The key to successful fraud risk control

The seven capabilities to achieving a strategic response to fraud

An Experian white paper

Experian
Decision Analytics

Consumer behaviour is changing, fuelled by the digital era, and economies are recovering. Meanwhile fraud statistics are back on the rise, along with the costs involved in managing it; losses to fraud around the world amount to £2.91 trillion a year[1].

Fraud is a widespread and complex problem. Targeting weaknesses and inconsistencies and thriving on uncertainty and complexity, its effects can be devastating – threatening your business processes, eroding the integrity of your employees, and tarnishing your reputation.

Regain control

Developing a strategic response to fraud can put you back in control and enable you to protect your customers.

One of the keys to successful fraud risk control is to clearly define the activities, processes, roles and responsibilities that will collectively inhibit and restrict the fraudster.

In this paper, we consider the core fraud risk control capabilities that organisations need to develop in order to effectively counter fraud and its damaging effects, and thereby create a strategic response to fraud.

Key highlights:

1. The increased risk of fraud
2. The increased complexity of managing fraud
3. Seven capabilities to achieving a strategic response to fraud
4. Benchmarking and developing fraud risk control capabilities
5. Next steps: Moving from capabilities to activities

The increased risk of fraud

Whilst the digital era has improved our lives in many ways, it has also enabled fraud to flourish at an alarming rate. It's a crippling problem for businesses, particularly those in data sensitive industries, such as financial services and telecoms. The same qualities that make digital commerce attractive to businesses – efficiency, speed, global accessibility – make it equally attractive to criminals.

Many organisations have expanded their capabilities and value propositions into new markets and regions. For example, we have seen supermarkets and telecommunications businesses becoming banks and leveraging not just their capabilities but their infrastructures, reputation and customer base. Moreover, this activity is not confined to national borders; across Europe, for example, we see ever increasing levels of cross-border activity.

The successful exploitation of these opportunities also brings with it increased exposure to fraud. Organisational growth into new markets and new territories, each with their own cultures and operating models, will commonly expose stresses, weaknesses and inconsistencies within organisational infrastructures which sophisticated fraudsters expressly target and seek to exploit.

We can't eradicate fraud altogether, but there is much more we can do to fight it.

[1]BDO Financial Cost of Fraud Survey, 2013

The increased complexity of managing fraud

Multi-channel customer management: Advanced technology and the digitally empowered consumer

The advancement of technology in business services, combined with the explosive growth in social media and data connectivity, has permanently altered – and, in many ways, brought together – the business and consumer landscape.

As this has evolved, customer behaviours and expectations have changed dramatically, and a new type of customer is emerging – one that is confident, better informed and connected. These digitally empowered customers expect organisations to deliver services on a par with the best experiences from other industries.

As a result, organisations are developing multi-channel infrastructures to meet heightened customer expectations. This can be challenging in its own right but becomes doubly so when organisations seek to integrate these channels across a diverse IT infrastructure, managing complex data flows, while creating and maintaining a seamless and satisfying customer experience.

Therefore, an organisation's ability to meet these customer expectations is becoming an area of competitive differentiation – those organisations that achieve it will have a positive reputation and high levels of customer recommendations.

Managing increased regulation

Regulatory pressures are creating further internal challenges for organisations in terms of how they engage with their customers and manage customer data. Ensuring regulatory compliance risks creating potentially damaging friction within the customer acquisition and on-boarding process, but the risk of non-compliance, including fines, penalties and the associated damage to reputation and brand, is even greater. In this increasingly scrutinised environment, it is clear that fraud at any level of the organisation needs to be tackled.

Managing cross-border activity

Cross-border expansion may be predicated on acquisitions, mergers, or joint-ventures, all of which may have complex implications on a highly diverse set of processes and IT systems.

These challenges will often be significantly compounded due to inconsistencies between the regulations or practices which apply within adjoining countries. If organisations are unable to successfully leverage their risk management capabilities to encompass the challenges created by cross border or new market expansion, then they will be significantly more exposed to the damaging effects of the sophisticated and highly organised fraud rings.

Organisational growth

New market ventures are often accompanied by the need to reach challenging revenue targets through rapid customer acquisition. This drive for growth can create a type of organisational myopia and the compromising of fraud risk controls which may be seen by some as being at odds with the need to acquire new customers.

Ultimately, developing a strategic response to fraud risk control will be about developing a set of complementary capabilities to enable the organisation to manage and achieve the optimum balance of fraud losses, costs, and sales revenues.

The seven capabilities to achieving a strategic response to fraud

Faced with the prospect of continuing margin erosion, and the escalating costs of trying to manage fraud and the associated losses, many Chief Executives recognise that only through change can their organisations successfully manage fraud challenges and achieve ambitious customer growth and revenue targets, while retaining market reputation.

The scale of the change will vary but ultimately will involve empowering the senior leadership team, having a clear understanding of the organisation's fraud risk control capabilities, and then creating an environment which successfully enables these capabilities to grow, develop and flourish.

In working with hundreds of clients around the world we have identified seven organisational capabilities which will have a critical bearing on the overall effectiveness of fraud prevention activity.

Capability 1: Leadership that can see across the multiple dimensions of fraud risk control

Managing the complex external and internal forces impacts a wide variety of stakeholders across the organisation. Fraud is an organisational issue as well as a risk issue.

In addition to the risk function, fraud prevention and management will have significant implications and challenges for sales, finance, customer experience, IT, operations, brand and PR.

Different stakeholders will view fraud through a range of different "lenses." In many instances multiple lenses will apply. For instance, risk departments are increasingly being expected to view fraud simultaneously encompassing risk, cost, revenue, process, customer, and strategy.

Yet how realistic is it for organisations to expect their risk function alone to be able to look through these multiple lenses simultaneously? Clearly, risk needs to be effective at engaging with stakeholders across the organisation but how realistic is it to expect them alone to have responsibility for developing a coordinated and strategic response to fraud risk control? It is therefore vital that the organisation's leaders recognise that fraud risk control is an enterprise-wide issue.

Capability 2: Effective governance

The multiple lenses of fraud risk control reveal a potentially complex picture of interdependencies and overlap.

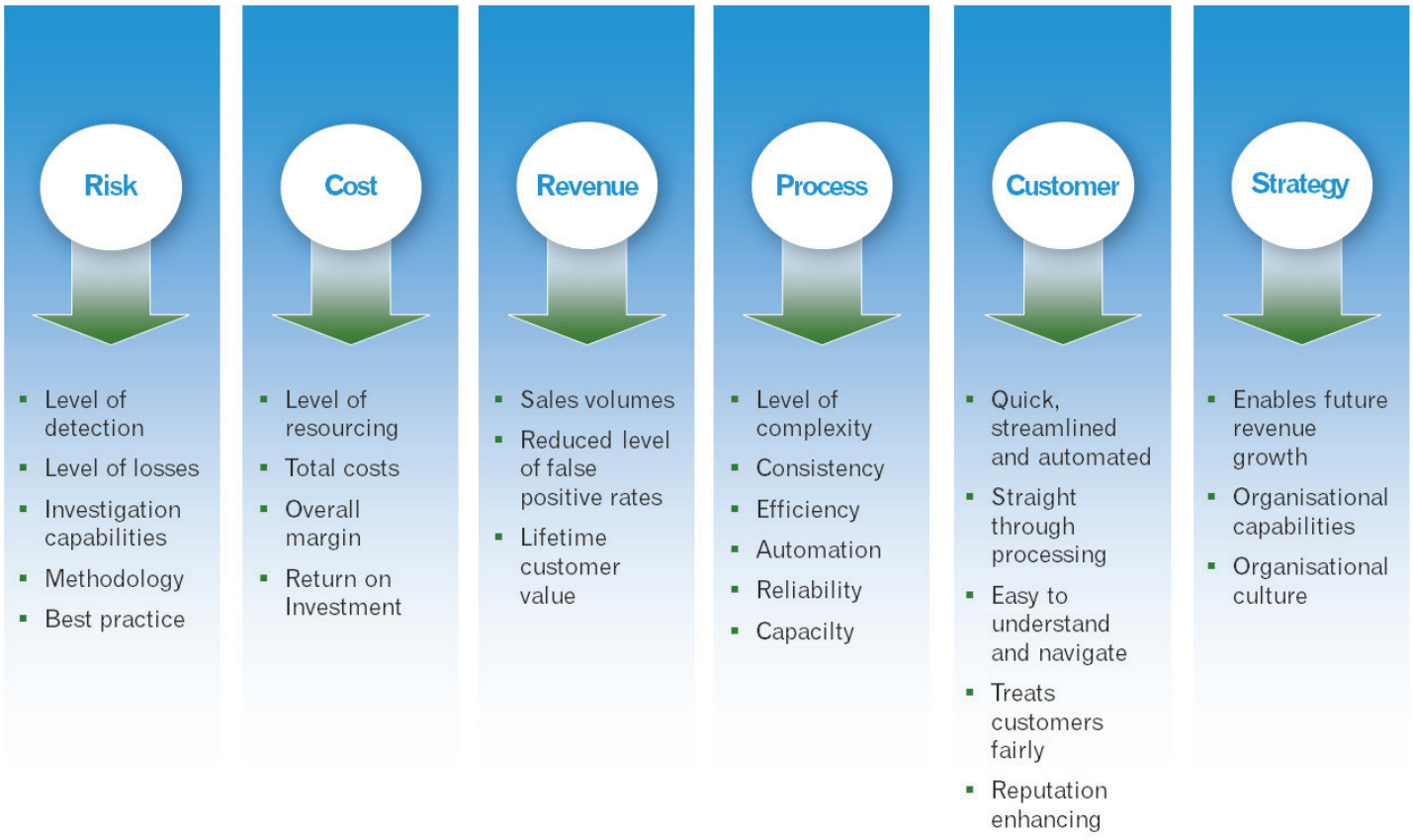
Without an enabling governance structure to foster and develop shared responsibility, attempts to manage and prevent fraud are likely to fall foul of competing priorities and internal tensions which may risk putting individual stakeholders directly at odds with each other.

Organisations that are able to successfully manage these interdependencies typically do so by creating a highly visible, cross departmental "committee" or "board" made up of the heads of the key business areas and typically reporting directly to the Chief Executive or to the main board. This would give the committee the requisite authority and visibility to cut through organisational structures and parochial interests.

As well as helping ensure greater alignment across business areas, a strong governance structure can also ensure that awareness of the importance of fraud risk control is raised across the organisation and can foster a culture of best practice sharing and adoption.

This type of approach is typically reserved for a very small number of strategic imperatives – those priority areas which require a level of focus and clarity and alignment which may, initially at least, be impossible to achieve within business as usual. Research consistently places data security risk and fraud risk within the top five areas of priority.

The multiple dimensions of fraud



The Fraud Risk Committee will act in a directive role in:

- Ensuring the organisation has a full understanding and awareness of the fraud risk
- Determining the overall appetite for fraud
- Defining the strategy which is reflective of the appetite
- Defining and organising the required fraud prevention and management capabilities
- Resourcing required capability development
- Assessing and communicating progress
- Identifying, promoting and sharing best practice

The Committee should collectively "own" the development of the organisation's fraud strategy which will then be implemented by the managers within the separate business areas.

A useful starting point will therefore be to identify all of the fraud related challenges which are faced by each department or business area. Having done so, potential performance indicators that will help measure the ongoing progress being made in overcoming the challenges, should also be defined.

The table on the following page illustrates this approach.

> The development of a strategy for risk control will need to have a clear understanding of the impact of fraud across all parts of the organisation.

Business Area	Fraud related challenges	Related key performance indicators
Risk	• Lowering exposure to fraud • Managing fraud risks within a defined risk appetite across entire lifecycle • Identifying negative customer activity • Raising customer acceptance rates • Differentiating between fraud and non-fraud losses • Optimising scarce fraud investigation resources • Creating a culture of fraud risk awareness • Maintaining the capability to stay ahead of fraudsters • Ensuring regulatory compliance	• Reduced fraud losses • Improved NPS Score • Increased fraud detection rates • Reduced false positive ratios • Reduced manual review rates • Reduced rejection rates
Sales	• Swift acquisition of genuine customers • Increasing customer retention • Increasing levels of cross selling and up-selling	• Increased customer acceptance rates • Reduced customer drop off rates during application and on-boarding process • Increase in quality customers
Finance	• Optimising P&L performance • Reducing operational costs • Raising customer acceptance rates whilst minimising risk of fraud	• Reduced time to profit for new customers • Increased customer acceptance rates • Reduced customer cost to serve • Reduced customer drop-off rates • Increased lifetime customer value • Increased fraud detection rates • Reduced overall losses due to fraud • Reduced cost of collections
Customer Experience	• Shortening customer acquisition process • Ensuring smooth and satisfying customer journeys • Treating customers fairly and consistently • Managing customer retention • Minimising potentially damaging effects of regulatory compliance	• Reduced customer referrals and manual intervention • Faster customer decisioning • Increased customer acceptance rates • Reduced customer drop off rates
IT	• Connecting and leveraging multiple internal and external data sets • Managing complex data flows to support multi-channel infrastructure • Maintaining SLA performance • Protecting customer data • Ensuring compatibility of 3rd party solutions • Reducing workflow management complexity • Maintaining a robust and scale-able infrastructure • Controlling / reducing OPEX costs	• Reduced cost to serve • Reduced customer drop off rates • Reduced systems intervention
Operations	• Ensuring fast, safe and accurate customer decisioning • Reducing business acquisition costs • Maximising operational efficiencies • Enabling swift adjustments to risk thresholds, fraud pattern detection and fraud referral processes • Need to minimise operational capital expenditure • Increasing straight through processing • Reducing the need for manual intervention	• Reduced operational costs • Reduced manual referrals • Increased straight through processing rates • Better customer experience
Brand and PR	• Minimising reputational risk of non-compliance • Protecting customer data across the whole lifecycle • Building loyalty and retention • Building brand advocacy • Providing end-customers with reassurance	• Frictionless customer experience • Increased acceptance rates • Reduced customer drop off rates • Reduced fraud losses • Enhanced positive PR • Increased net promoter scores

Having considered application fraud from the perspective of each separate business area, an aggregate, organisational view can then be constructed and used as the basis for determining and assigning relative levels of responsibility, accountability, and consultation along with the definition of cross organisation “strategic” targets and key performance indicators.

These will be critical tools which will be used by the organisation’s leaders to manage the strategy within the overall governance structures.

Capability 3: A defined fraud appetite

This is a vital area of activity. It will typically involve conducting an assessment of the organisation's exposure to fraud risk from three perspectives.

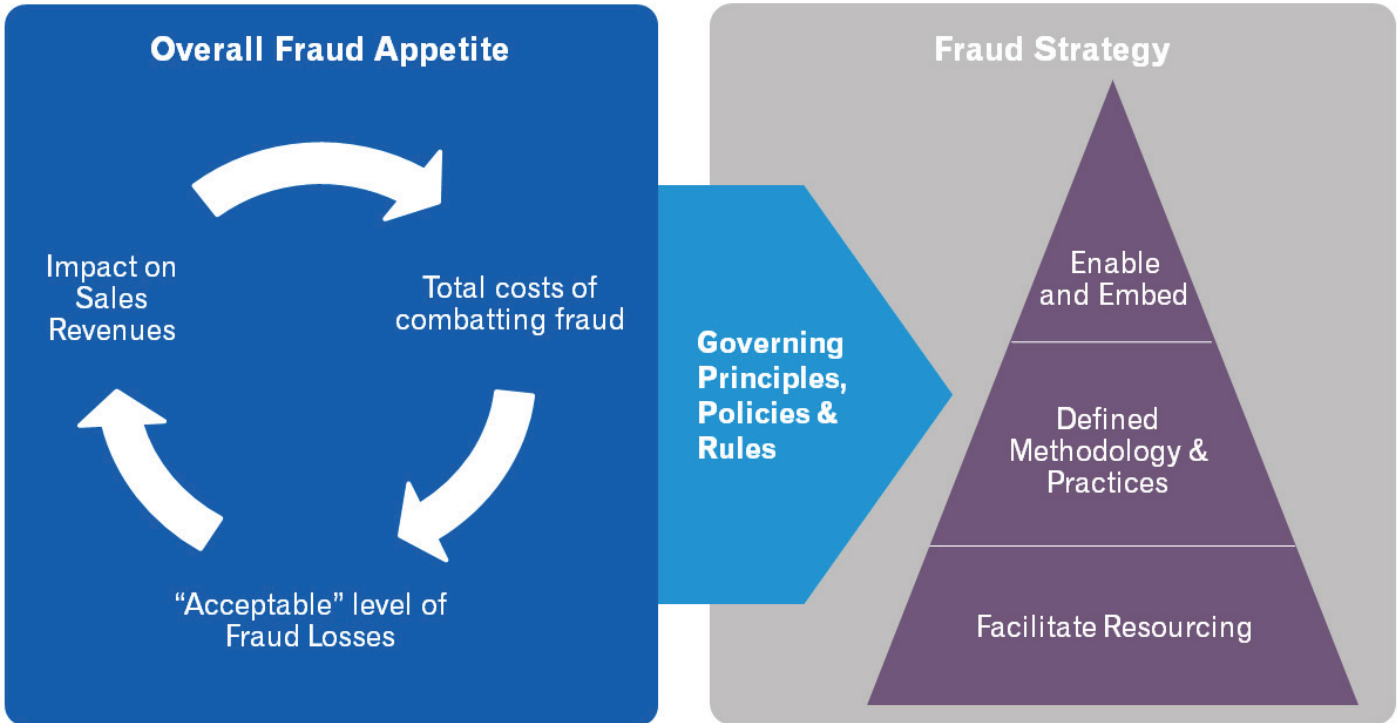
Firstly, the overall level of fraud losses would need to be quantified. For many organisations this is not quite as straightforward as it sounds. This is because a proportion of an organisation's fraud losses may be hidden in their bad debt book. Typically, between five percent and 20 percent of an organisation's bad debt is unrecoverable fraud.

Secondly, an assessment of the potential impact of combatting fraud on the organisation's customer acquisition and sales revenues objectives would need to be made. This would need to consider such aspects as channel growth and cross border activity, both of which would hold potentially significant implications on fraud risk exposure.

Thirdly, consideration would need to be made of the costs of identifying, investigating and managing fraud.

Having completed an assessment of the impacts of fraud, organisations should seek to define the level of fraud that it is prepared to accept in achieving its revenue, customer acquisition and customer management strategies. Often this is accompanied by a set of guiding principles.

The statement and the accompanying principles can then be used to develop more detailed policies and rules as well as informing day-to-day decision making by managers across the business and to shape and inform resourcing, practices and processes.



These principles and policies can then be used to shape the board's ongoing activities regarding:

- Providing the organisation with appropriate resources (systems, data, expertise etc.) to support the strategy
- Defining the methodologies and practices to be used to support the strategy
- Enabling managers to implement the strategy and build a fraud risk awareness culture across their individual teams

Having defined the fraud risk threshold, it is vital that this is communicated across the organisation and regularly reviewed to ensure that it remains fully aligned with the organisation's overall strategy.

Capability 4: Data optimisation

Access to appropriate data and data analytics resources are critical to effective fraud risk control. To successfully operationalise the strategy will require:

- Access to internal data (which may be spread across multiple systems), and to combine it with appropriate external data
- Access to appropriate data analytics tools
- The development of fraud models and scorecards that are reflective of the principles , policies and rules defined by the board
- The development of systems that can support automated decisioning

The collective effect of this will be to enable organisations to move beyond manual yes / no decisioning based on credit policy alone and to deliver consistent and measurable results.

> Over the past several years, we have seen a marked rise in the number of major frauds discovered through data analytics. Moving forward, we expect more organisations to build on this success story, and use these leading data analytics tools to help detect and mitigate fraud.

Capability 5: Operationalised risk management practices

A well-crafted statement of the organisation's overall threshold for fraud and the accompanying principles, policies and rules will help the business understand what it has to do, but the quality of how this activity is implemented and operationalised is the next critical capability.

Effectively operationalised risk management practices will help deliver ongoing value through:

- The establishment of process certainty by integrating and automating workflow across multiple business areas
- Enabling fraud risk management to be highly responsive and capable of addressing identified gaps in fraud risk control as they emerge
- Enabling fraud risk management to proactively identify and mitigate risks before they threaten the organisation.

Capability 6: The development of defined, visible customer journeys

Hand in hand with the operationalisation of fraud risk control capabilities will go the development of clearly defined customer journeys which have been agreed by the business through the appropriate fraud risk control governance structures created within capability 2.

This will bring value from the following perspectives:

The process of securing agreement by the business and of bringing clear definition and visibility to customer journeys will ensure the alignment of all parts of the organisation.

In turn, this will help ensure that the organisation's revenue growth requirements are balanced with its appetite for fraud in a manner that is consistent with the organisation's brand values and customer experience objectives.

Finally, this process will help identify and remove or manage the risk of unintended consequence associated with poor, ineffective and unsecure customer journeys.

Capability 7: Culture and awareness

Fraud prevention often requires non-technical processes and tools – for example training and awareness.

To make this happen, effective fraud risk control needs to become embedded into business-as-usual with all employees aware of its importance, as well as their individual roles and responsibilities in its delivery.

An embedded culture of fraud risk control will help create significant value for the business through:

- Increased efficiency where people fully understand the rationale for fraud

- Increased proactivity and early identification of suspicious activity resulting from heightened awareness
- Increased openness and transparency regarding critical issues and challenges facing the organisation and the role of all employees in successfully addressing them
- Reduced reputational risk through damaging effects on customer service or regulatory compliance
- Increased consistency of decisioning and customer journeys.

To bring this about requires the winning of hearts and minds which will involve aligning activity on multiple fronts including:

- Ensuring consistency of leadership behaviours from the senior leadership team in endorsing fraud risk control, and the key supporting principles that underpin the organisation's fraud risk strategy
- Developing an ongoing programme of general awareness raising
- Best practice identification, training and adoption
- Ongoing transparent communications which highlight progress made and challenges in equal measure
- The promotion of collective and individual responsibility within performance management processes.

Benchmarking and developing fraud risk control capabilities

It is vital that leaders are able to identify the required capabilities and do everything they can to foster their development.

Having identified the required capabilities, it will be important for the leadership team to jointly agree how well developed these capabilities currently are and what level of development they aspire to achieve.

Through our work in helping to develop these capabilities we have been able to identify the following fraud risk control maturity model.

By defining and benchmarking its required fraud risk control capabilities, your organisation will effectively have defined its expectations regarding "what does good look like." This will enhance your ability to align potentially divergent stakeholders by encouraging them to design their own business domains around these expectations.

Capability definition and benchmarking will also help give confidence and assurance that any future investments in people and systems or other capabilities will secure the maximum possible impact on risk control performance.

INCREASING CAPABILITY MATURITY					
KEY CHARACTERISTICS	INITIAL	REPEATABLE	DEFINED	MANAGED	OPTIMISED
	Ad hoc processes Not repeatable or scaleable	Signs of repeatable processes but breakdown in times of stress Increasing stakeholder engagement	Established governance structures Documented standards Road-tested procedures	Dedicated MI reporting Process adaptability Adoption of best practice	Ongoing virtuous circle of insight informing improvement and innovation Culture change
	DEPENDENCY on heroic efforts of a few key people	DEPENDENCY on increased awareness and planning	DEPENDENCY on management interaction based on established practices	DEPENDENCY on systems and process performance	DEPENDENCY on dynamic capabilities that can support ongoing process improvement

The following table considers the relative levels of maturity that typically relates to each of the seven capabilities that we have identified within this white paper.

	FRAUD CAPABILITY MATURITY MODEL				
	INITIAL	REPEATABLE	DEFINED	MANAGED	OPTIMISED
LEADERSHIP	Un-coordinated attempts to develop response to fraud Inconsistent understanding of implications of fraud risk for the business	Increasing recognition of vulnerabilities created by parochial self-interest Collaborative leadership Recognition of need for governance	Support for centrally co-ordinated programme of process definition, and integration across the business	Internal and external capability benchmarking Ongoing commitment to capability development	Commitment to ongoing programme of acquisition of internal and external insight to enhance understanding of evolving fraud risk
GOVERNANCE	Informal and undisciplined practices Ad hoc definition of fraud risk policies and controls Unpredictable results	Increasing co-ordination and alignment of roles and responsibilities Basic management controls and reporting structures established Development of MI	Establishment of cross organisation Fraud Committee Development of shared "strategic KPIs" across multiple business areas Activity frameworks established across multiple business areas	Clear linkage of strategic activities and performance outcomes Strategic KPIs centrally managed, measured and controlled Fraud MI reporting shared across the organisation	External benchmarking of organisational capabilities Multi country standardisation Committee initiates on-going regular reviews across all aspects of the organisation's fraud risk control activities
APPETITE	Lack of understanding of total effect of fraud on losses, costs and sales revenue	Creation of a fraud vision statement shared across the business Centrally co-ordinated development a set of fraud principles to support the vision and help guide managers in its implementation Increased harmonisation of policies and procedures	Organisation develops an accurate understanding of the total effects of fraud Introduction of defined appetite for fraud Defined processes monitoring, referral and investigation processes and methodologies to support the strategy	All additional resourcing and expertise requirements are fully reflective of the overall strategy for fraud risk control Fraud risk appetite periodically reviewed	External benchmarking of fraud risk exposure Accurate longer term forecasting of fraud performance indicators
DATA OPTIMISATION	Limited data retrieval capability to unlock existing internal data	Increased access and exploitation of the value of internal data Increasing use of analytics begins to reveal hidden cost and effects of fraud	Enhanced data retrieval capability Ability to integrate data across new and existing channels of customer engagement	Establishment of analytical structures to support data mining Adoption of data driven solutions for referral and investigation	Connection of multiple data sources to investigative matching capabilities via a single processing point External sectoral or national data sharing
OPERATIONALISED RISK MANAGEMENT PRACTICES	Ill defined "Work-arounds" Fraud risk controls development largely reactive	Focus on building consistency and repeatability Basic processes defined Breaches in fraud risk control inform on-going process improvement Increasingly proactive approach	Operationalised risk management process Agile risk controls to keep up with emerging fraud practices Regular vulnerability testing and process level risk assessment	Recognition and understanding of how processes interrelate to support the strategy Process performance becomes predictable Increased ability to develop counteractive fraud control measures more effectively	Closed loop of investigation, detection and improvement of gaps in fraud control Root cause analysis of security breaches to identify gaps in risk control Best in class integrated workflow and investigative case management
CUSTOMER JOURNEYS	Fragmented customer journeys Customer journey definition routinely fails to account for all scenarios and processes	Lack of standardisation and uniformity but move towards consistency	Defined customer journeys reflecting all organizational processes	Smooth, efficient and quick customer journeys across all channels Common understanding of key risk points and consistent referral processes	Ability to enhance and improve customer journeys in response to customer feedback without compromising security Minimal customer fall off rates
CULTURE AND AWARENESS	Effective fraud risk control reliant on entrepreneurial spirit and "heroic efforts" Reactive Little awareness of the overall business environment and the impact of fraud upon it	Increased understanding of fraud and its effects Best practices identified but patchy adoption Increased awareness of the level of fraud within the business	Increased sharing of insight and best practice All managers fully understand their role and contribution to the organisation's effective fraud risk control On-going fraud awareness programme	Best practice routinely identified, shared and embedded Early problem recognition Continuous monitoring and improvement On-going communications programme to re-enforce culture of fraud risk control	Empowerment and responsibility All employees fully understand their role and contribution to the organisation's effective fraud risk control

Next steps: Moving from capabilities to activities

Fraud is a mounting problem, but Experian has the tools, technology, insight, and expertise to tackle it. With the proper prevention system in place, organisations can avoid unnecessarily expensive, crippling problems later on. This will be an ongoing challenge for organisations in all sectors, but it shouldn't cost tens of billions or cause a major problem for millions of people worldwide.

Having identified the organisational capabilities, the supporting activities need to be defined and implemented across the business so that you can gain control of fraud at a strategic level.

Experian's fraud consultants work with organisations to develop a strategic response to fraud, helping to define a fraud risk strategy; identify and prevent fraud; and review and improve existing fraud strategies to keep up with current and emerging threats.

For additional information on how to tackle and control fraud, please visit www.experian.com/da.

About Decision Analytics

Experian Decision Analytics enables organisations to make analytics-based customer decisions that support their strategic goals, so they can achieve and sustain significant growth and profitability. Through our unique combination of consumer and business information, analytics, decisions, and execution, we help clients to maximise and actively manage customer value.

Meaningful information is key to effective decision-making, and Experian is expert in connecting, organising, interpreting and applying data, transforming it into information and analytics to address real-world challenges. We collaborate closely with clients to identify what matters most about their business and customers, then create and implement analytics-based decisions to manage their strategies over time.

In today's fast-paced environment where developing, implementing, and sustaining an effective strategy is imperative, Experian Decision Analytics helps organisations unlock a wealth of benefits immediately—and set the stage for long-term success.

Increased revenue: Our products and services enable clients to increase revenue by providing the insight and agility they need to find and engage the right customers, target products more effectively, and grow market share.

Controlled risk: A broad range of risk-management products and services help organisations verify identity and manage and detect fraud, optimise collection and recovery, and balance risk and reward.

Operational efficiency: Experian Decision Analytics helps organisations quickly integrate various information and processes to enhance operational efficiency and boost agility. Our flexible, collaborative approach helps organisations increase speed to market, enhance business agility and improve the quality of customers' experiences.

Compliance as differentiation: Proven expertise lets clients use compliance as a source of competitive advantage. Experian Decision Analytics helps ensure compliance with essential regulations, while helping organisations better understand customers.

About the Author

Liam Rawsthorne

Liam Rawsthorne is Head of Fraud Consultancy for Experian EMEA. He joined Experian in 2008 from the telecommunications industry in the UK where he spent 20 years working with fixed and cellular, primarily with Telefonica O2 but has managed fraud in micro finance, retail/personal finance and an ISP. Liam has managed every aspect of Fraud and Security, from operational fraud management, strategy, investigations, internal, channel fraud risk, government and law enforcement agency liaison and physical security etc.

Prior to working in fraud risk Liam worked within the government sector holding positions with the Citizens Advice Bureau and the UK's Crown Prosecution Service.

www.experian.com/da