three essential steps to a better FIU

Strong leadership, a pragmatic data strategy and powerful case management are the keys to building an effective Financial Intelligence Unit.
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 WatersTechnology. Chartis’ 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](http://www.chartis-research.com) for more information.

Join our global online community at [www.risktech-forum.com](http://www.risktech-forum.com).
About NICE Actimize

NICE Actimize, a provider of financial crime, anti-money laundering, enterprise fraud and compliance solutions, is a leader in Autonomous Financial Crime Management.

The Autonomous journey begins with NICE Actimize’s ActOne, which aims to transform financial crime investigations by introducing intelligent automation and visual storytelling for speed and accuracy.

Intelligent automation saves time by enabling a virtual workforce of robots to collaborate with human investigators, while visual storytelling uncovers more risks by showing relationships between entities, alerts and cases in a visual manner.

The Autonomous path continues with the release of X-Sight, NICE Actimize’s Financial Crime Risk Management Platform-as-a-Service, which leverages the cloud. For more information, contact info@niceactimize.com.
Table of contents

1. Introduction: FIs under pressure  
2. Improving detection and cutting costs  
3. Bringing it all together – centralizing into one unit  
4. Building the FIU: the technology approach  
5. Conclusion: three key steps  
6. How to use research and services from Chartis  
7. Further reading
List of figures and tables

Figure 1: Constructing the entity view from multiple data sources 8
Figure 2: Differing definitions of the Financial Intelligence Unit 10
Figure 3: Key FIU projects in Europe and the US 11
Figure 4: FIUs offer advantages over traditional siloed approaches to financial crime risk management 12
Figure 5: Reporting lines of the FIU 13
Figure 6: Case management as a unifying layer in the FIU 15
Three essential steps to a better FIU

Financial Institutions (FIs) face an anxious and uncertain future, as they wait for criminals to strike and regulators to descend. Nor can they ignore digital developments, because their customers demand them and criminals exploit them. But tackling these problems requires huge amounts of data, vast numbers of employees to process it, and big costs.

New ‘entity risk’ approaches promise to surmount the problem of organizational and geographic ‘silos’ inherent in monitoring transaction risk, enabling FIs to build three-dimensional pictures of risky entities. Automation can help to reduce employee costs, particularly within a centralized system.

Financial Intelligence Units (FIUs), which offer a way to centralize and automate, are already proving popular with FIs. But there are many definitions and types of FIU, and each FI will have its own idea of what constitutes a successful unit.

New research by Chartis and NICE Actimize pinpoints an effective starting point – to view the FIU as a technology infrastructure with three essential elements: strong, clear leadership, a pragmatic data strategy, and powerful case management. While developing a truly effective FIU is a long, complex process, by starting with these three essentials FIs can transform the FIU into a valuable resource in financial crime risk management and protection.
1. Introduction: FIs under pressure

FIs are complex organisms, made up of diverse interconnected branches, business lines and departments, often spread across country and state borders. If a single part becomes compromised, it can affect the entire entity, as highlighted recently by money-laundering scandals and failures at two large banks, one of which – Danske Bank – involved billions of Euros and thousands of customers.

These cases can be complex and protracted, and the fines they trigger are often retrospective in nature – the Danske Bank scandal occurred between 2007 and 2015. FIs can find themselves operating under the shadow of their past mistakes, waiting anxiously for a possible knock on the door from regulators, and in the meantime trying to find the best way to protect themselves.

Costly compliance

FIs must also cope with steady growth in the number of transactions they handle, as well as the number of Suspicious Activity Reports (SARs) they have to file. Their attempts to deal with the problem have mostly resulted in annual increases in spending geared toward improving their risk management operations. Establishing huge compliance departments to monitor sanctioned entities and transactions has been the best way forward, despite the costs involved – compliance departments can contain thousands of full-time employees and cost billions of dollars across the industry.

But the success of these programs has been mixed, and several years into their development FIs are keen to see some benefit from them. Compliance departments are expected not only to prove their worth, but also to develop more complete views of FIs’ historical transactions and customer relationships and behaviors, to improve how they tackle financial crime.

Digital demands

The so-called ‘digital revolution’ is also having a transformative impact, particularly in retail banking. As bricks and mortar bank branches fade into obscurity and front-office staff numbers decline, what differentiates financial providers often tends to be the quality of the digital experience they provide. In some developing regions, notably many African countries, FIs often leave out bricks and mortar branches altogether.

As growing numbers of digital start-ups enter the market, the pressure is mounting on established FIs to match them with more convenient services and more flexible customer relations. Customers want high-speed, frictionless services (such as payments, onboarding and account comparison), provided through digital and mobile channels. At the same time, data breaches and the still-fresh wounds of the financial crisis mean that FIs cannot compromise on security for fear of regulatory and public censure. But new transaction systems, payment channels and identity verification methods cost money, and create more data that someone must process.

Meanwhile, digitally enabled criminals are using technology to target bigger institutions and plunder more assets, and to disguise themselves more effectively while doing so. In the digital sphere the tools of their trade are becoming commoditized, and collaboration with organized criminals and even nation states is now easier in hidden areas of the internet such as the ‘dark web’.

---

2. The latest research from Chartis indicates expenditure of about $20bn dollars in 2018.
2. Improving detection and cutting costs

FIs have two goals:

- To get better at detecting fraud, to avoid losses from crime and the fines that ensue.
- To keep technology and staff costs down.

Digital technology can help, offering new ways to tackle fraud and financial crime. But it can be a cost burden too – as it advances and evolves, so the need to invest in it grows. A big part of the problem is having to monitor financial crime risk across ‘silos’ – disparate business units and even companies, often widely dispersed across the globe.

Detecting fraud – the move to entity risk

Technology may be costly, but new applications are contributing to marked improvements in fraud detection. One important area of Financial Crime Risk Management (FCRM) where technology is proving especially effective is in helping FIs to move from the transaction-based risk management of old to a more ‘holistic’ form of entity-based risk management that uses data from multiple sources across the organization (see Figure 1).

The focus of FCRM has shifted: no longer is it merely about monitoring whether a user or organization – an ‘entity’ – conducts transactions outside prescribed boundaries. Nowadays FCRM involves constructing a coherent and multi-dimensional view of how people behave, and in the process creating data that can be fed into ever more sophisticated tools and techniques (such as behavioral analysis). In short, FIs can now view their customers as complex individuals rather than just a combination of transactions.

This has several benefits:

- There is no constant need to switch investigations between silos: across systems, branches or institutions.
- There is no need for FIs’ employees to take copious notes at every stage of a customer relationship, because they can refer to pre-existing information instead.
- Using specific and sophisticated software (such as graph analytics and entity resolution tools), it’s possible to get a more ‘three-dimensional’ view of an entity, helping FIs make better, more informed decisions about how to deal with it.

Which type of entity to pursue?

Investigators can now assemble an ‘image’ of how customers behave based on data about their transactions and identity. Creating an ‘entity view’ is not straightforward, however, and presents FIs with several choices. Guiding their decisions are two important, and different, goals for their entity risk system: whether to aim for a ‘golden source’ entity, or take the less complex – but no less valuable – ‘dynamic’ option.

- To create ‘golden source’ entities, FIs establish a consistent view of an entity that they then enrich and update, feeding that information into analytics systems. The key to this entity view is that it persists and can be edited over time.
- To create a ‘dynamic’ entity, data is assembled ‘on the fly’ and pulled from separate systems as and when it is needed, depending on the specific business case. While this is less computationally taxing (continuously reconciling different systems around a singular entity takes work), it lacks the consistency of the ‘golden’ option.

Both types of entity view are a big step forward in FCRM. And while they may differ in the type of entity they analyze, both have similar underlying requirements: to achieve a better, more accurate view of the people that engage with financial providers.
The approach an FI takes will depend mainly on how big and complex it is. ‘Golden source’ entities provide a more stable view over time, but may only work for relatively small FIs. For large Tier 1 FIs, which contain and produce huge amounts of data, maintaining and validating trusted views of individuals can be prohibitively complicated and/or costly. At the other end of the scale, the smallest institutions may not enjoy the same benefits from aggregating their FCRM processes. They have relatively straightforward FCRM requirements around sanctions monitoring and due diligence, as well as smaller numbers of customers and much lower costs.

Chartis believes that the largest FIs will prefer a ‘dynamic’ view of entities, which assembles views from pre-existing data sources in real or near-real time, to aggregate information from FCRM silos while avoiding a costly consistent view. Medium-sized FIs, meanwhile, are more likely to opt for the ‘golden source’ entity view, by building data lakes using Hadoop and similar technologies.

Reducing employee costs – automation

Technology can also help to tackle the problem of oversized compliance departments. While FIs are cautious about reducing the size of these, they are aware that they can put their employees to more effective use by assigning them to more complex investigative functions rather than repetitive FCRM ‘busywork’ (such as SARS reporting).

Automating much of the repetitive work they do can help in this, by using Robotic Process Automation (RPA) to make FCRM processes faster and more accurate, saving time and money. This could involve determining which parts of a workflow are being performed in a repetitive way (by monitoring the system itself or via scraping), or developing faster ways to surface information (by auto-completing forms with the correct reference information, for example).

---

3 Such as more ‘long-term’ criminals, who appear to be standard customers before going on to commit fraudulent acts.
3. Bringing it all together – centralizing into one unit

Ideally, to harness the potential of entity-based risk management and automation, FIs must bring all their FCRM tools and processes together into a centralized system. To overcome the problem of organizational and FCRM silos, FIs can create a single analytical control hub to gather and analyze data about a particular entity, whether it’s tracking fraud and AML-related activity or combining information from different institutions or even countries.

Because all information about an individual is collected in the same place, FIs can assign complex investigative functions to employees who can gain a more complete view of the entities they are viewing, rather than being confined to an AML or fraud silo. The risk of duplication is also reduced – investigators are less likely to perform the same search on an entity that has already been cleared by a worker elsewhere in the organization.

By combining centralization with automation, FIs can first get a more complete picture of their processes, and then pinpoint those intensive, repeatable activities that can be automated across the organization. These could include document checking, onboarding and searching for customers within the bank’s data or third-party data stores. However, it’s worth remembering that because RPA will be applied to those processes most amenable to automation, the effects on overall FCRM will be asymmetric. Processes such as the final step of scoring a sanctioned entity as a true or false positive are typically assigned to people, rather than to RPA – so individuals will remain a central part of FCRM systems.

A key point, however, is that bringing together the relevant people and data will permit a better entity view. In this way, better data can be fed back into systems to drive further improvements. One way this can be accomplished is in a Financial Intelligence Unit (FIU).

What is an FIU?

FIUs are already fairly commonplace – almost all FIs have one in some form or another. There are a variety of FIU types (see Figure 2).

- Some are defined **business units**, in which a team of senior investigators is assigned to provide deeper insight into specified financial crime risk processes.
- Some are defined more clearly as **technical solutions** that bring together FCRM systems across geographical and risk-management silos.
- An FIU can be provided by an **institution**, or can be set up as a governmental or regional unit that bridges FCRM silos or countries.

**Figure 2: Differing definitions of the Financial Intelligence Unit**

*Source: Chartis Research*
In the remainder of this report we will focus on the challenges and benefits of bridging silos and countries with a technology infrastructure (shown in the red boxes in Figure 2), although clearly this will come with its own organizational functions too.

Several Tier 1 FIs in the US and the European Union have built their own technological FIUs in recent years. Notably, a number of ambitious centralization projects have been launched, aiming to bring together fraud, sanctions and AML systems across silos and geographies (see Figure 3).

Centralization, automation and protection

A basic and important goal of these FIU projects is to eliminate silos between different areas of FCRM to increase the accuracy of investigations. Many FIUs are still in-flight, and the FIs concerned have yet to fully realize the benefits. Nevertheless, it is already clear that they offer potential advantages over existing siloed approaches to FCRM (see Figure 4 for a summary).

Figure 3: Key FIU projects in Europe and the US

Source: Chartis Research
Figure 4: FIUs offer advantages over traditional siloed approaches to financial crime risk management

Aggregated case data, advanced analytics and better detection.
In a next-generation FIU, investigators can uncover criminal activity based on meaningful patterns in FIs’ lakes of data, using tools such as Machine Learning.

Building an entity view.
When investigators process alerts in a centralized FIU, they can analyze a particular entity in the context of a host of historical behavioral data that is available to them. This gives them a clearer view of the nature of entities, and makes decisions about them quicker and easier.

Long-term data quality and improvements.
FIUs can reduce the overall number and complexity of duplicated data feeds, and improve data lineage and traceability. It’s a virtuous cycle too, with better investigative data fed back into the system to improve the overall quality of data over the longer term.

Better experience for staff and customers.
An FIU system should produce fewer false positives, so traders are less likely to be pulled away from their jobs for the wrong reasons. Customers are also likely to appreciate having fewer of their payments declined on often spurious grounds.

Scalable support.
We would see ‘FIU utilities’ emerge more broadly (so far the phenomenon is restricted to Tier 1 FIs). In this context, a high-performing FIU could become the gold standard that clients and regulators will come to expect from financial providers.

Source: Chartis Research
4. Building the FIU: the technology approach

Chartis believes that a strong and effective technology infrastructure is a useful place to start in bridging organizational and geographic silos. Recent advances in case management functionality and data processing have made this possibility more realistic.

Outlining a complete roadmap for an FIU is a lengthy undertaking – it can be a highly complex activity that will differ by FI. Nevertheless, we believe that within the technology-infrastructure approach there are three solid initial blocks on which FIs should build their FIU strategy:

- Clear, supportive leadership.
- A coherent data infrastructure and strategy.
- Effective case management functionality to unify the system.

Supportive leadership

An effective FIU must have well-defined lines of responsibility – before a line of code is written or a module installed, those running the project must know who is responsible for it, and how the organization will benefit from implementing it. Projects designed to bridge silos often stall because those involved are unclear about who is responsible for what, with many preferring to stick with the status quo rather than make potentially radical changes.

An FIU is an important project that cuts across business units and regions, so support and sponsorship from the very top of the organization are essential. To date, those in charge of the FIU have typically reported to the CRO via compliance departments (see Figure 5). In recent years, however, a number of banks have chosen to put their Chief Compliance Officer in charge of the FIU, reporting directly to the CEO. This highlights the growing importance of the compliance department within their organizations.

Outlining a complete roadmap for an FIU is a lengthy undertaking – it can be a highly complex activity that will differ by FI. Nevertheless, we believe that within the technology-infrastructure approach there are three solid initial blocks on which FIs should build their FIU strategy:

- Clear, supportive leadership.
- A coherent data infrastructure and strategy.
- Effective case management functionality to unify the system.

Supportive leadership

An effective FIU must have well-defined lines of responsibility – before a line of code is written or a module installed, those running the project must know who is responsible for it, and how the organization will benefit from implementing it. Projects designed to bridge silos often stall because those involved are unclear about who is responsible for what, with many preferring to stick with the status quo rather than make potentially radical changes.

An FIU is an important project that cuts across business units and regions, so support and sponsorship from the very top of the organization are essential. To date, those in charge of the FIU have typically reported to the CRO via compliance departments (see Figure 5). In recent years, however, a number of banks have chosen to put their Chief Compliance Officer in charge of the FIU, reporting directly to the CEO. This highlights the growing importance of the compliance department within their organizations.

4 Such as those conducted by Chartis for its FCRM research (see, for example, Financial Crime Risk Management Systems 2016; Update Report).
FIUs will require a data lake in which to develop entity views. Those FIUs that take the ‘dynamic’ route may require an additional data repository to store and source entity information that can be aggregated quickly into a given view.

Beyond this, the FIU’s data strategy should support a range of analytical capabilities, including:

- **Search-based investigation and case management functionality.** Investigators should be able to drill down into data about individuals and groups of entities. An example might be viewing a network of highly connected customers that have generated a series of transaction monitoring alerts that were marked as false positives when they were triaged in isolation. Only by looking at the aggregate view of these alerts, and the connections that exist between the customers, does the system spot the suspicious activity.

- **Reporting, including user-driven reports.** Reporting will typically involve standardized templates such as SARs, but may also involve custom reports (on a new financial crime trend, for example, that needs to be raised with senior analysts).

- **Data quality reporting.** ‘Dirty’ or poor-quality data is more likely to be hiding in large volumes of information. Incomplete and inconsistent data can lead to misidentified customers and duplicate payments. FIs can avoid this issue by reporting data quality ‘profiles’.

- **Rule building, simulation and advanced analytics.** With a centralized repository of financial crime analytics, FIs can simulate the effects of changes in organizational policy or the analytics themselves. Advanced stochastic techniques (such as graph analytics) can be used to resolve entities more effectively. This could enable FIs to analyze the ‘distance’ between entities, in terms of their similarity (‘Is Entity A actually the same individual as Entity B?’) and how much risk there is in transacting with them (‘through how many connections is Entity A related to sanctioned Entity B?’).

  In addition, if FIs can build their own rules they can address new forms of financial crime as they emerge. By segmenting and analyzing groups of entities in terms of their behavior, for example, an FI could identify an entity that is acting unusually, and provide inputs into rules-based analytics (such as ‘apply Rule X to Behavioral Segment Y’).

Increasingly, FIs now want to tune their own models and analytics. Solution developers and vendors can enable this either by enabling them to change the weights and features involved in an analytics set, or by allowing them to build their own rules within programming languages such as R and Python.

**Effective case management**

Of the analytical capabilities highlighted above, arguably the most important component is case management functionality. This is the coordination and integration layer of an FCRM solution, the vital unifying layer that brings together the various inputs to an FIU (see Figure 6).

Typically, case management solutions are customized workflow engines, delivering analytics and tasks to users, including alert management, selection, case investigation, resolution and regulatory reporting.

One challenge of a centralized FIU is keeping ‘business as usual’ processes running while being able at the same time to look across silos. Case management can be used to build a ‘two-layer’ system in which individual FCRM silos are kept broadly separate for those who are not part of the FIU, while one-click access enables a more advanced investigations process that accesses the information aggregated across silos. By doing this FIs can create a central repository of all fraud and financial crime cases across the organization.

This ensures that known ‘bad cases’ can be used to inform future risk-based decisions. Take a transaction monitoring alert generated by a first-line risk management system, for example. If the customer at the center of this alert has been previously connected to an application fraud case, then the alert is much more likely to be genuine.

Assuming the FI has the right level of business intelligence and reporting capabilities in place, this enables multiple sources of data to be aggregated, so representatives of multiple lines of business can engage with investigations.

---

2 Anti-fraud processes that do not need further automation, for example, can be kept running without overcomplicating them with access to FIU capabilities.
Figure 6: Case management as a unifying layer in the FIU

Send money, save money, or spend money.

**Figure 6: Case management as a unifying layer in the FIU**

**Outputs**
- Reporting layer

**Analytics**
- Global search
- Tactical alert generation
- Thematic reviews
- Cross-border alert aggregation
- Advanced analytics/AI

**Case management**
- Case management
- Alert management

**Processing**
- Batch processing tier
  - ETL
  - Entity extraction
  - Network build and filter
  - Scoring

- Dynamic processing tier
  - ETL
  - Entity extraction
  - Network build and filter
  - Scoring

**Point solutions**
- Financial crime
  - KYC
  - Transaction monitoring
  - Anti-fraud
  - Payment screening

- Compliance
  - Market abuse
  - Communications monitoring
  - Sanctions monitoring

**Unified data**
- Data layer

**Inputs**
- Internal data
- External data

*Source: Chartis Research*
5. Conclusion: three key steps

By providing a clear level of oversight for FCRM systems, FIUs can improve FIs’ insight and investigative capabilities, and help to tackle financial crime and reduce costs. But technology-focused FIUs can be complex, multi-layered implementation projects that FIs should approach tactically step by step. And to prevent costs spiralling out of control they must also remain focused on overall business, data and technology requirements.

A successful technology-driven FIU is built on three main foundations: effective organization, strong data infrastructure and powerful case management functionality. By creating effective entity views in an FIU, time-consuming processes can be passed over to automated systems, and investigators can be moved off repetitive tasks such as SARs reporting and onto more effective and complex investigative work.

Finally, if FIs can adapt how they analyze and use the data surfaced through an FIU, they can open up other potential applications. The FIU could form a useful foundation from which to address a wider range of use cases, such as supporting cybercrime investigations, addressing credit risk, or implementing more effective trader surveillance. FIUs even have marketing value: by advertising their impregnability and investigative skill, FIs can gradually build on their investment, and keep the regulators at bay a little longer.
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

Financial Crime Risk Management Systems: Enterprise Fraud; Market Update 2018

Financial Crime Risk Management Systems: Know Your Customer; Market Update 2018


Technology Solutions for Credit Risk 2.0, 2018

Spotlight: Artificial Intelligence in finance – a primer

Spotlight on Cryptocurrencies

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