Ovum
TMT intelligence | informa

Ovum Decision Matrix: Selecting an Anti-Financial Crime Solution, 2017–18

Publication Date: 14 Dec 2017 | Product code: ENV004-000002

Matthew Heaslip

Summary

Catalyst

As banks face the ever-changing landscape of financial crime threats, the role of anti-financial crime platform providers is becoming increasingly important. This in turn makes the task of identifying, assessing, and engaging the most appropriate anti-financial crime platform provider more critical than ever.

This Ovum Decision Matrix (ODM) provides a broad and detailed assessment of 10 major providers that have established a strong presence supporting banks' anti-financial crime capabilities. It provides a comprehensive view of the anti-financial crime competitive market landscape. The ODM considers a range of capability areas across both risk and compliance, including "know your customer" (KYC), anti-money laundering (AML), watch-list screening, and transaction fraud prevention, along with broader general analytics strengths, for example. The compliance and operations costs to banks from tackling financial crime threats and regulation are already significant, so platforms need to ensure fraud prevention and compliance requirements can be managed efficiently, and that they can absorb new threats and regulations as they arrive.

Ovum view

Recent changes in the threat dynamics of financial crime have left the banking industry with a dilemma, with some having been forced to exit higher-risk markets or submarkets. Cybercriminals and fraudsters are deploying increasingly sophisticated techniques to launch less frequent but ever larger attacks, particularly via less defended routes previously assumed to be lower risk. The huge Bangladesh Bank attack in February 2016, which saw $101m successfully withdrawn fraudulently via a malware-engineered SWIFT request, has opened eyes to the emergent threat.

To respond to these threats, it is vital for banks to have an effective IT and technology strategy to enhance and strengthen their whole-business, enterprise-wide anti-financial crime capabilities. Ovum believes that as banks struggle to meet these technology challenges, a greater proportion will be driven to build long-term strategic relationships with anti-financial crime platform providers.

Given the substantial direct and indirect costs inherent in financial crime, the stakes are high, and so the support provided by platform providers is becoming critical to ensure an effective defense against the emerging threats. Some of those vendors are countering the emergent and legacy threats through new techniques, such as moving to integrated financial crime capabilities. There are also wider industry efforts to leverage advances in analytics (e.g., new data approaches, the move to machine learning, and AI) as part of the effort to improve both the effectiveness (e.g., reducing false positives while increasing detection rates) and the efficiency (e.g., enhancing investigation and reporting flows) of banks' anti-financial crime operations. As a result, making the correct choice of partner – or partners – will be one of the most important decisions to be made by bank executives.

Key findings

- BAE Systems, FICO, and NICE Actimize offer market-leading anti-financial crime platforms.
- Oracle and SAS have high-quality all-round platforms that are strong challengers.
- Temenos' platform has an impressive compliance-related set of capabilities.

- ACI's wider specialism in payments positions its platform as a key retail threat option.
- IBM's platform has top-quality analytics and is suited to best-in-market third-party modules.
- LexisNexis Risk Solutions' platform should be considered on the AML/BSA compliance side for both its platform and supporting data sets.
- Smaller financial institutions should consider Intellect to meet regulatory requirements quickly.

Vendor solution selection

Inclusion criteria

The list of participants assessed in this report is not intended to be exhaustive; however, Ovum believes it is representative and offers readers an in-depth analysis of the leading anti-financial crime platform providers. Inclusion within the report itself highlights that a platform provider is considered worthy of consideration by Ovum. Ten anti-financial crime platform providers are considered in this report. These are listed in Table 1.

The decision to include a provider for evaluation in this report is based on the following criteria:

- The platform provider must be judged in an initial assessment by Ovum as having mid- to long-term potential and a sufficient degree of focus on the banking sector.
- The provider must offer a range of its own solutions to the banking industry that encompasses most of the following categories: AML/KYC, customer behavioral monitoring/analysis, watch-list management, application fraud, payments fraud, multichannel interaction, regulatory/SAR reporting, and case management/investigation. Ovum's definition of these categories is included in the report. The provider should also be active in pursuing opportunities on a stand-alone basis, (i.e., marketing anti-financial crime solutions separately to core banking platforms).
- The participants must provide Ovum with sufficient information to allow an accurate assessment, including the completion of Ovum's request for information (RFI) document, together with a detailed briefing.

Exclusion criteria

- The vendor did not wish to participate in the report. Vendors, for various reasons, do not always want to engage in analyst reports, especially if the emphasis of their product strategy has changed or the company is heading in a new direction.
- The product offers some anti-financial crime features, but these are not central to the core offering at present.
- The product is very new to market and is not yet commercially proven.
- The provider is still reliant upon its domestic market and has not yet proven itself capable in a global context.

Methodology

Based on Ovum's initial assessment and knowledge of the trends in technology investment in the anti-financial crime platform market globally, a range of vendors were invited to respond to a detailed

request for information (RFI). This required them to provide data and supporting documentation relating to three primary areas: technology, execution, and market impact. In addition to the RFI, the vendors were invited to provide briefings on their solutions. This was further supplemented by Ovum's own data and information sources, to provide a level of validation.

The analysis of these three primary areas was based on a scoring assessment exercise with various sub-criteria. For each response within the RFI that aligned with the respective sub-criteria, vendors were rated on a 10-point scale based on a consistent set of best-practice criteria or benchmarks defined by Ovum.

The overall outcome for each sub-criteria is a result of the weighted sum of questions and analysis of the digital banking platforms. Weightings are based on analysis of the importance of each criterion in the selection process of an anti-financial crime platform by a financial institution.

Technology assessment

In this assessment dimension, Ovum analysts develop a series of features and functionality that would provide differentiation between the leading solutions in the marketplace. Ovum also considers actual client deployments to show real-world uptake and operational capability. The criteria groups identified for anti-financial crime are as follows:

- **KYC/CDD:** Features aimed at ensuring banks know who their customers are (KYC), and performing enhanced customer due diligence checking and management.
- **Anti-money laundering (AML):** Systems, processes, and training available to support the ongoing mitigation and management of money-laundering risk.
- **Watch lists:** Processes surrounding the confirmation that individuals are not subject to sanctions or terror/crime watch-list monitoring.
- **Integrated approach:** Bringing together data from across organizations to provide both an overall understanding of individual customers and an enterprise-wide defense of financial institutions against fraud threats.
- **Transaction fraud prevention:** Systems intended to monitor for and prevent fraudulent payments or applications, across a range of business lines.
- **Analytics:** An assessment of the analytics capabilities embedded within the platform, including the use of latest technologies and approaches.
- **Case management and reporting:** Supporting the investigation of suspected financial crime cases and the creation and submission of regular or ad hoc reports for regulatory or internal purposes.

Execution assessment

In this dimension, Ovum analysts review the capability of the solution in the following areas:

- **Maturity:** The stage that the platform is at in the maturity lifecycle is assessed here, relating to the maturity of the overall technology/service area in meeting the full range of financial crime–related threats and tasks.
- **Innovation:** Innovation can be a key differentiator in the value that an enterprise achieves from a software or services implementation.

- **Partners and development strategy:** Weighing the vendor's use of R&D and partners to strengthen and further improve its anti-financial crime offering, as well as related delivery and support capabilities.
- **Deployment and maintenance:** Referring to a range of assessed criteria and information, Ovum assesses the deployment and integration process along with upgrades and maintenance.
- **Training and support:** Financial crime is a dynamic, ever-changing threat, so ensuring bank staff fully understand the risk and how to get the best out of the software available is a key concern.

Market impact

The global market impact of a solution is assessed in this dimension. Market impact is measured across five categories, each of which has a maximum score of 10.

- **Market presence:** This looks specifically at the relative scale of each vendor within the anti-financial crime market, including client base, product portfolio, and specialist staff numbers, among other metrics.
- **Market growth:** Compares the recent success of each anti-financial crime platform, using a range of factors including number of client wins and revenue growth.
- **Anti-financial crime focus:** Many of the vendors have large portfolios covering numerous sectors, so Ovum assesses the relative scale and importance to each group of anti-financial crime products.
- **Geographic coverage:** Ovum assesses a mixture of the national and regional client base of each vendor, along with their support and development footprint.
- **Group organizational scale:** This weighs each business's overall size at group level, particularly by revenue and staff, to indicate the total resources they have available.

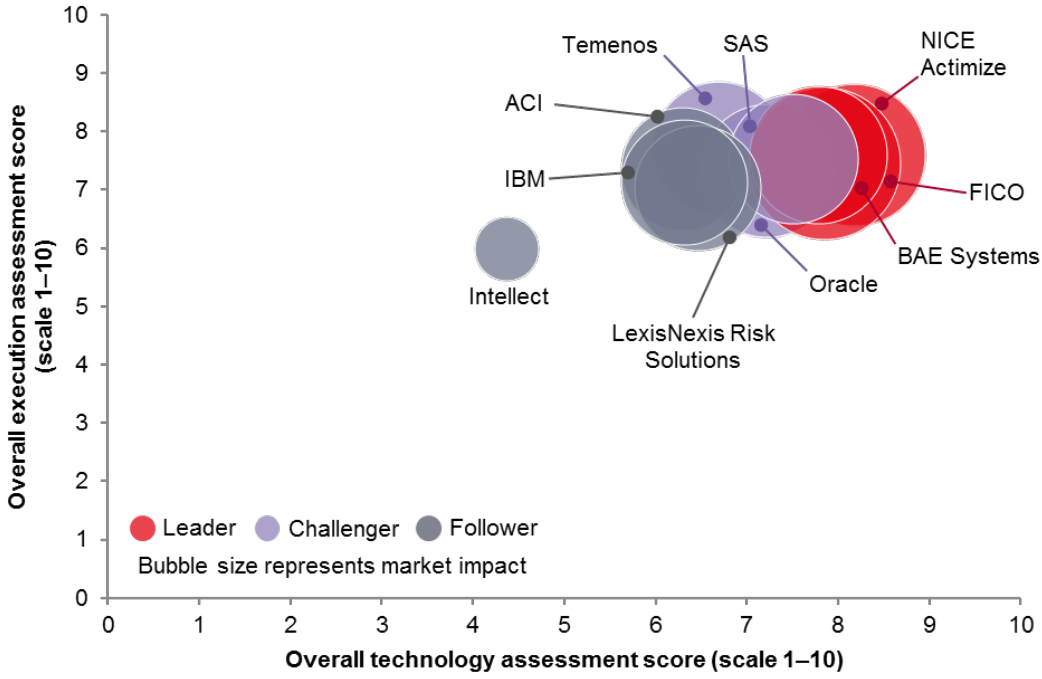
Ovum ratings

- **Market leader:** This category represents the leading solutions that we believe are worthy of a place on most technology selection shortlists. The vendor has a commanding market position with a product that is widely accepted as best-of-breed.
- **Market challenger:** The solutions in this category have a good market positioning and offer competitive functionality, in some cases with market-leading capabilities in specific areas. They should be considered during a technology selection process.
- **Market follower:** Solutions in this category are typically aimed at meeting the requirements of a particular kind of customer. As a tier-one offering, they should be explored as part of the technology selection.

Market and solution analysis

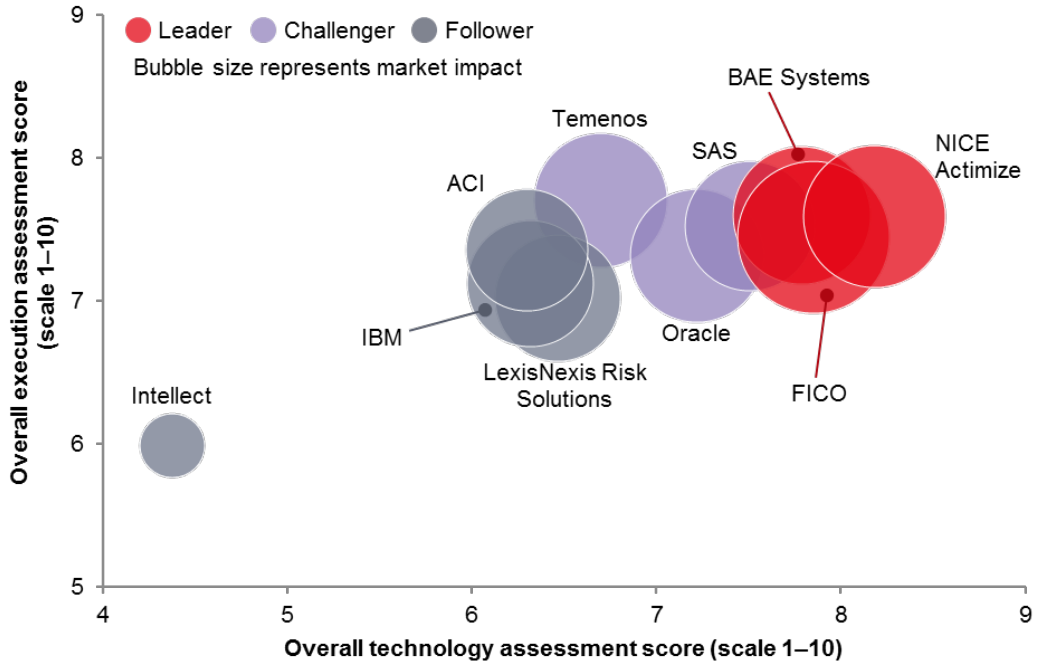
Ovum Decision Matrix: Anti-financial crime platforms, 2017–18

Figure 1: Ovum Decision Matrix: Anti-financial crime platforms, 2017–18



Source: Ovum

Figure 2: Expanded view of Ovum Decision Matrix: Anti-financial crime platforms, 2017–18



Source: Ovum

Table 1: Ovum Decision Matrix: Anti-financial crime platforms, 2017–18

Market leaders	Market challengers	Market followers
BAE Systems	Oracle	ACI
FICO	SAS	IBM
NICE Actimize	Temenos	Intellect
		LexisNexis Risk Solutions

Source: Ovum

Market leaders: BAE Systems, FICO, NICE Actimize

BAE Systems, FICO, and NICE Actimize lead the market, with the highest average scores across the three areas of consideration. The key characteristic separating the leaders from the market challengers is their consistently strong all-round performance in offering financial institutions enterprise-wide platform coverage. Each market leader also has its own best-in-market features, such as FICO's analytics, NICE Actimize's enhanced customer due diligence, and BAE Systems' investigative network analysis. All three vendors also maintain a sizable all-round market presence, including the number of services offered, geographic coverage, and client base. These are the key vendors that financial institutions should short-list, particularly when a single supplier is required to provide enterprise-wide, multi-threat coverage.

Market challengers: Oracle, SAS, Temenos

The market challengers all possess many attributes similar to the market leaders, putting those vendors under significant pressure for their places. SAS and Oracle both offer the same style of all-around coverage, with very respectable blended averages of 7.2 and 7.1, respectively. These two challengers are market leaders in analytic capabilities, and generally offer a high standard in most categories. Temenos, in contrast, is a more specialist provider, with a strong market position for KYC/AML/watch-list-screening capabilities. As a result, the vendors appeal to slightly different markets. SAS and Oracle should be considered for short-listing alongside the market leaders for all-round coverage, whereas Temenos should be short-listed by financial institutions looking for specific onboarding- and compliance-related products.

Market followers: ACI, IBM, Intellect, LexisNexis Risk Solutions

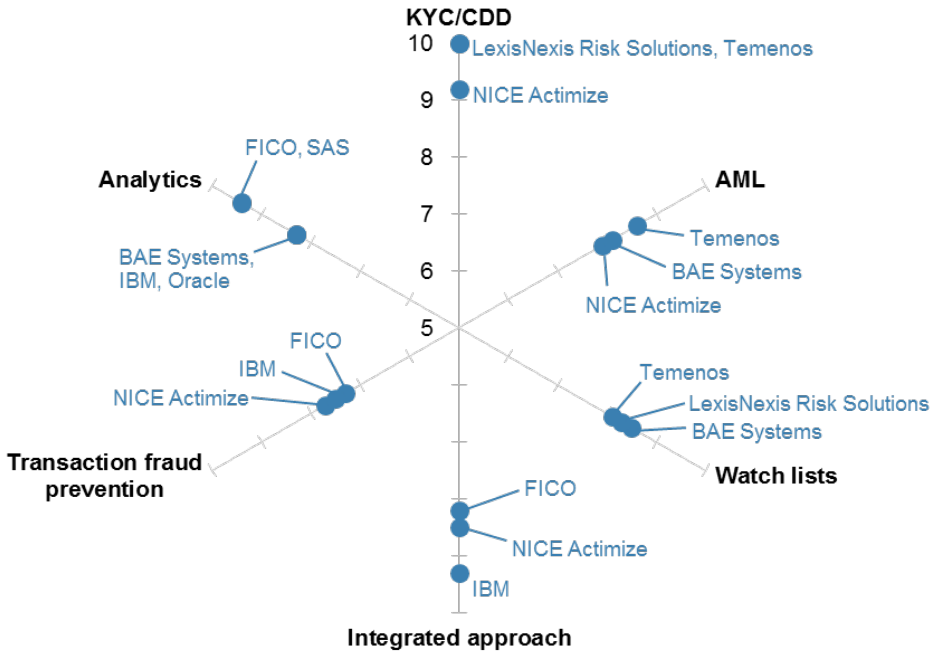
The market followers are a diverse group, with a range of vendors that should still be considered for short-listing by financial institutions, although in different ways. Backed by its wider expertise and knowledge across the payments fraud space, particularly in its retail merchant fraud prevention business, ACI is a leader in countering consumer payment-related fraud threats. ACI should therefore be considered for short-listing by retail banks in particular. IBM has taken a flexible approach to all-round coverage, using its expertise in systems integration and wide network of technology partners to offer financial institutions the opportunity to exploit specialist market-leading third-party modules. For financial institutions looking for a new, highly flexible approach to enhancing key aspects of their defenses, IBM should be actively considered. LexisNexis Risk Solutions ranks very strongly on its

risk-scoring, customer-screening, and AML/BSA compliance-related services, so should feature on the short lists of institutions looking to strengthen their capabilities in those areas. Although it is a relative newcomer to the space, Intellect offers smaller banks the opportunity to quickly put in place all-round threat coverage, via an easily deployable platform.

Market leaders

Market leaders: Technology

Figure 3: Ovum Decision Matrix: Anti-financial crime platforms, 2017–18, Market leaders – technology

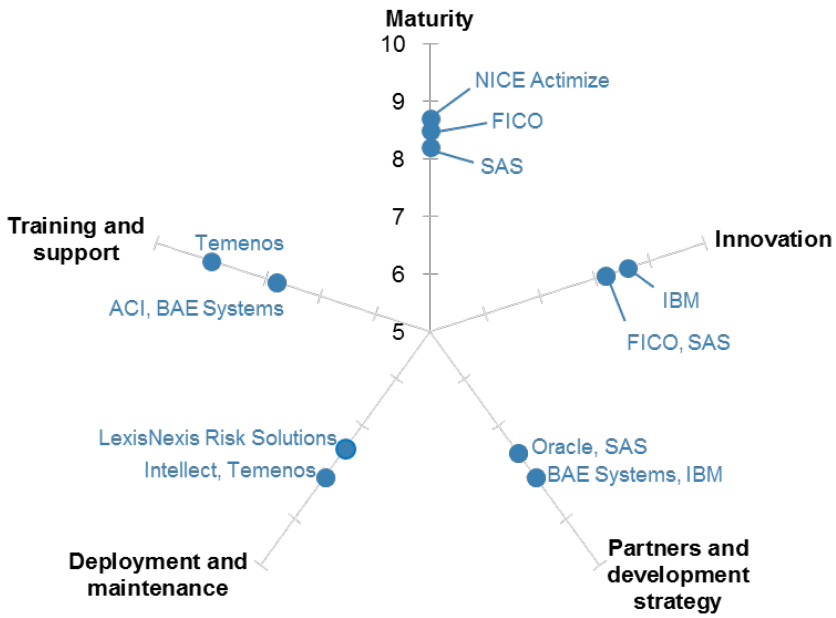


Source: Ovum

A range of key technological areas should be considered when looking at enterprise-wide coverage. These split broadly between three groups: compliance- and onboarding-related areas (KYC, AML, watch list), ongoing multichannel transaction fraud prevention, and background analytics and integration capabilities. Not all vendors target all subsegments, with Temenos and LexisNexis Risk Solutions, for example, specializing more in the compliance and onboarding side of the market. This highlights the importance for financial institutions of carefully considering the full range of platforms on offer when looking to enhance or replace specific systems.

Market leaders: Execution

Figure 4: Ovum Decision Matrix: Anti-financial crime platforms, 2017–18, Market leaders – Execution

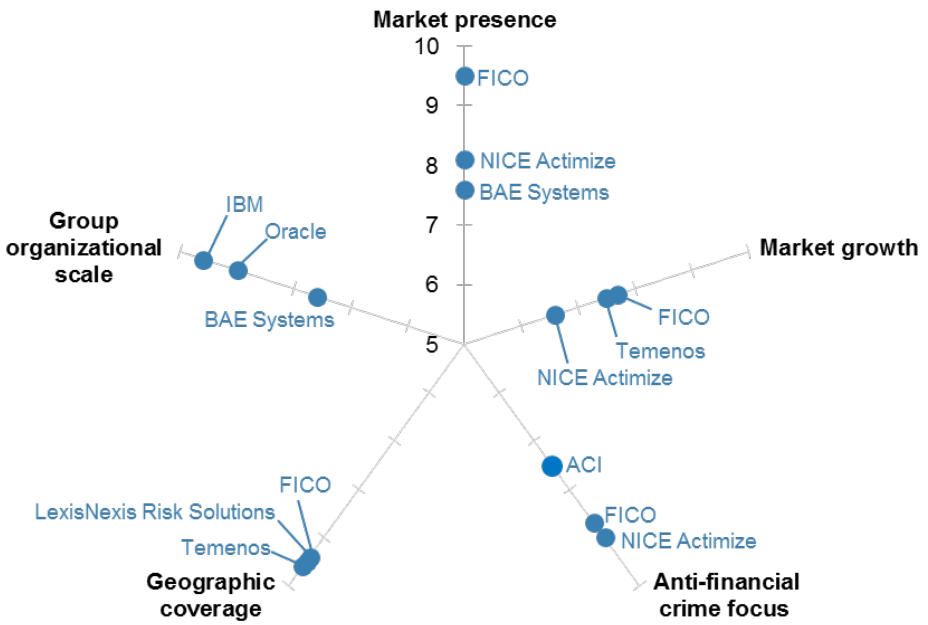


Source: Ovum

The execution dimension helps us better understand how well a vendor is positioned to meet the many deployment, integration, and maintenance needs of modern organizations. It also considers how well vendors are planning for the future and building third-party technology partner relationships to help meet emerging challenges. The vendors operating in the anti-financial crime platform market generally offer high overall execution standards, although some stand out in individual aspects. IBM and SAS, for example, have particularly strong visions for the future of the market and how to get there, and have the resources in place to follow that path. Likewise, Temenos stands out for its high-quality all-round deployment, maintenance, training, and support options, although ACI, BAE Systems, and Intellect also do well in those areas.

Market leaders: Market impact

Figure 5: Ovum Decision Matrix: Anti-financial crime platforms, 2017–18, Market leaders – Market impact



Source: Ovum

The anti-financial crime platform market includes a range of vendors, which come in a variety of different shapes and sizes. There is a sharp divide, for example, between the large, diversified mega-groups (BAE Systems, IBM, Oracle), which may include large financial services divisions, and those smaller competitors for which anti-financial crime solutions are a significant business segment (ACI, FICO, and NICE Actimize). Reflecting the high global demand for their services at the current point in time, most vendors have good geographic coverage and are recording strong market growth figures. While most vendors hold strong positions in particular market segments, Ovum weighs their overall platform footprint, with the market leading platforms from BAE Systems, FICO, and NICE Actimize all holding established positions in the total market.

Vendor analysis

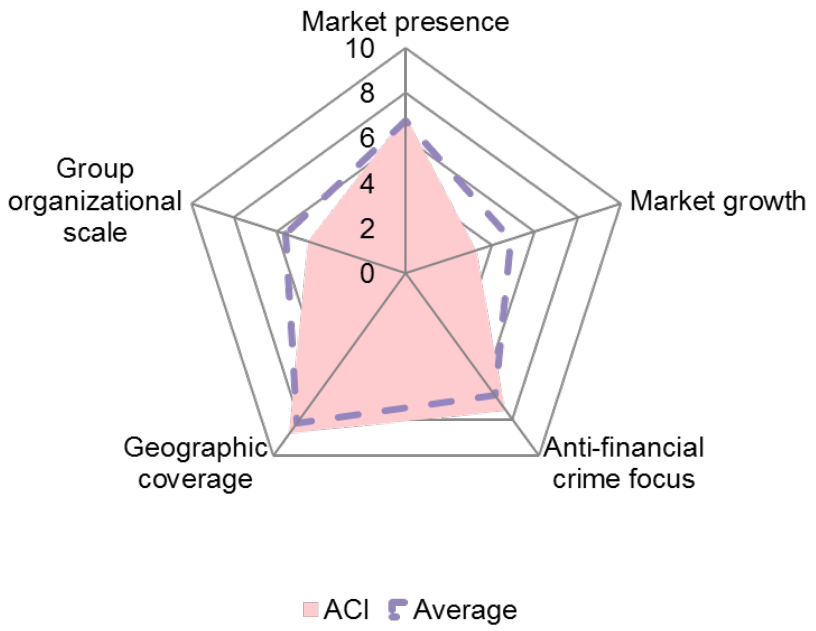
ACI Worldwide

Background

ACI is a publicly listed global financial services technology vendor, headquartered in the US and founded in 1975, with a pronounced specialism in payments. Part of the UP Payments Risk Management suite, the company's anti-financial crime platform – ACI Proactive Risk Manager – was first launched in 1997 and has since established a broad client base. ACI has anti-financial crime research and development centers in the US, UK, Romania, and South Africa.

Market impact assessment

Figure 6: ACI – Market impact

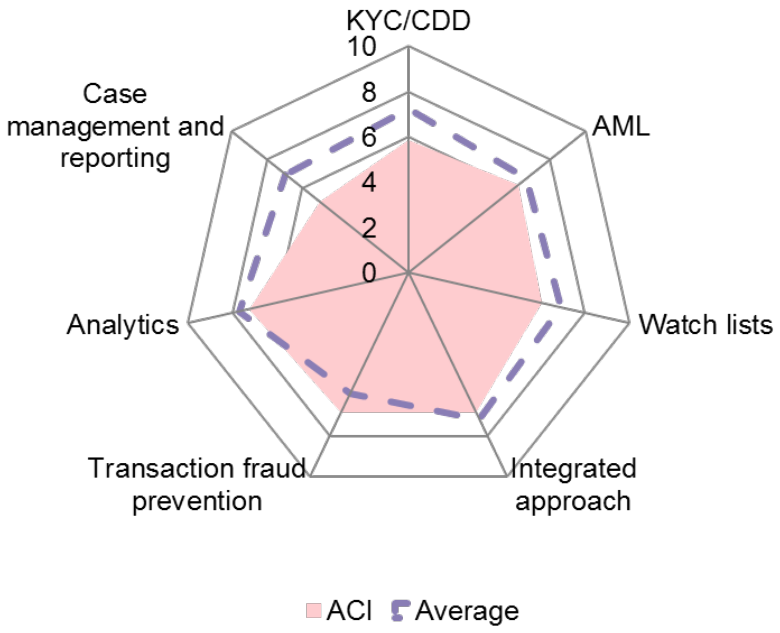


Source: Ovum

Anti-financial crime services, particularly those related to ACI's wider specialism in payments, form an important segment of the company's overall business. Exploiting its expertise in payments, ACI has established itself firmly as an important player in the market. ACI Proactive Risk Manager has clients in 40 countries around the world and is currently deployed in a number of languages, including English, Spanish, and Portuguese. ACI Worldwide as a group is a large organization, with total revenues of over $1bn in the last financial year, although it is more modest in overall scale than some of the mega-groups in the field.

Technology assessment

Figure 7: ACI – Technology assessment



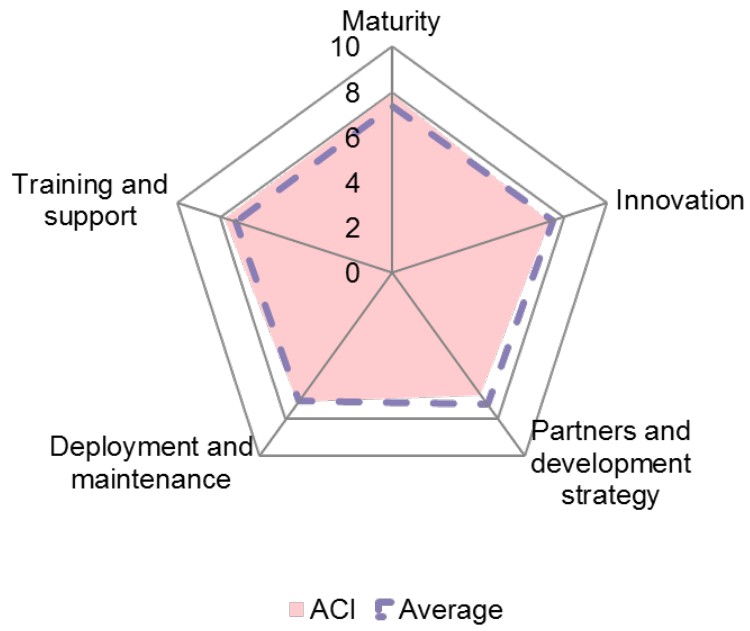
Source: Ovum

Proactive Risk Manager's platform provides a broad selection of modules, for an all-round set of anti-financial crime capabilities. Exploiting the company's expertise in payments, particularly on the merchant side, ACI has a strong, fully scalable retail payment fraud prevention proposition, making use of a wide range of data sets while supporting real-time, low-latency transaction monitoring and, where necessary, intervention. The platform is fully scalable, with a client base of financial institutions of all tier sizes. The company uses a range of real-time and near-real-time rule-based monitoring, with machine learning embedded to review and improve ongoing accuracy, with reducing potential inconvenience for end customers firmly in mind.

ACI offers a well-rounded set of case management and reporting capabilities, with 20 parametrizable, ready-made reports on the Proactive Risk Management platform and additional reports available through the Case Management module. This includes those for regulatory purposes, such as SARs, with support available to enhance them through the use of third-party tools. With real-time data access, ACI's graphical dashboards offer financial institutions' case officers an easy-to-review and customizable experience.

Execution assessment

Figure 8: ACI – Execution assessment



Source: Ovum

Since its launch in 1997, the Proactive Risk Manager platform has built a strong client base, and it is now one of the more mature propositions in the market. ACI has a focus on research and development, as well as on utilizing technology partners to enhance its offering, and is already proactively looking ahead to the next generation of threats, such as those involved with the growth of instant/immediate payments. The company provides a market-leading set of training and support options, including a range of e-learning courses through ACI's Learning Management System. The platform is available through various deployment options, although most clients currently opt for on-premises.

Recommendation: ACI is a market follower

ACI Proactive Risk Manager offers financial institutions a rounded set of anti-financial crime capabilities, with a strong proposition for dealing with the threat of retail payments fraud. ACI is therefore a vendor that financial institutions should consider when exploring their technology options, particularly those concerned about existing and emergent payment threats.

BAE Systems

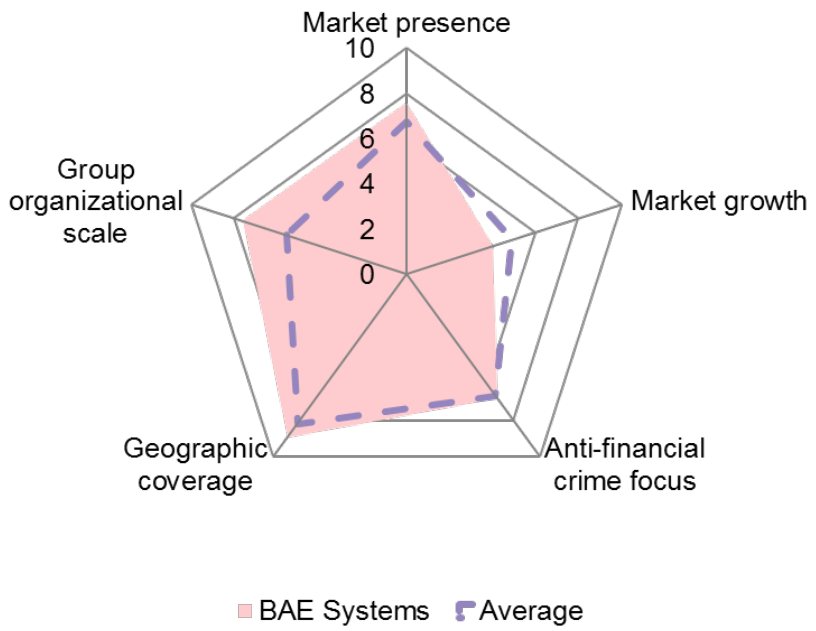
Background

BAE Systems is a publicly listed global defense, aerospace, and security company. The BAE Systems Applied Intelligence division is headquartered in the UK, with offices across Europe, North America, and Asia, and is focused on solutions related to AML compliance, anti-fraud, and cybersecurity. NetReveal, the core anti-financial crime platform from BAE Systems, was launched in 2005 and has an established client base across a wide range of geographies. BAE Systems Applied Intelligence

maintains R&D centers in the UK, Ireland, and Malaysia, with support engineers based in the US, Australia, and Poland in addition to those previously mentioned locations.

Market impact assessment

Figure 9: BAE Systems – Market impact

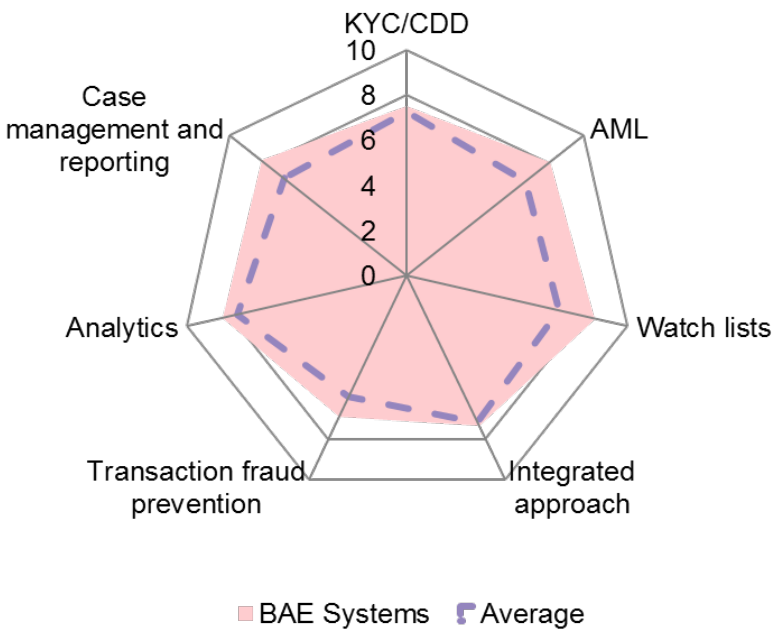


Source: Ovum

As a large diversified company with group revenues of £17.8bn (c.$23.5bn) in 2016, services related to anti-financial crime account for a comparatively small segment of BAE Systems' revenue. Nonetheless, BAE Systems Applied Intelligence has built a sound position within the market, with its core anti-financial crime platform in operation with clients across Canada, the US, Europe, the Middle East, Africa, and Asia. BAE Systems has not recorded quite the same growth rate as seen elsewhere, which may be a reflection of its brand being so strongly associated with defense rather than financial services.

Technology assessment

Figure 10: BAE Systems – Technology assessment



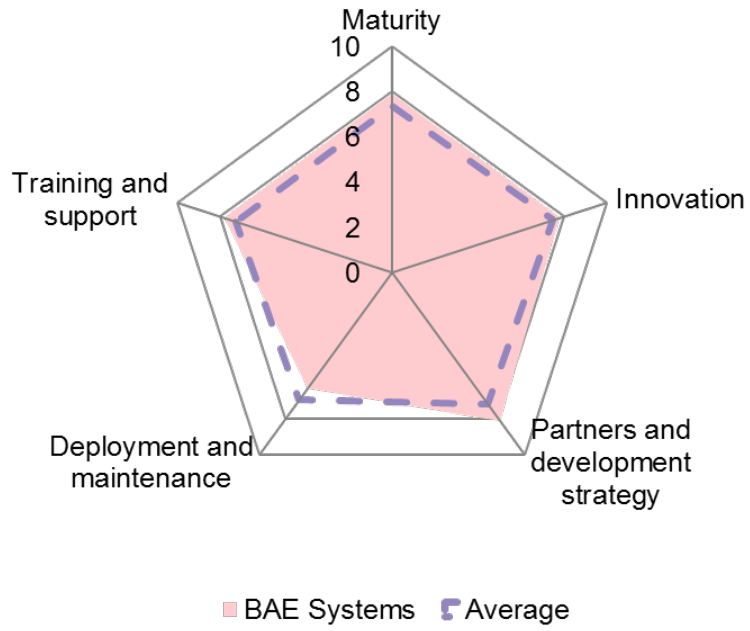
Source: Ovum

BAE Systems' NetReveal platform includes a wide range of anti-financial crime modules supporting a broad set of capabilities for financial institutions. NetReveal has its own financial crime data model designed to collect and sort information from institutions' different source systems, but also operates effectively with a range of legacy and third-party data sources and compliance engines. That data is then fed through the platform's risk-scoring modules, with suspicious entities and transactions triaged and sent on for investigation.

Making use of other divisions' experience in network analysis and watch-list management, BAE Systems provides high-quality investigation and customer-monitoring capabilities. This includes strong network visualization and alert enrichment, with numerous automated elements, to improve the speed and effectiveness of the decision-making process. The NetReveal platform includes dedicated out-of-the-box modules, such as Sanctions and PEP Screening, as well as CDD, but it is also readily configurable to support financial institutions' FATCA and other regional regulatory compliance reporting and management requirements.

Execution assessment

Figure 11: BAE Systems – Execution assessment



Source: Ovum

BAE Systems has a clear innovation strategy, with a strong set of priorities aimed at enhancing the predictive analytics and machine-learning elements of its NetReveal modules to help further reduce false positives and enhance its investigative capabilities. BAE Systems also looks to provide additional APIs to help clients make better use of individual modules within legacy frameworks. It offers a strong all-around set of training and support options to help financial institutions meet their requirements effectively. The NetReveal platform and its modules are all available as a SaaS offering.

Recommendation: BAE Systems is a market leader

BAE Systems' NetReveal is one of the leading anti-financial crime platforms in the market. NetReveal offers financial institutions of all sizes high-quality overall coverage, with notable strengths in its investigative and case management capabilities. Ovum recommends that financial institutions short-list BAE Systems' NetReveal as a competitive anti-financial crime platform solution.

FICO

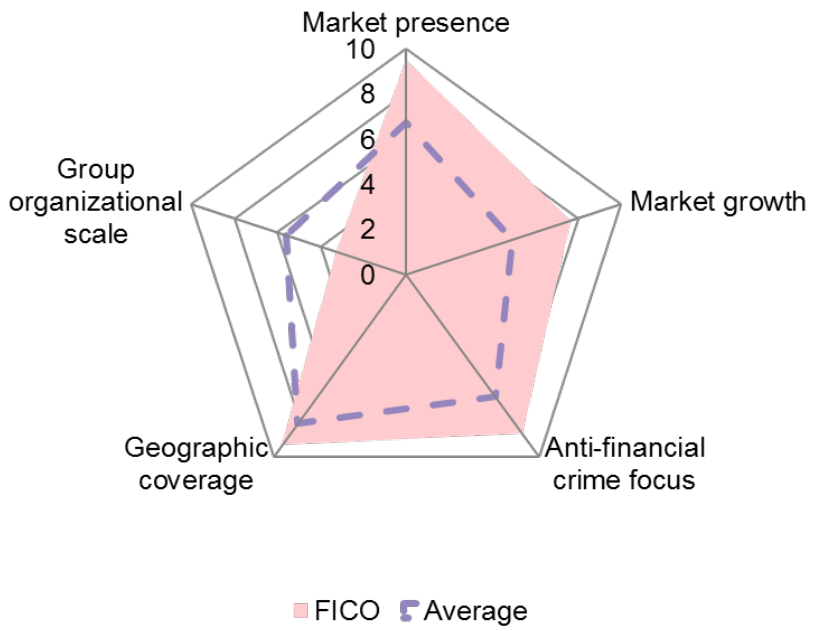
Background

FICO is a publicly listed financial services–focused vendor headquartered in the US, with offices in 90 countries around the world. FICO was founded in 1956 and enhanced its anti-financial crime capabilities through the acquisition of Tonbeller in 2015, which brought with it a range of compliance-related solutions and capabilities. FICO's Falcon enterprise fraud platform and Tonbeller's Siron Anti-Financial Crime Solutions work side by side, with the split a reflection of the 2015 acquisition. Both parts of the overall offering maintain sizable and diverse client bases and have recorded strong

growth figures in recent years. FICO has two anti-financial crime platform R&D centers – one in the US and the other in Germany.

Market impact assessment

Figure 12: FICO – Market impact

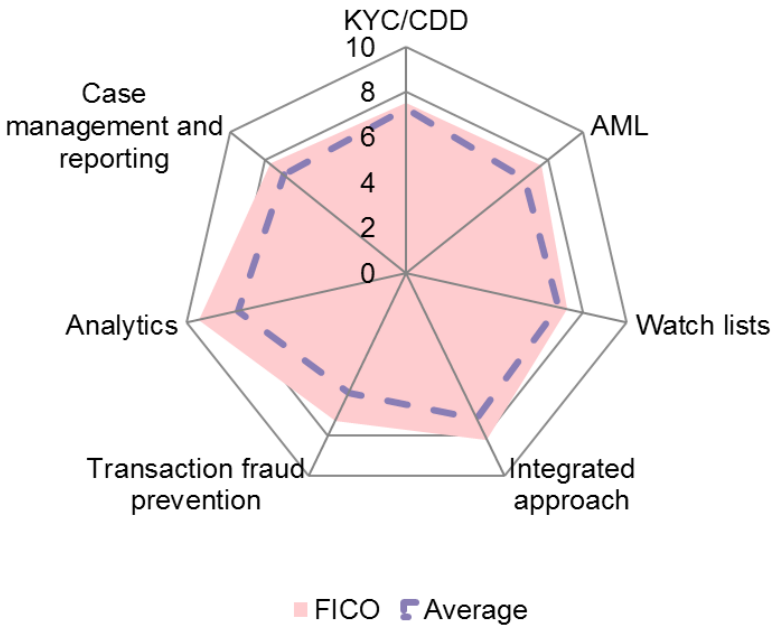


Source: Ovum

Benefiting from its acquisition of Tonbeller in 2015, FICO maintains a sizable market presence given its specialism in anti-financial crime products and services. Further targeted acquisitions and a strong network of partner processors continue to cement the company's position as one of the major players in the field. While FICO is well positioned in its core market, the group as a whole is relatively small compared to some of its larger, diversified competitors.

Technology assessment

Figure 13: FICO – Technology assessment



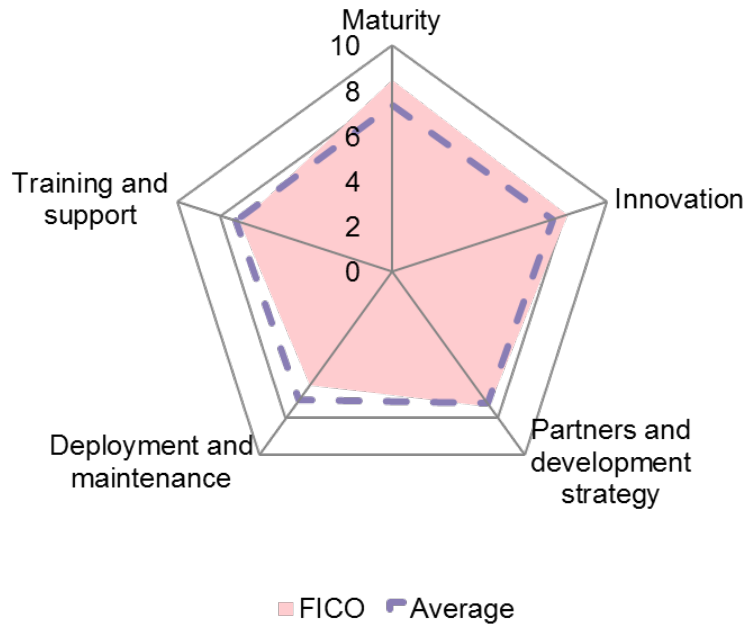
Source: Ovum

FICO's anti-financial crime offering is based around its two platforms – Falcon and Siron. Falcon provides features including transaction monitoring and fraud prevention, with Siron focusing on compliance-related requirements. Together, FICO's platforms provide a strong, broad range of capabilities, supporting a high degree of enterprise-wide threat coverage. The platforms have been built to work with a range of databases and third-party watch lists, all of which feed into their screening and analysis modules. Falcon makes use of machine learning, artificial intelligence, and automation to provide strong predictive and risk-scoring capabilities. Falcon's card payment module reportedly screens roughly 65% of global credit card transactions, using real-time behavioral monitoring. FICO's Card Compromise Manager assists with that process by identifying common points of purchase across compromised cards to help reduce the impact of new cases.

FICO offers a good rounded set of case management and reporting capabilities, including Siron TCR (for FATCA screening and investigations), Siron Risk and Compliance Cockpit (RCC), and Alert and Case Management (ACM). Its Identity Resolution Manager makes use of social network analysis to help fraud managers investigate new cases quickly and effectively.

Execution assessment

Figure 14: FICO – Execution assessment



Source: Ovum

FICO has a particularly strong plan for developing its platforms, with a clear set of priorities to enhance modules and plug any weaker elements in its overall offering. While the two platforms will continue to be available independently, FICO also has a timeline in place to fully integrate the two and strengthen their enterprise-wide coverage. The company maintains a high standard of customer support and product training, although FICO only offers AML training on demand. Both platforms are available via a range of deployment options, although most clients currently choose on-premises.

Recommendation: FICO is a market leader

FICO's Falcon/Siron combination is currently one of the leading anti-financial crime propositions available in the market. FICO can provide strong all-around coverage, with particularly strong capabilities in card fraud prevention and customer behavioral monitoring. The platforms offer banks of all sizes market-leading capabilities, either in full deployment or as individual/multiple stand-alone modules. Ovum recommends that banks short-list FICO's Falcon and Siron combination when searching for a competitive anti-financial crime solution.

IBM

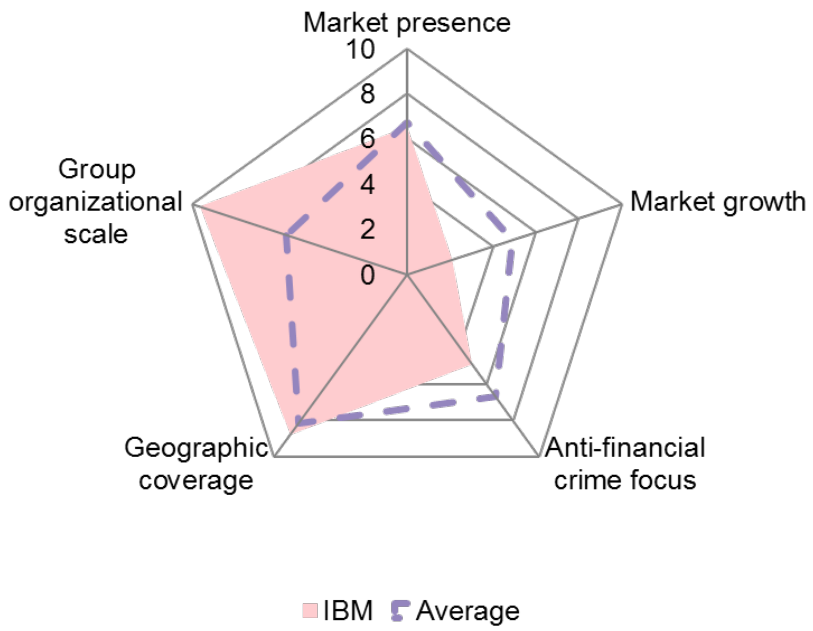
Background

IBM is a publicly listed vendor with a significant financial services presence. It is headquartered in Armonk, US, with offices worldwide. IBM started doing business in 1911, with a recent reorganization of its financial services arm under the Watson brand following its 2016 acquisition of Promontory. That acquisition has added considerable weight to IBM's expertise and consulting resources in compliance and risk management. IBM's core anti-financial crime platform, IBM Financial Crimes Insight,

launched in 2014 and is building up a global client base. IBM has 12 research labs globally, with more than 290 fraud-related patents filed.

Market impact assessment

Figure 15: IBM – Market impact

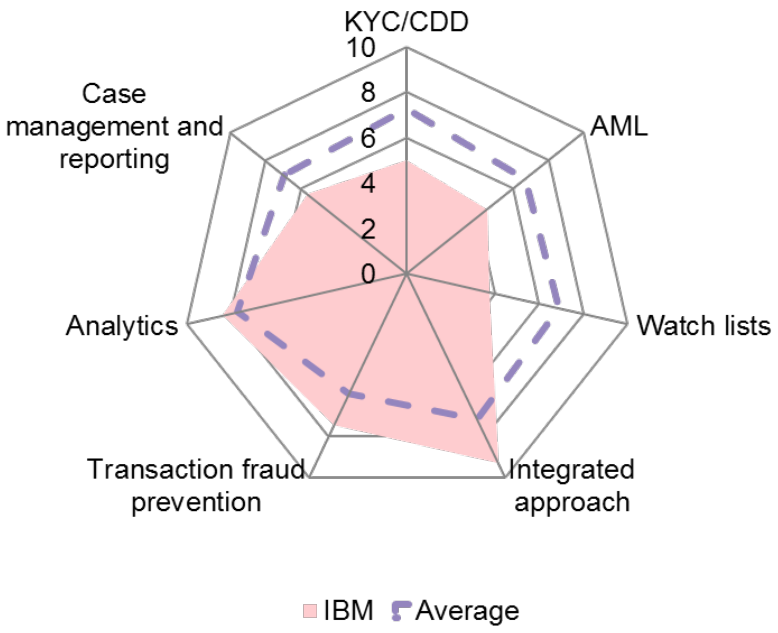


Source: Ovum

As a large diversified global technology company, IBM's services related to anti-financial crime within its Watson Financial Services unit form a relatively small part of the overall business. Nonetheless, IBM is an established major player within the financial services technology market in general, as well as specifically when dealing with anti-financial crime products and services. The company's core anti-financial crime platform has clients worldwide and is currently deployed in a range of languages, including English, French, German, and Brazilian Portuguese. With group revenues of almost $80bn in the last financial year and more than 380,000 staff, IBM is by far the largest general company under consideration in this ODM.

Technology assessment

Figure 16: IBM – Technology assessment



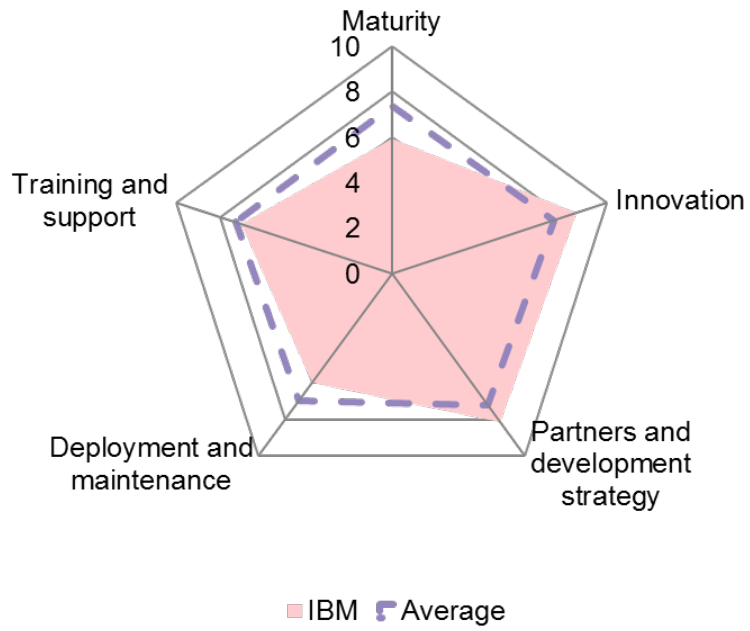
Source: Ovum

IBM's Financial Crimes Insight platform has been designed with a strong focus on providing all-round coverage, using best-of-class third-party plug-ins in areas such as KYC and AML to supplement its own capabilities. Those modules, both in-house and third party, fit smoothly into the overall platform courtesy of IBM's expertise in both enterprise-wide analytics and systems integration. Along with the use of third-party plug-ins, the platform works with multiple modern and legacy back-end systems, with a range of data-sourcing and processing capabilities. The company offers a strong set of payments fraud prevention capabilities, built around its cognitive approach that looks to build rounded customer profiles, making heavy use of machine learning and AI functionality. Indeed, IBM has leading analytical capabilities, utilizing many of the latest technologies.

IBM offers highly adaptable dashboards for case management purposes, which provide a fully customizable experience. Making use of expertise from IBM Research, there are also plans to integrate further big data visualization capabilities to maintain its strength in that area. Indeed, across the full platform, IBM has advanced plans to directly offer next-generation capabilities, along with a simplified new approach to historic and emergent challenges.

Execution assessment

Figure 17: IBM – Execution assessment



Source: Ovum

IBM Financial Crimes Insight is a mature platform for dealing with payment fraud prevention and analytics, and makes use of third-party providers to complement IBM's own capabilities in other areas. IBM has one of the clearest innovation strategies, aimed at not only enhancing the platform's capabilities but also transforming the way existing tasks and challenges are dealt with by financial institutions, making use of specialist technology partners where appropriate. IBM's platform ranks highly for its maintenance setup, with a selection of training and support options on offer. The platform is available via a range of deployment options, including SaaS and on-premises.

Recommendation: IBM is a market follower

IBM Financial Crimes Insight offers financial institutions a strong set of analytical capabilities and payment fraud prevention capabilities, with a forward-looking strategy that aims to transform the way banks tackle risks related to financial crime in general. Vendors should therefore consider short-listing IBM, particularly when looking to modernize legacy systems.

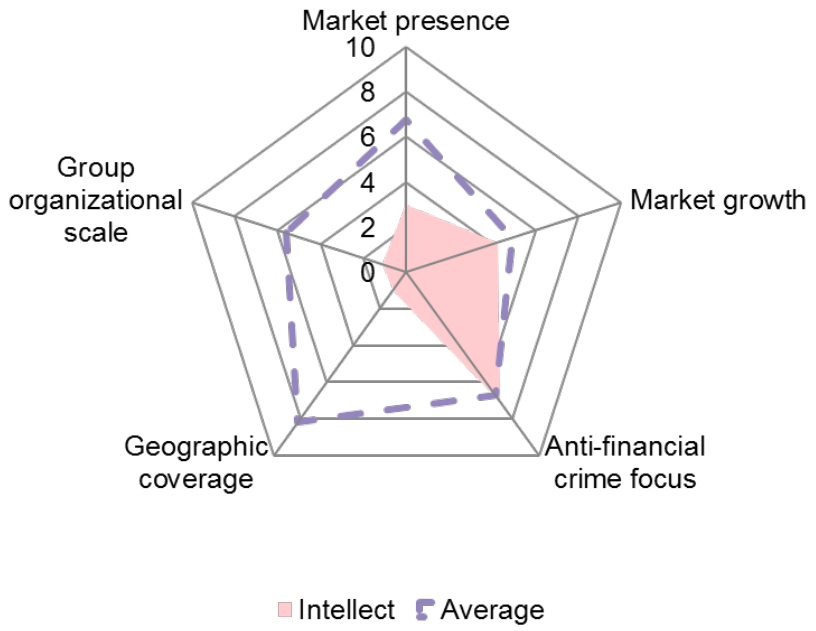
Intellect Design Arena

Background

Intellect is a publicly listed financial services technology vendor headquartered in India with offices across around the world. The company was founded in 2003, and its core anti-financial crime platform, based around Intellect AML, launched in 2009 and has since broadened its coverage over a range of capabilities, with modules including the Intellect Fraud Early Warning System. Intellect has two main anti-financial crime research and development centers, in Chennai and Mangalore in India.

Market impact assessment

Figure 18: Intellect – Market impact

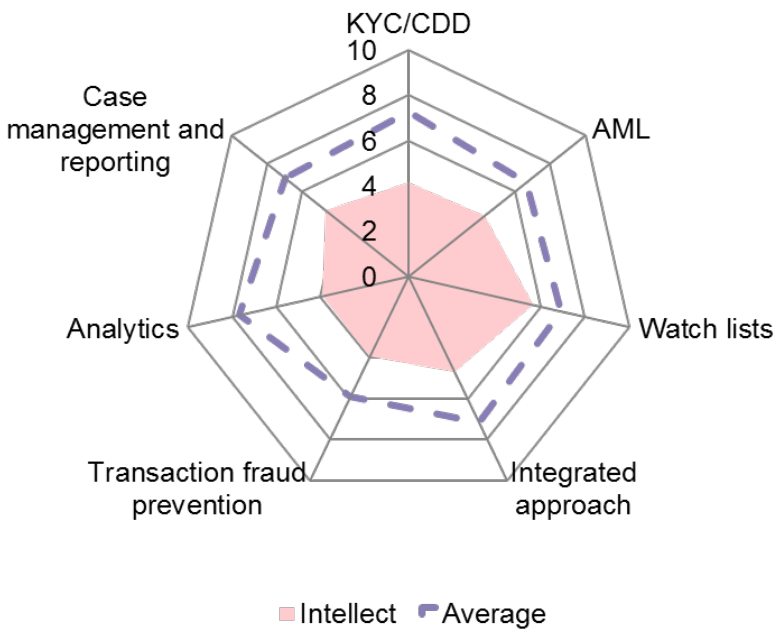


Source: Ovum

Intellect has a defined specialism in financial services technology, of which its anti-financial crime products form an important segment. Since launching its anti-financial crime platform in 2009, Intellect has recorded strong growth, building a solid position in its core market of India, and is now expanding overseas. The core anti-financial crime platform is currently only deployed in English, but support is already provided in Arabic, and the platform is capable of operating with a broader range of languages. With group revenues of over $136m in the last financial year, Intellect Design Arena is the smallest of the vendors under consideration, which reflects its relative youth.

Technology assessment

Figure 19: Intellect – Technology assessment



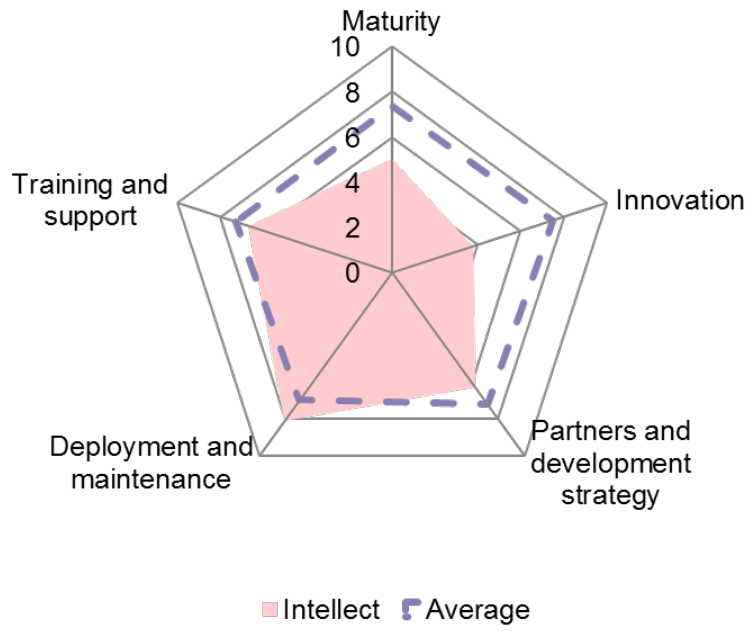
Source: Ovum

Intellect has a broad range of capabilities based around its original core AML platform, meeting most of the requirements for a financial institution. The platform and its various modules were designed to operate with a range of modern and legacy back-end systems, with data processed via third-party providers. The platform provides a selection of watch-list and sanctions filtering and monitoring tools, making heavy use of automation for efficiency of operation. Suspicious transactions and entities flagged by rules-based models are then put through a series of investigative tools, including behavioral, link, and graphical analysis.

Intellect provides financial institutions with a comprehensive out-of-the-box module for case management and reporting, which comes with a range of prebuilt reports for standard regulatory tasks (CTR/STR/CCR/CBTR). The interactive dashboards provide a range of options for investigators to explore both institution-wide and individual customer suspicious transactions in different numerical and graphical formats.

Execution assessment

Figure 20: Intellect – Execution assessment



Source: Ovum

As a relatively new product from a modestly sized company, the Intellect AML platform is less mature than others on the market. Intellect does have in place a range of target measures, such as greater use of machine learning, focusing its research and development on enhancing its offering. One of Intellect's great strengths is its focus on ensuring smooth deployment, ongoing support, and training, providing rapid deployment and integration pathways particularly for smaller customers. The platform is available via a range of deployment options, including cloud services.

Recommendation: Intellect Design Arena is a market follower

Intellect provides an all-around anti-financial crime platform that is quick to deploy and easy to maintain, with strong support and training on offer. Smaller financial institutions should consider Intellect for short-listing to rapidly meet regulatory requirements.

LexisNexis Risk Solutions

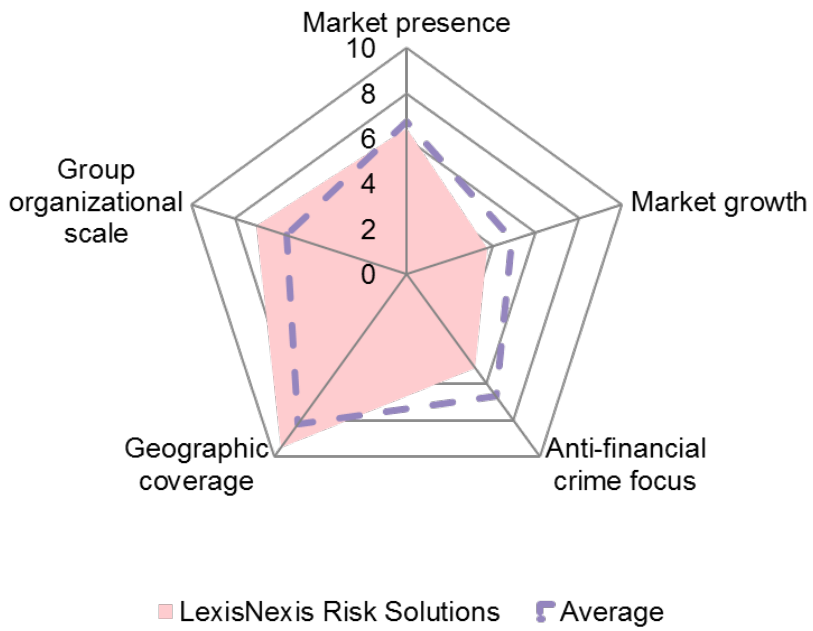
Background

Part of the RELX Group, LexisNexis Risk Solutions is a financial services–focused vendor headquartered in the US. It is a key provider of data and supporting analytic platforms for risk, particularly in the insurance, financial services, and law enforcement sectors. LexisNexis Risk Solutions was founded in 2004 and has recently made a number of acquisitions related to financial crime capabilities, including WorldCompliance in 2013 and Tracesmart and Risk Metrics in 2014. The company has two interrelated core anti-financial crime platforms, Bridger Insight XG and Risk Defense Platform, which launched in 1996 and 2016, respectively. LexisNexis Risk Solutions' main

anti-financial crime R&D centers are in the US and the UK, but the company has research centers worldwide.

Market impact assessment

Figure 21: LexisNexis Risk Solutions – Market impact assessment

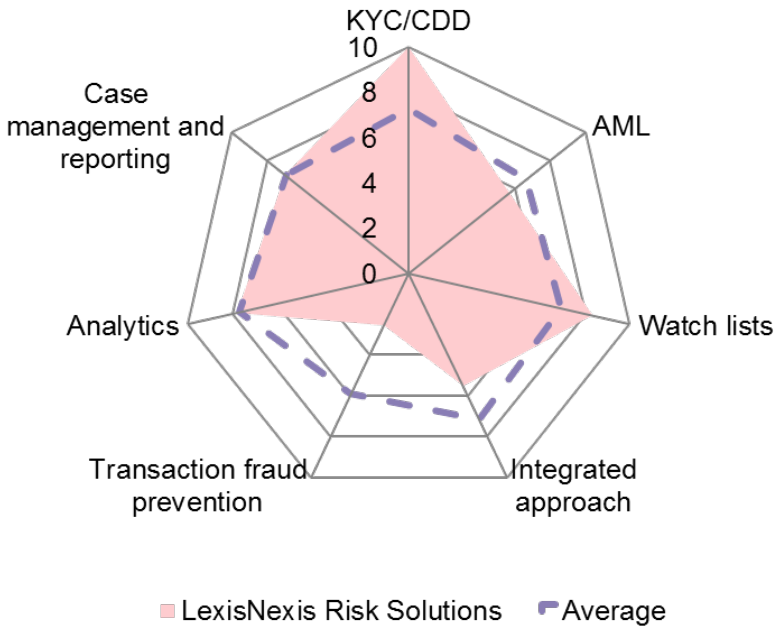


Source: Ovum

LexisNexis Risk Solutions has a broad specialism in risk-related technology products, with a wide set of anti-financial crime capabilities, including those not directly related to financial services. As a result, the company is firmly established as a significant player in the anti-financial crime market, and has recently added depth to its global client base. The core anti-financial crime platform is in deployment in a range of languages, including English, French, German, Japanese, Portuguese, Simplified Chinese, and Spanish. With group revenue of over $9bn in 2016, anti-financial crime services represent a modest section of parent group RELX's overall business, although LexisNexis Risk Solutions itself is highly focused on the financial services industry.

Technology assessment

Figure 22: LexisNexis Risk Solutions – Technology assessment



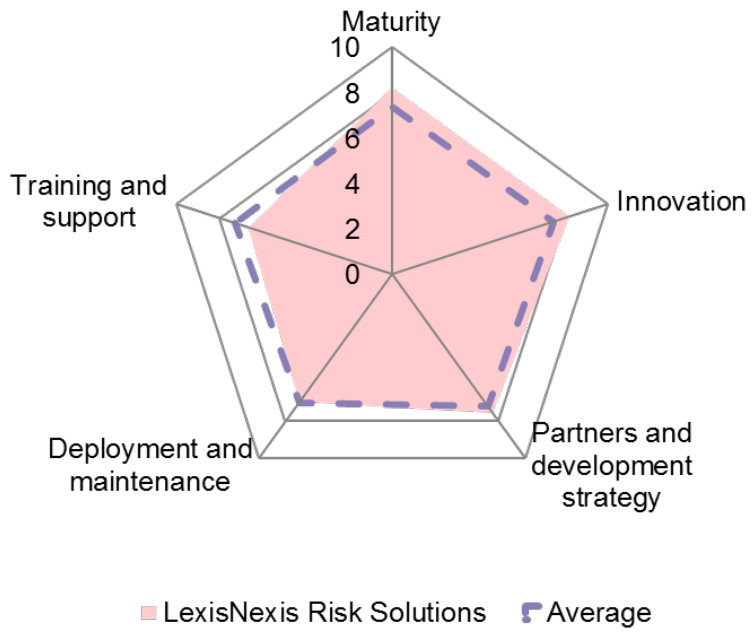
Source: Ovum

LexisNexis Risk Solutions' two-platform combination provides a selection of capabilities for financial institutions, but with a particular focus on threats related to customer onboarding and risk monitoring, as well as watch-list screening and AML/BSA compliance. Exploiting the company's wider expertise in risk scoring, the Bridger Insight XG platform provides a market-leading solution for KYC and watch-list-screening tasks, aimed at improving the efficiency of bank processes in those areas as well as providing a degree of KYC onboarding customization for different consumer risk groups. The company also has strong capabilities aimed at preventing account takeover and synthetic identity–related fraud. Both platforms have been designed to operate with a range of modern and legacy databases, along with the company's own data assets, such as WorldCompliance and the Risk Defense Platform, as well as public records and commercial data sets. The analytics modules make use of advanced big data and analytic linking technologies to identify and assess risk-relevant information. It also makes use of unsupervised machine learning and advance analytics to help automate the alert management process.

The Bridger Insight XG platform and Risk Management Solutions portal offer financial institutions a strong set of workflow and reporting capabilities as off-the-shelf products. With speed and efficiency in mind, Bridger Insight XG's dashboards provide case officers with a clear display of all the relevant information related to an alert, including the confidence score for each match. The platform is also fully capable of meeting a range of ad hoc internal report requirements, as well as external regulatory reports, such as SARs. The company's expertise in public records and commercial information also feeds into it, providing leading FATCA screening and regulatory reporting capabilities.

Execution assessment

Figure 23: LexisNexis Risk Solutions – Execution assessment



Source: Ovum

LexisNexis Risk Solutions' anti-financial crime offering is one of the most mature in the market, particularly within its specialist fields. Innovation is important to the company, with its research and development efforts focused on developing key areas to enhance the capabilities of the two platforms, such as including additional machine-learning capabilities in its modules. The company provides strong client support, with support centers based in the US, the Philippines, and Wales. The platform is available via a range of deployment options, including SaaS, cloud-based, and hosted.

Recommendation: LexisNexis Risk Solutions is a market follower

LexisNexis Risk Solutions' combination of two platforms offers financial institutions a quickly deployable set of anti-financial crime capabilities, with market-leading capabilities in customer due diligence and watch-list screening for AML/BSA compliance. Financial institutions should therefore consider short-listing LexisNexis Risk Solutions, particularly on the AML/BSA compliance side, for both its platform and supporting data sets.

NICE Actimize

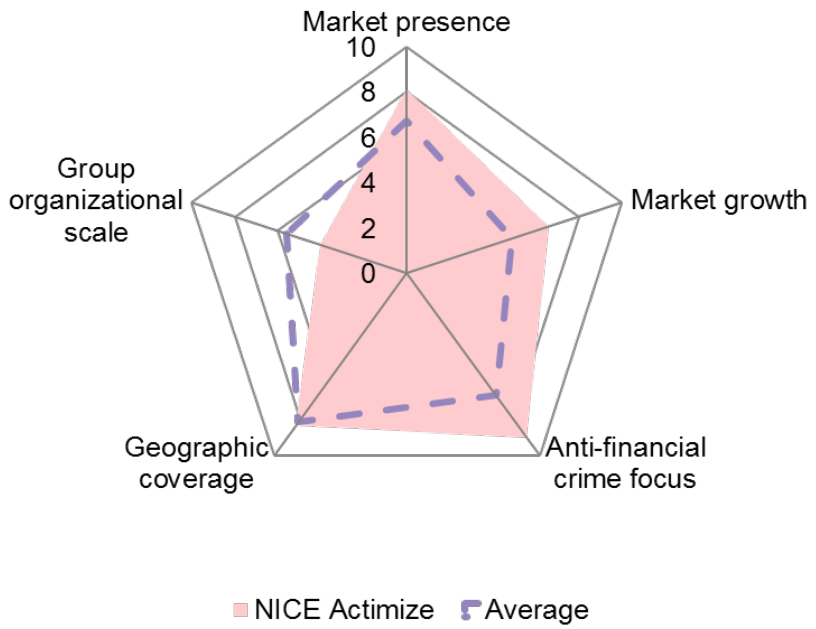
Background

NICE Actimize, a NICE (Nasdaq:NICE) business, is a financial services and solutions-focused vendor headquartered in Hoboken, NJ, in the US and Ra'anana, Israel, with offices across North America, Europe, and Asia. Actimize was founded in 1999 and became a wholly owned subsidiary of NICE in 2007. Actimize's core anti-financial crime platform, the Enterprise Risk Case Manager, was first launched in 2001 and has since built up a diverse client base, recording strong growth figures in

recent years. NICE Actimize's main anti-financial crime R&D center is based in Israel, although it has others around the world.

Market impact assessment

Figure 24: NICE Actimize – Market impact

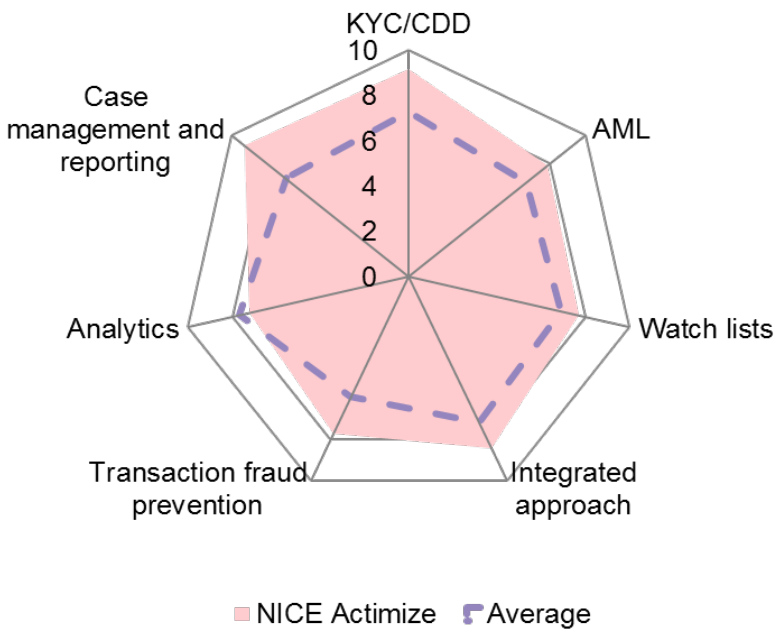


Source: Ovum

NICE Actimize has a defined specialism in anti-financial crime related services, which accounted for about 25% of overall company revenue in 2016. Making the most of that specialist position, NICE Actimize has recorded solid growth in both clients and revenue in recent years, establishing itself firmly as a major player in the market. The core anti-financial crime platform has clients across 42 different countries around the world, supported in a wide range of languages, including English, French, German, Spanish, Portuguese, Italian, Hebrew, Polish, Japanese, and Chinese. Parent company revenues were more than $1bn in the last financial year.

Technology assessment

Figure 25: NICE Actimize – Technology assessment



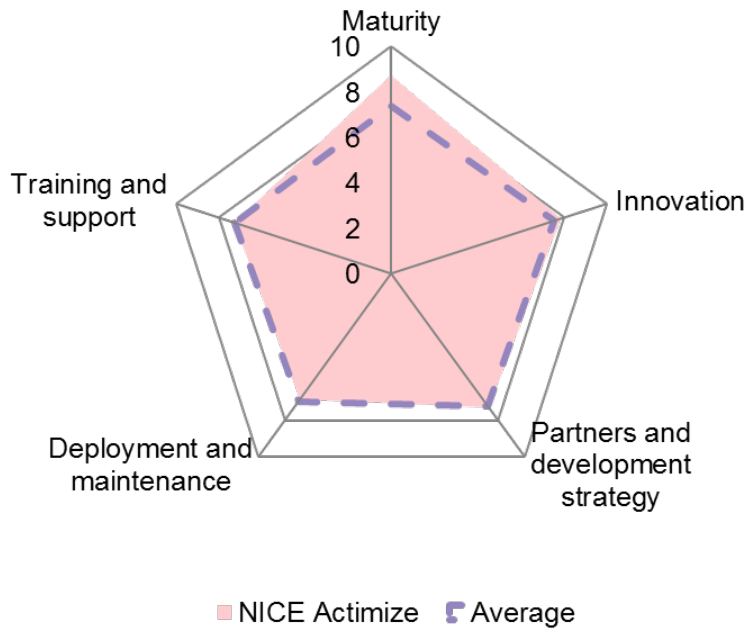
Source: Ovum

Based around a core Enterprise Risk Case Manger (ERCM) platform, NICE Actimize's anti-financial crime modules provide a broad selection of capabilities. With end customers in mind, the ERCM includes a customizable CDD module, using machine-learning-supported risk scoring, to help financial institutions improve their customer experience while maintaining a high standard of protection. With many components designed with interconnection and multichannel integration in mind, the platform supports a high degree of enterprise-wide threat coverage. With implementation in mind, the platform was built to work with multiple modern and legacy back-end systems, with data processed via the Actimize Big Data Store and a cross-platform Data Intelligence Layer. It is in this shared layer that many core analytics functions are performed, such as network analysis and behavioral profiling, to help ensure banks have a single but multichannel understanding of their customers.

NICE Actimize has a strong set of case management and reporting capabilities, including its Tuning Insights and Visual Analytics Insight packs, which provide a high degree of customizable experience. With real-time data access, these interactive dashboards provide advanced data visualization, supporting banks in their reporting, investigation, and model-refining tasks. Actimize's STAR and FATCA Compliance modules also provide purpose-built out-of-the-box capabilities for regulatory filing and compliance management.

Execution assessment

Figure 26: NICE Actimize – Execution assessment



Source: Ovum

Having established a wide client base since its launch in 2001, the ERCM platform is one of the most mature in the market. NICE Actimize also has a clear innovation strategy, aimed at focusing its R&D on improving the platform's capabilities, such as further integrating machine-learning capabilities into its modules, with some major releases in the pipeline. NICE Actimize provides staggered support options, with technical errors resolved within two hours to next business day depending on the level of severity. The platform is available via a range of deployment options, including as a cloud service, although most clients currently opt for on-premises.

Recommendation: NICE Actimize is a market leader

NICE Actimize's ERCM is one of the leading anti-financial crime platforms available in the market. The solution provides strong all-around coverage, across the full range of core capability areas. Fully scalable, the ERCM suite offers banks of all sizes market-leading capabilities, both for enhancing existing systems and for greenfield deployments. Ovum recommends that banks short-list NICE Actimize's Enterprise Risk Case Manager when searching for a competitive anti-financial crime platform solution.

Oracle

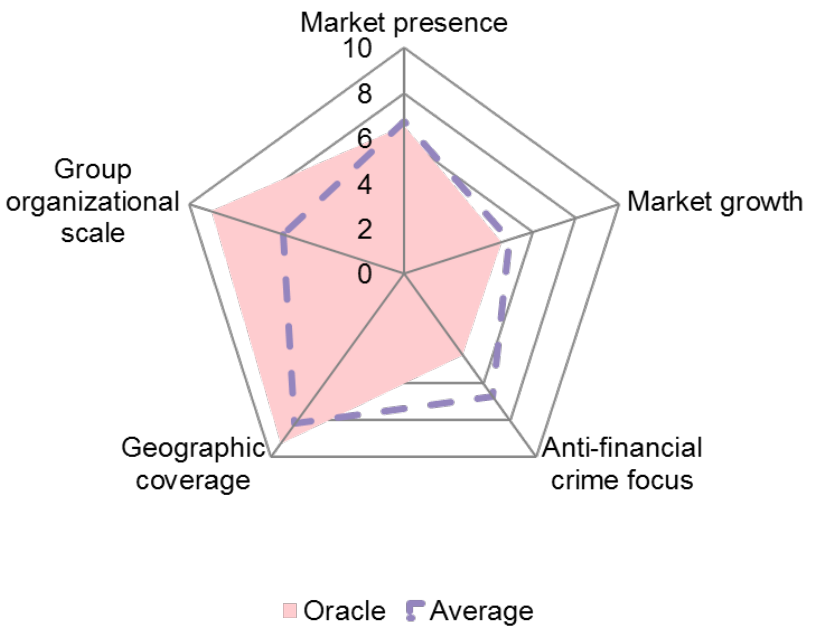
Background

Founded in 1977, Oracle is a publicly listed global computer technology vendor headquartered in Redwood City, California, US, and a significant on-premises and cloud provider of enterprise applications, data and analytics, and hardware/infrastructure. As part of Oracle's Financial Services Analytical Applications line of business, the company's core anti-financial crime platform, the Oracle

Financial Crime and Compliance Management (FCCM) solution, was launched in 1999 and has since built up a diverse client base. Oracle maintains anti-financial crime research and development centers in the US, UK, Ukraine, India, and Singapore, and acquired Mantas in 2006 to strengthen its capabilities in this field.

Market impact assessment

Figure 27: Oracle – Market impact

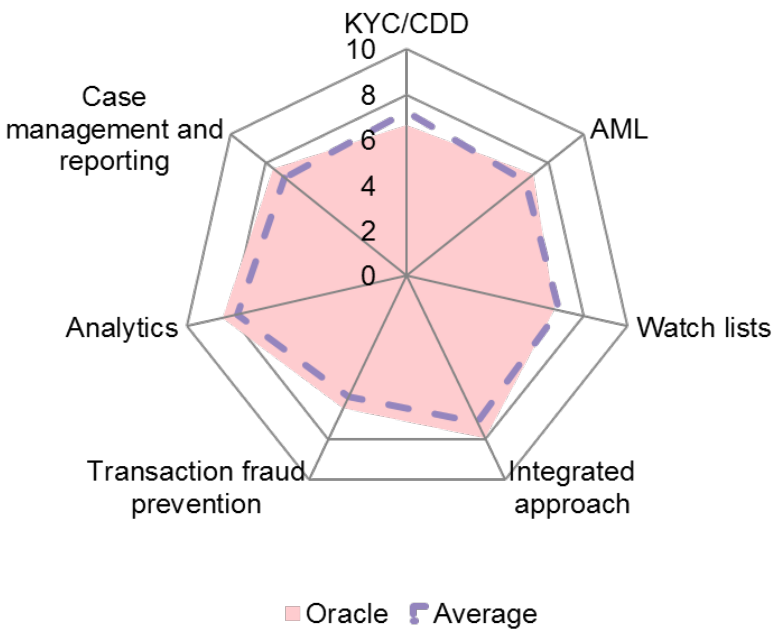


Source: Ovum

Oracle is well established as a significant player in the anti-financial crime market, utilizing its global resources to extend its worldwide client base, with a strong presence in North America and EMEA. The core FCCM anti-financial crime platform is currently deployed in a wide range of languages, including English, Simplified Chinese, French, German, Korean, Spanish, Russian and Portuguese. Oracle is a large diversified group with global revenues of over $37bn in 2016, meaning anti-financial crime services form a relatively small portion of the group's operations, although interrelated data and analytics capabilities form a much larger segment of the business.

Technology assessment

Figure 28: Oracle – Technology assessment



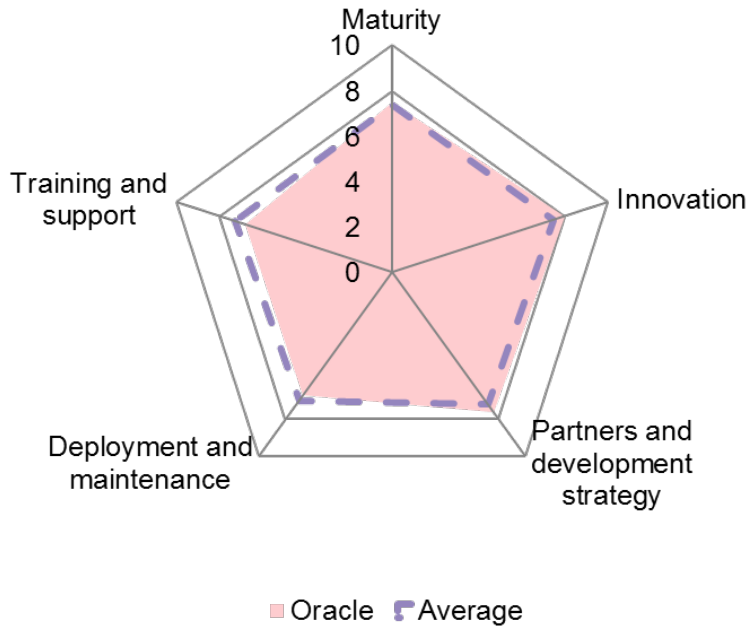
Source: Ovum

Oracle's FCCM anti-financial crime platform provides a broad all-round selection of capabilities, which has been designed to provide financial institutions with a good degree of enterprise-wide coverage. With implementation in mind, the platform was built to work with data fed through the OFSAA data management platform, which helps bring together inputs from modern and legacy front-end systems. These are then fed into Oracle's various analytics modules, one of Oracle's key strengths, with the Oracle Financial Services Crime and Compliance Studio an example that makes use of machine learning and graph analytics. Indeed, the company is one of the leading providers for extending big data and machine-learning techniques to anti-financial crime tasks. Oracle also offers a particularly strong set of AML capabilities, although it does not provide employee non-product AML training as standard.

Oracle has a strong set of out-of-the-box case management and reporting capabilities that leverage the company's Business Intelligence reporting application, which offers a configurable set of reports and dashboards. With real-time data access, those interactive dashboards provide a range of advanced graphical data displays. The company also has a strong range of compliance-related reporting modules, including those dealing with FATCA, CRS, and compliance regulatory reporting such as CTR, SAR, and STRs.

Execution assessment

Figure 29: Oracle – Execution assessment



Source: Ovum

The FCCM platform, as one of the longer-running propositions on offer, has established a sound client base since its launch, with leading analytical capabilities. Oracle also has one of the strongest innovation strategies, aimed at using its research and development resources to enhance and extend the capabilities of the platform through the latest techniques, where necessary through technology partners. Oracle provides a range of support options, with the FCCM platform being one of the best for clients in terms of ongoing maintenance and upgrades. The platform is available via a range of deployment options.

Recommendation: Oracle is a market challenger

Oracle's FCCM is a challenger in the anti-financial crime platform market, providing a high standard of all-round capabilities for banks of all sizes, and strong big data capabilities. FCCM is a strong standalone offering and benefits from being able to support broader analytical requirements across the risk, finance, and customer insights stack. Ovum recommends that banks consider Oracle's FCCM platform when searching for a competitive anti-financial crime platform solution.

SAS Institute

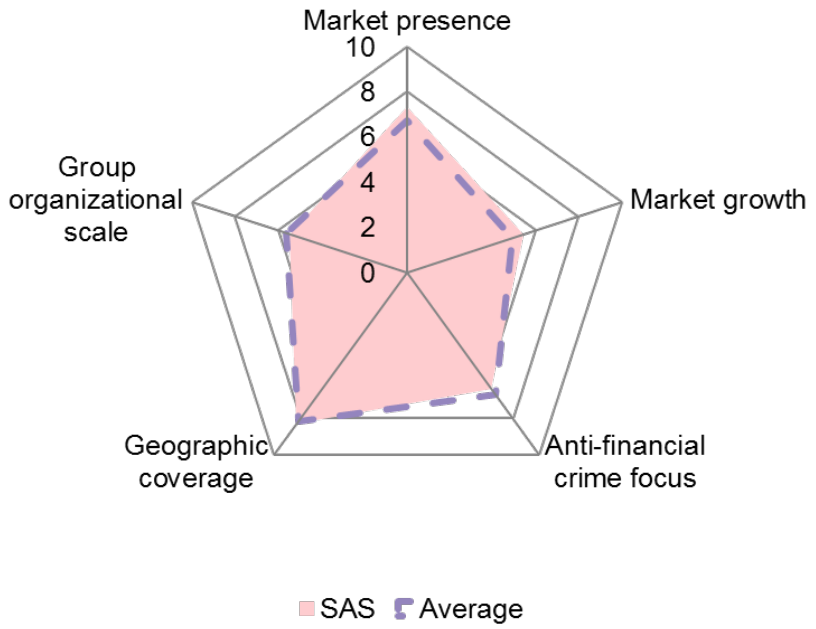
Background

SAS is a private multinational analytics provider headquartered in Cary, North Carolina, US. The company was founded in 1976 and now has offices in 55 countries around the world. As part of SAS's Fraud and Security Intelligence Division, the company's core anti-financial crime platform, the SAS Fraud and Financial Crimes platform, was launched in 2003, and in the intervening 14 years it has

built up a diverse global client base. SAS has three main anti-financial crime research and development centers, based in the US, UK, and India.

Market impact assessment

Figure 30: SAS – Market impact

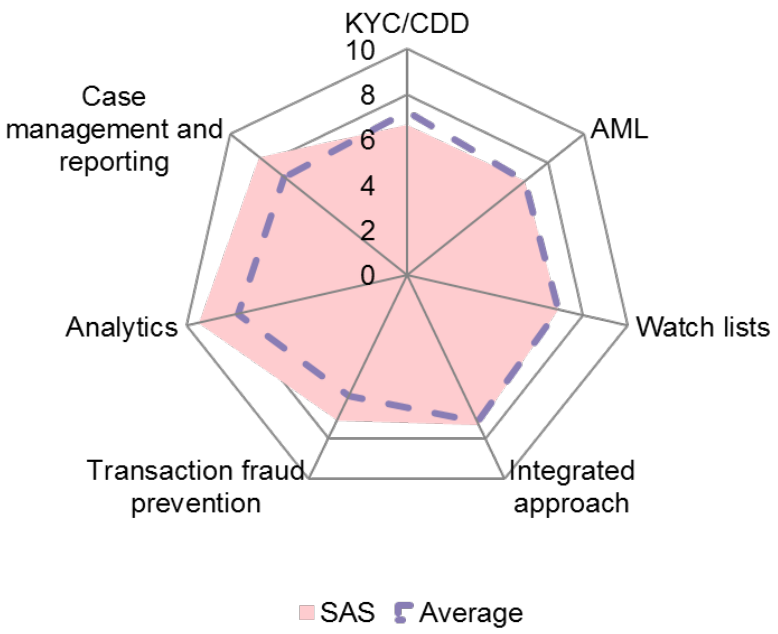


Source: Ovum

With its broad portfolio of analytics-related services, anti-financial crime products form an important but balanced part of SAS's overall business. In recent years, SAS has successfully expanded beyond its core North American market, recording strong growth in a range of emerging markets, such as China. As a result, the core anti-financial crime platform now has a wide global client base, and is deployed in a wide range of languages, including English, French, Spanish, German, Italian, Portuguese, Arabic, Mandarin, Japanese, Korean, and Russian. SAS also maintains a significant presence in the wider financial services market as a well-established analytics developer and provider. With group revenues of over $3bn in the last financial year, SAS is one of the midsized overall vendors competing in the market.

Technology assessment

Figure 31: SAS – Technology assessment



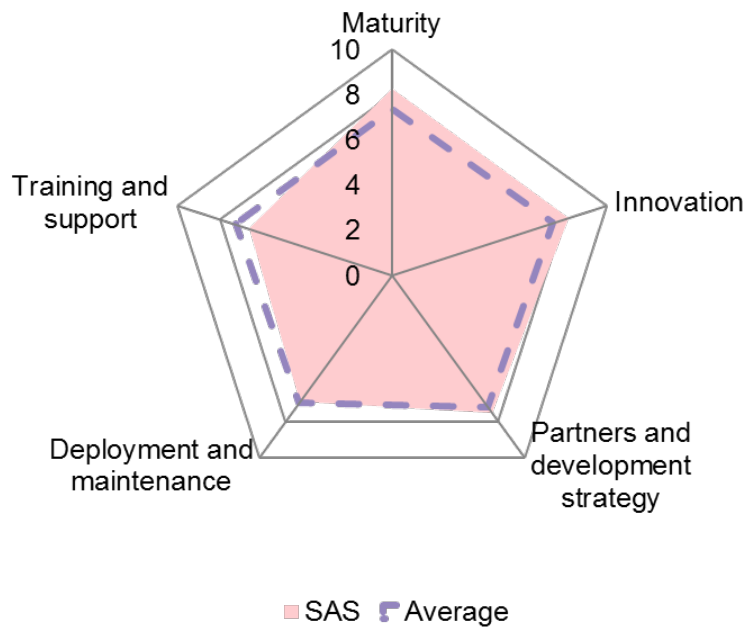
Source: Ovum

SAS's Fraud and Financial Crimes platform offers financial institutions a high degree of all-round, enterprise-wide anti-financial crime capabilities. The platform has been designed to work with a wide range of modern and legacy database systems, which all feeds through into SAS's key market-leading capability – its analytics engines. For payment fraud screening and prevention, for example, SAS's modules make use of advanced machine-learning techniques as part of a real-time process to risk score transactions. That process includes SAS's Event Stream Processing engine, which offers financial institutions the chance to train, validate, and score supervised machine-learning models in real time, via an intuitive and easy-to-comprehend dashboard. Supported by those analytics capabilities, SAS is particularly strong in terms of direct fraud prevention.

The Fraud and Financial Crimes platform offers a high standard of case management and reporting capabilities, including its Visual Analytics reporting module, which provides a fully customizable experience. SAS's interactive dashboards provide clear graphical displays to aid bank staff in their work, but the company is also piloting natural language generation options for situations where clear written responses are more efficient than visual displays. The company also provides a full range of regulatory reporting modules, including a prepopulated SAR tool, which stands out as a particularly clear and efficient means for banks to process their SAR responses and report them to the regulators.

Execution assessment

Figure 32: SAS – Execution assessment



Source: Ovum

Providing a high degree of enterprise-wide coverage, with some market-leading capabilities, SAS's Fraud and Financial Crimes platform is one of the more mature propositions in the market. SAS has one of the clearest innovation strategies in the market and is already trialing a number of next-generation capabilities. The company is also looking at embedding its advanced analytics capabilities across the full range of its modules, beyond those where they are already in operation. SAS provides a strong level of product-specific support options, such as AML optimization consultations, to help banks get the most from their anti-financial crime technology. The platform is currently available via a range of deployment options.

Recommendation: SAS is a market challenger

SAS's Fraud and Financial Crimes platform provides strong enterprise-wide coverage for financial institutions, including market-leading analytics capabilities. Ovum highly recommends that banks consider SAS's Fraud and Financial Crimes proposition when short-listing options for competitive anti-financial crime platform solutions, particularly when it comes to preventing fraudulent transactions.

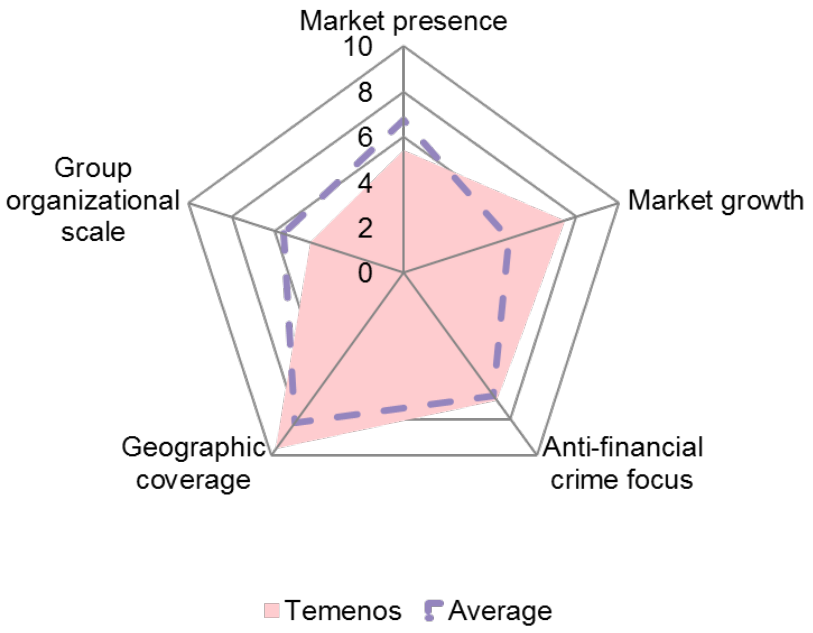
Temenos

Background

Temenos is a publicly listed financial services–focused vendor headquartered in Geneva, Switzerland, with offices in 42 countries. Temenos was founded in 1993 and now has over 4,400 staff. Its Financial Crime Mitigation product family was launched in 2004 and has since built a diverse client base, recording high growth figures in recent years. The company has research and development centers in Belgium, India, Switzerland, and Romania, with support bases in a range of additional locations.

Market impact assessment

Figure 33: Temenos – Market impact

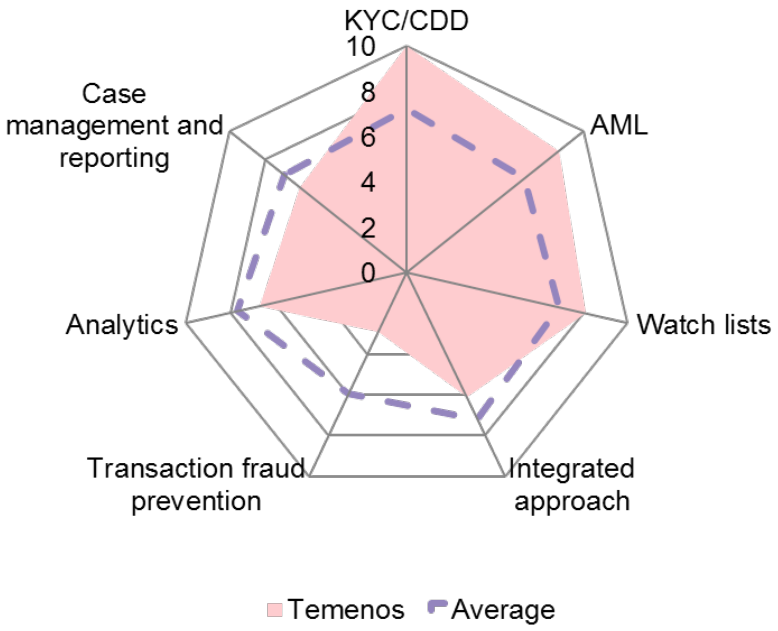


Source: Ovum

Temenos has a strong specialism in services related to anti-financial crime, which represent a core revenue stream for the overall group, with a particular focus on products related to compliance and customer screening. Exploiting its specialist position, Temenos has recorded strong growth in both clients and revenue in recent years. The core anti-financial crime platform has clients in 48 different countries and is already deployed in a wide range of languages, including English, German, French, Italian, Spanish, Portuguese, Greek, Hebrew, Simplified Chinese, and Arabic. Temenos recorded group revenues of over $635m in the last financial year, which is sizable but still modest compared to some of its larger counterparts with highly diverse businesses.

Technology assessment

Figure 34: Temenos – Technology assessment



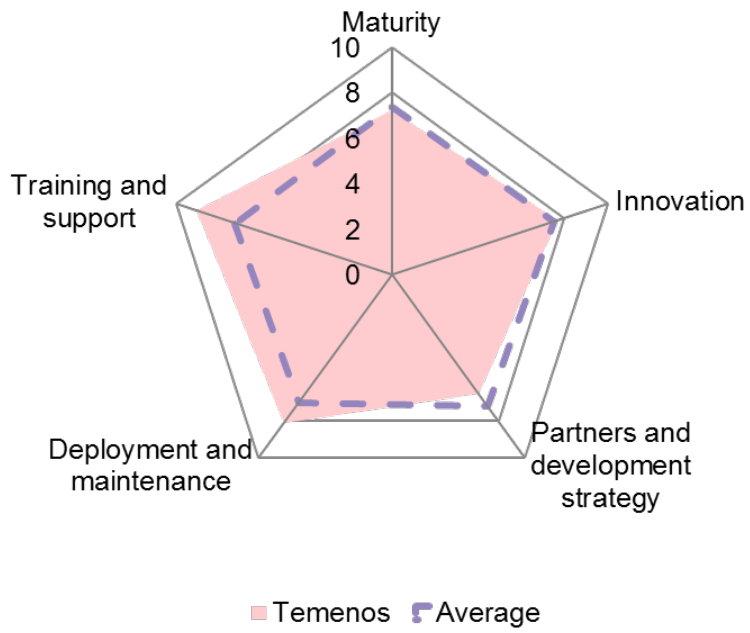
Source: Ovum

The modules available in Temenos' Financial Crime Mitigation (FCM) product family provide a broad selection of capabilities. Temenos has a market-leading specialism in compliance and customer-screening capabilities, with top-ranking KYC/CDD and AML capabilities. The product family has been designed to be highly configurable to work with multiple modern and legacy back-end systems, with transaction and alert data processed in real time. The FCM KC+ module is capable of flexibly supporting any form of automated document verification process and performs ongoing risk scoring against customer behavior.

Temenos' FCM Knowledge Manager provides a central solution for case management and reporting, with a full, flexible range of customizable reports for internal clients. SAR and watch-list reporting is handled separately by FCM Profile, making use of AI capabilities, with the reporting process integrated with the investigation phase aimed at continually reducing the level of false positives. FATCA and other tax reporting can be integrated into FCM modules, but is provided elsewhere in the Temenos product range.

Execution assessment

Figure 35: Temenos – Execution assessment



Source: Ovum

Temenos has a strong, mature offering within its areas of specialism, although there are some gaps in coverage. To help deal with those areas, the company has a clear innovation strategy and roadmap, aimed at enhancing the platform's capabilities, such as further integrating machine-learning and AI capabilities. Temenos has a strong focus on providing a flexible and pain-free deployment experience, suited to clients both large and small looking to quickly gain key capabilities, which is also reflected in strong training and ongoing support options. The platform is available for deployment both on-premises and via SaaS, although most clients currently opt for on-premises, as is the current trend within financial services, given the relative infancy of SaaS technology and risk-averse nature of the industry.

Recommendation: Temenos is a market challenger

Temenos' FCM is currently a challenger in the anti-financial crime platform market. The suite provides high-quality KYC, AML, and watch-list capabilities, and is fully scalable to offer banks of all sizes the chance to quickly implement market-leading coverage in those areas. Ovum recommends that banks consider Temenos' Financial Crime Mitigation Product Family when searching for a competitive anti-financial crime platform solution.

Appendix

Author

Matthew Heaslip, Analyst, Financial Services Technology

Daniel Mayo, Chief Analyst, Financial Services Technology

daniel.mayo@ovum.com

Ovum Consulting

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Ovum's consulting team may be able to help you. For more information about Ovum's consulting capabilities, please contact us directly at consulting@ovum.com.

Copyright notice and disclaimer

Ovum

TMT intelligence | informa

CONTACT US

www.ovum.com

analystsupport@ovum.com

INTERNATIONAL OFFICES

Beijing

Dubai

Hong Kong

Hyderabad

Johannesburg

London

Melbourne

New York

San Francisco

Sao Paulo

Tokyo