CRI | GROUP
Corporate Research and Investigations

PLAYBOOK

ENABLE BETTER RISK MANAGEMENT

Uncertain Times Demand a New Approach to Risk

Risk management is a full-time, ongoing endeavour for organisations in today's business world, and it poses constant challenges. The first part of reducing risk is having a strategy, and taking action. This Playbook is key to help you in any decision-making.

CRI | GROUP
Corporate Research and Investigations

HELPING YOU MAKE INFORMED, SOUND DECISIONS

Since 1990, Corporate Research and Investigations Limited (CRI Group) has been safeguarding businesses from fraud and corruption, providing employee background screening, insurance fraud investigations, investigative due diligence, third-party risk management, compliance and other professional investigative research services. Globally, we are a leading Compliance and Risk Management company licensed and incorporated entity of the Dubai International Financial Center (DIFC), Abu Dhabi Global Market (ADGM) and Qatar Financial Center (QFC). CRI Group protects businesses by establishing the legal compliance, financial viability, and integrity levels of outside partners, suppliers and customers seeking to affiliate with your business.

Based in London, United Kingdom, CRI Group is a global company with experts and resources located in key regional marketplaces across the Asia Pacific, South Asia, the Middle East, North Africa, Europe, North and South America. Our global team can support your organisation anywhere in the world.

The international nature of business today dictates an increasing demand for proactive measures such as global investigations, compliance & risk management solutions to reduce the exposure to organisations of economic crime and civil wrongs, particularly in the financial, government and multinational business sectors.

Are you making informed sound decisions regarding M&A, strategic partnerships & selection of employees, vendors or suppliers?

→ **Visit CRIGroup.com.**

Part One:
RISK MANAGEMENT

Effective risk management has many different elements. These include having an ethical code of conduct, regular risk assessments, proper third-party due diligence, thorough background screening and other important processes.

In Part One of the Playbook, we'll explore how these tools can be implemented to help better protect your organisation. Every risk management strategy is different, depending on the size, industry and location of the organisation. But there are best practices and expert tools that will help any organisation immediately.

WHAT IS RISK?

The Oxford English Dictionary (OED) defines risk as: "(Exposure to) the possibility of loss, injury, or other adverse or unwelcome circumstance; a chance or situation involving such a possibility."

The Cambridge Advanced Learner's Dictionary gives a simple summary, defining risk as *"the possibility of something bad happening".*

However the definitions of risk differ in the business practice; risk can be perceived either positively (upside opportunities) or negatively (downside threats). A risk is the potential of a situation or event to impact on the achievement of specific objectives.

The International Organization for Standardization (ISO) Guide 73 provides basic vocabulary to develop common understanding on risk management concepts and terms across different applications. ISO Guide 73:2009 defines risk as:

"effect of uncertainty on objectives"

Note 1: An effect is a deviation from the expected – positive or negative.

Note 2: Objectives can have different aspects (such as financial, health and safety, and environmental goals) and can apply at different levels (such as strategic, organisation-wide, project, product and process).

Note 3: Risk is often characterised by reference to potential events and consequences or a combination of these.

Note 4: Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated likelihood of occurrence.

Note 5: Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of, an event, its consequence, or likelihood.

This definition was developed by an international committee representing over 30 countries and is based on the input of several thousand subject matter experts. It was first adopted in 2002. Its complexity reflects the difficulty of satisfying fields that use the term risk in different ways.

WHAT IS RISK MANAGEMENT?

Risk management is focused on anticipating what might not go to plan and putting in place actions to reduce uncertainty to a tolerable level. The international standard definition of risk for common understanding in different applications is "effect of uncertainty on objectives" (Guide 73:2009 Risk Management - Vocabulary". ISO)

The understanding of risk, the methods of assessment and management, the descriptions of risk and even the definitions of risk differ in different practice areas (business, economics, environment, finance, information technology, health, insurance, safety, security etc). This book provides links to more detailed articles, whitepapers and ebooks on these areas. The international standard for risk management, ISO 31000, provides a common approach to managing any type of risk (ISO 31000:2018 Risk Management - Guidelines, ISO.)

Working with the risk owner, the project professional ensures that risks are clearly identified before moving on to the risk analysis step of the risk management process.

The project risk management process reflects the dynamic nature of projectwork, capturing and managing emerging risks and reflecting new knowledge in existing risk analyses.

A risk register is used to document risks, analysis and responses, and to assign clear ownership of actions.

In a risk environment that is growing more perilous and costly, boards need to help steer their companies toward resilience and value by embedding strategic risk capabilities throughout your organisation.

HOW IS RISK MANAGEMENT EVOLVING TO TACKLE MODERN CHALLENGES?

Risk management's profile is rising and evolving to become an integral part of the business. No longer simply a siloed middle-office function, risk is moving into the front office and becoming key to conducting business. As trading and risk merge closer together, there's a greater need for more streamlined, integrated risk management processes that work in harmony throughout the organisation, draw on a single source of data and deliver a complete view of risk across asset classes.

At the same time, the risk function is exploring new ways to do more with less, especially when it comes to supporting complex risk metrics. Over the past decade, for regulatory compliance and competitive advantage, many organisations were quick to adapt. You should be looking to do the same. Calculating risk with greater accuracy can help improve your bottom line. But the work involved can also stretch your resources and potentially push up your costs.

PRINCIPLES OF RISK MANAGEMENT

to have effective risk management,
an organisation has to comply with 11 principles:

1. Risk management **creates & protects value**
2. Risk management is **part of decision making**
3. Risk management is **systematic, structured & timely**
4. Risk management is **transparent & inclusive**
5. Risk management **takes human & cultural factors into account**
6. Risk management is **tailored**
7. Risk management is based on the **best available information**
8. Risk management **explicitly addresses uncertainty**
9. Risk management **facilitates continual improvement** of the organisation
10. Risk management is an **integral part of all organisational processes**
11. Risk management is **dynamic, iterative & responsive to change**

At CRI Group we belive in simplify risk management, we can help you with a wide range of risk management solution, regardless of the size, nature, or location of a business. Public, private and community enterprises can all benefit from a risk management strategy because it covers most business activities, including research, planning, management and communications. Implementing a risk management plan can help organisations increase the likelihood of achieving objectives, improve the identification of opportunities and threats and effectively allocate and use resources for risk treatment.

GET A FREE QUOTE NOW!

BUSINESS RISKS EVERY ORGANISATION SHOULD PLAN FOR

Building a business takes work—and risks. But some risks are more dangerous than others. Here are a few risks that every business owner should keep in mind. Running a business takes hard work, which can reap the rewards of customers, revenue and satisfaction. While success is the ultimate goal, business risk may stop you from achieving the goals you set. When it comes to risk management, there are steps you can take, however. Here are seven types of business risk you may want to address in your company.

1. Economic Risk

The economy is constantly changing as the markets fluctuate. Some positive changes are good for the economy, which lead to booming purchase environments, while negative events can reduce sales.

It's important to watch changes and trends to potentially identify and plan for an economic downturn. To counteract economic risk, save as much money as possible to maintain a steady cash flow. Also, operate with a lean budget with low overhead through all economic cycles as part of your business plan.

2. Compliance Risk

Business owners face an abundance of laws and regulations to comply with. For example, recent data protection and payment processing compliance could impact how you handle certain aspects of your operation.

→ **For more on data compliance read: "GDPR, Everything You Need to Know" and "GDPR: A 21st Century Approach to compliance"**

Staying well versed in applicable laws from federal agencies like the Occupational Safety and Health Administration (OSHA) or the Environmental Protection Agency (EPA) as well as state and local agencies can help minimise compliance risks. If you rely on all your income from one or two clients, your financial risk could be significant if one or both no longer use your services. Start marketing your services to diversify your base so the loss of one won't devastate your bottom line.

Non-compliance may result in significant fines and penalties. Remain vigilant in tracking compliance by joining an industry organisation, regularly reviewing government agency information and seeking assistance from consultants who specialise in compliance.

3. Security and Fraud Risk

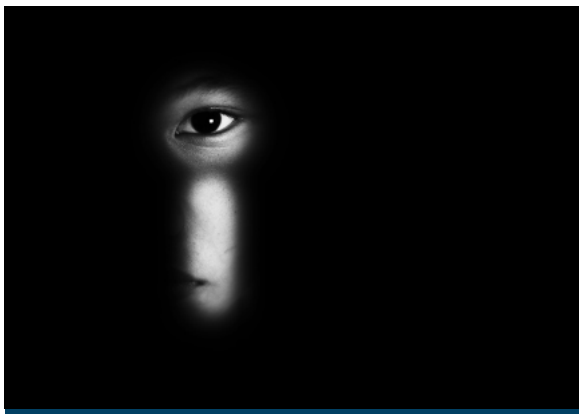
As more customers use online and mobile channels to share personal data, there are also greater opportunities for hacking. News stories about data breaches, identity theft and payment fraud illustrate how this type of risk is growing for businesses. Not only does this risk impact trust and reputation, but a company is also financially liable for any data breaches or fraud.

To achieve effective enterprise risk management, focus on security solutions, fraud detection tools and employee and customer education about how to detect any potential issues.

4. Financial Risk

This business risk may involve credit extended to customers or your own company's debt load. Interest rate fluctuations can also be a threat. Making adjustments to your business plan will help you avoid harming cash flow or creating an unexpected loss.

Keep debt to a minimum and create a plan that will start lowering that debt load as soon as possible. If you rely on all your income from one or two clients, your financial risk could be significant if one or both no longer use your services. Start marketing your services to diversify your base so the loss of one won't devastate your bottom line.



DEBUGGING FEARS THAT PARALYZE FRAUD PREVENTION

Often, an organisation doesn't put a robust process in place until it's in the news with a violation, an FCPA incident or an internal case of undetected embezzlement that might have gone on for years. But why? As money walks out the door, why wouldn't companies adopt a more proactive stance for early detection?

The answer is fear. Fear can prevent a mom-and-pop shop or a Fortune 500 industry leader from becoming serious about fighting fraud. Business analytics and portal systems certainly enable companies to more quickly mine through volumes of data and identify red flags, yet they're not a requirement for fraud prevention. Depending on the size of the company, it can data mine and detect fraud early with such basic tools as Microsoft Access and Excel. And while companies pay lip service to efforts to fight fraud, they're often slow to take advantage of even these most elementary methods. Read more about the fear factor that play into the decision — or indecision — to fight fraud.

READ MORE

5. Operational Risk

This business risk can happen internally, externally or involve a combination of factors. Something could unexpectedly happen that causes you to lose business continuity. That unexpected event could be a natural disaster or fire that damages or destroys your physical business. Or, it might involve a server outage caused by technical problems, people, or power cut.

Some reasons for operational risk include the following:

- Internal fraud
- External fraud
- Employment practices
- Client and business practices
- Business continuity practices

→ **Learn more about the "Top Risk Management Concerns and The Need for Leadership During COVID-19"**

Many operational risks are also people-related. An employee might make mistakes that cost time and money. Whether it's a people or process failure, these operational risks can adversely impact your business in terms of money, time and reputation. Address each of these potential operational risks through training and a business continuity plan. Both tactics provide a way to think about what could go wrong and establish a backup system or proactive measures to ensure operations aren't affected.

→ **Investigative operations (via commercial investigations) focus on the current status of your business – i.e. location of assets, financial information, identification of unmet needs of any market, gauge brand awareness and identity in the market, etc.) Learn more about HERE!**

For example, more businesses are using cloud storage to protect company data and rely on remote team members to maintain operations. Automating more processes also helps to reduce people failures.

6. Reputational Risk

There has always been the risk that an unhappy customer, product failure, negative press or lawsuit can adversely impact a company's brand reputation. However, social media has amplified the speed and scope of reputation risk. Just one negative tweet or bad review can decrease your customer following and cause revenue to plummet. To prepare for this risk, leverage reputation management strategies to regularly monitor what others are saying about the company online and offline.

Be ready to respond to those comments and help address any concerns immediately. Keep quality top of mind to avoid lawsuits and product failures that can also damage your company's reputation.

7. Competition (or Comfort) Risk

While a business may be aware that there is always some competition in their industry, it's easy to miss out on what businesses are offering that may appeal to your customers. In this case, the business risk involves a company leader becoming so comfortable with their success and the status quo that they don't look for ways to pivot or make continual improvements. Increasing competition combined with an unwillingness to change may result in a loss of customers.

Enterprise risk management means a company must continually reassess their performance, refine their strategy, and maintain strong, interactive relationships with their audience and customers.

Additionally, it's important to keep an eye on the competition by regularly researching how they use online and social media channels.

→ **Business Intelligence is most effective when it combines data derived from the market in which your business operates in (external) with data from within such as financial and operations data (internal). When combined, this data can provide a complete picture so that you can make any business decision ranging from operational to strategic – such as product positioning or pricing. Learn more about HERE!**

Business Intelligence is most effective when it combines data derived from the market in which your business operates (external) with data from within such as financial and operations data (internal). When combined, this data can provide a complete picture so that you can make any business decision ranging from operational to strategic – such as product positioning or pricing.

What is Business Intelligence?

Business Intelligence Solutions take many shapes and forms in today's complex business environment. Budgets are stretched and the challenges facing a business and its employees can sometimes lead to issues that start off small, but then lead to wider spread problems which can affect the very fabric of your organisation and damage both your credibility, reputation and bottom line profits.

CRI® takes two approaches to BI solutions:

- Intelligence operations (via market research and analysis): we focus on researching the future and potential growth of your business – i.e. determine the commercial viability and potential for success in the market, analyse consumer behaviour and business trends in that market, etc.
- Investigative operations (via commercial investigations): we focus on the current status of your business – i.e. location of assets, financial information, identification of unmet needs of any market, gauge brand awareness and identity in the market, etc.)

GET A FREE QUOTE NOW!

WHY IS RISK MANAGEMENT ESSENTIAL?

Trust and reputation are a critical part of the relationship between an organisation and its stakeholders. Simple compliance does not fully meet the expectations most stakeholders have with their organisations, and so it is important that entities demonstrate a fuller commitment to effective risk management. A risk management plan is a perfect way to show that commitment:

Establish a reliable basis for **decision making**

Improve **organisational effectiveness & efficiency**

Improve the **identification of opportunities & threats**

Improve organisational **resilience**

Increase the likelihood of **achieving objectives**

Trust your workforce and your business relationships

As with all major undertakings within an organisation, it is important that executives and management be fully involved and support the risk management process. The benefits can be communicated and illustrated to them, as well as the negative effects of not having such a framework in place. Understanding the risks faced by the organisation is the first step in protecting it from harm.

GET A FREE QUOTE NOW!

With a risk management plan in place, your organisation will have benefits in a number of areas, examples of which include:

Compliance with all relevant legal & regulatory requirements & international norms

Improved stakeholder confidence & trust

It is a clear indicator to your customers, & other stakeholders that as an organisation, you are committed to managing risks in every part of your business.

Establishment of a reliable basis for decision making & planning

Improved mandatory & voluntary reporting

Effective allocation & use of resources for risk treatment

It can be used by organisations to compare their risk management practices with an internationally recognised benchmark, providing sound principles for effective management & corporate governance.

Guidance for internal or external audit programmers.

In competitive bidding for commercial tenders, it will enhance your company's reputation & give you a competitive advantage.

Increased likelihood of achieving objectives

Improved governance

Encouraged proactive management

Improved identification of opportunities & threats

Awareness of the need to identify & treat risk throughout the organisation

Improved controls

Part TWO:
RISK MANAGEMENT SOLUTIONS

Become more resilient by making every risk known!

In Part Two of the Playbook, we'll explore how an effective risk management plan can be achieved and implemented through several services including due diligence and background screening.

HOW RISK MANAGEMENT & DUE DILIGENCE INTERLOCK?

These are challenging and complex times. COVID-19 is forcing organisations to adapt quickly and change their business model in the process. In an era of compliance, with many regulations and regional "interpretations", leaders and organisations need to be careful about how they conduct business, who conducts business in their name and with whom. This demands extraordinary attention to the means and mechanisms used by the organisation.

Due diligence, in legal terms, entails taking reasonable steps to satisfy any legal or regulatory requirement, regardless of size or type of business conducted.

Businesses also need to take any of a number of mandated steps to ensure that the organisation remains safe from any unwanted or unauthorised action taken in their behalf. For example, when making an investment such a merger or an acquisition, the organisation needs to take the appropriate action on the proper due diligence necessary to make the most informed decision possible.

Being casual about the due diligence process is a failure to execute the proper level of investigation regarding the assets being purchased or financed or the management team being backed and vetted.

Where Risk Management Comes into Play

Risk management is the identification, evaluation, and prioritisation of risks (defined in ISO 31000 as the effect of uncertainty on objectives) followed by coordinated and economical application of resources to minimise, monitor, and control the probability or impact of unfortunate events or to maximise the realisation of opportunities.

A formal business discipline that relies on the forecasting and evaluation of any risks, along with identification and (where feasible or warranted) implementation of procedures to avoid or minimise their impact.

Risks can come from various sources including your employees. From a risk management perspective, the penalties on conducting business that can result from unwanted or unauthorised third-party relationships or any employee unethical business action are very high—making it imperative to perform due diligence when trying to protect your business and brand.

Inadequate due diligence can easily take down an organisation; from damaged reputation to brand devaluation, from regulatory violations to fines and jail terms for directors, the risks are very high.

The risks from losses of such potential magnitude should not be ignored. At such cost, implementing the most stringent and effective controls and protections in place even at a cost STILL makes absolute financial sense. And the only way to fully protect a corporation's assets, therefore, is through a strong and viable 360 due diligence program.

→ **Learn more about "When is due diligence most critical?"**

Managing risk and due diligence should begin with a policy and a plan. Here we will focus on the human element of risk management, specifically background investigations.

Organisations need to perform due diligence to make sure that their business is adequately conducted by their employees and through their partners' and vendors. Such insurance invariably includes regular security audits, ISO certification, pre-employment background checks, TPRM, etc...

There are several incentives to practice due diligence and perform risk management to ensure you conduct business appropriately and comply with all applicable laws and regulations. Anything less is just asking for trouble and losses!

What Can (and Should) Organisations and Risk Professionals Do?

The very first step to mitigating risks and exposures starts with a risk assessment. There are plenty of risk assessment checklists and tools available. If you want to dive deeper into how to start a risk assessment, just read our "Risk assessment breakdown: Identification, Analysis, Evaluation" to learn more. Once risk professionals get a handle on their due diligence processes and other compliance regimes, it's time to start the entry process into the regulatory life cycle:

- Prioritisation and planning
- Implementation of a response
- Integration of related tools, technologies, audits, processes and procedures to integrate compliance into normal operations

The first steps toward achieving compliances are usually big ones and may require substantial time and effort. But after that, it's just a matter of sticking to a routine to maintain compliance, meet reporting requirements and keep up with changes to governing regulations and day-to-day tools and operations.

GET A FREE QUOTE NOW!

Case Study: DUE DILIGENCE EXPOSES FRAUDULENT BUSINESS

A multinational company engaged in the provision of equipment and supplies used by the medical industry contacted CRI®. The client wished to contract with a company founded in Egypt (and also having operations in Iraq). Before entering into contractual arrangements, the client wanted to ensure that there are no regulatory or reputational problems associated with the business in Egypt, and thus wanted to know their track record, integrity and reputation.

During the course of this integrity due diligence, CRI® local operatives focused on whether the company in question was a legitimate business, and sought to identify the key players running operations both in Egypt and Iraq for the company in question. However, no information was found from local industry resources; specifically, corporate registration authorities, local chamber of commerce, etc. to support that the company was who they claimed to be.

More questions arose as the experts worked to find out more about their backgrounds, political connections, and reputation. Research showed no physical locations; the office address was found to be a residential site with no indication of business operations. No commercial relationships in Iraq were evident.

Local operatives further investigated the company's distribution capabilities in the country, especially to the north and south, as claimed in a questionnaire provided to the client. Yet no information was found from any source to corroborate the company's claims. Additionally, discreet interviews with local individuals found that no one was aware of the company.

Things just weren't adding up in a positive way in trying to establish that the company was a legitimate business. Skepticism was confirmed when a local agent researched court and police resources, finding that the company's principal was previously charged with "criminal breach of trust" and there was still a trial proceeding with regional trial courts. Three other civil damages claims against the principal were discovered, with USD $1.2 million claimed in liabilities.

When this evidence was presented to the client, CRI®helped them avoid becoming entangled with a fraudulent business and an alleged criminal – protecting the client from making a bad business deal that could have resulted in severe economic loss and a potentially damaged reputation.

→ **Check out CRI® Insights! Find publications including white papers and case studies.**

Have a **lack of visibility** or understanding danger of the risks posed by your relationships with many types of third parties?

Want **greater visibility into third-party performance and risks**?

Need to improve operational costs, process, efficiencies, and organisational agility?

Need to **gain greater control** over the risks?

Want to be confident that third parties are compliant with your business' policies, as well as their own—based on government regulations and industry requirements?

YES, I COULD USE THE HELP

3PRM™ THIRD-PARTY RISK MANAGEMENT

CRI Group's own exclusive, expert-developed 3PRM™ services help you proactively mitigate risks from third-party affiliations, protecting your organisation from liability, brand damage and harm to the business. Whether your organisation has a large, well-established third-party program, is in the early stages of development, or is anywhere in between, 3PRM™ solution can improve the health of your program and future-proof your entire business in many forms.

Our 3PRM™ solution streamlines the third-party risk management process through scalability, and efficiencies – from third-party risk identification to assessment what sets us apart is that our 3PRM™ solution includes:

- **Due Diligence**
- **Screening & background checks**
- **Business intelligence: information management**
- **Investigations: i.e. IP, fraud, conflict of interest, etc**
- **Regulatory compliance**
- **Anti-bribery and anti-corruption (ABAC) compliance**
- **Employee auditing training & education**
- **Monitoring & reporting**

GET A FREE QUOTE NOW!

From cybersecurity to anti-bribery, our solution is flexible and responsive to the various risk domains that are most important to your business. With a network of trained professionals positioned across five continents, CRI Group's 3PRM™ services utilise one of the largest multi-national fraud investigation teams the industry has to offer.

TOP 10 THINGS YOU MUST KNOW BEFORE CONDUCTING A MERGER OR ACQUISITION

Mergers, acquisitions and related major business transactions are often indicators of expansion and success for organisations. This can be an exciting time, with business growth being one of the inherent goals among most organisations and their leaders. It's also a time to be cautious, however. There are plenty of risks – some apparent, some hidden – when engaging in mergers and acquisitions. At such a critical juncture, conducting thorough, comprehensive due diligence is the key to mitigating those risks. **Here are 10 important things every organisation should know before conducting a merger or acquisition:**

1

THE COMPANY YOU ARE ACQUIRING MIGHT BE OVERVALUED:

Have financials been inflated? Assets overvalued? 60% of financial professionals say overpaying for deals is the biggest risk facing buyers, according to a 2016 survey conducted by the Financial Executives Research Foundation. A proper investigation including site visits and an expert review of financial information can help mitigate this risk factor.

2

THE ORGANISATION MIGHT BE INVOLVED IN BEHIND-THE-SCENES LEGAL BATTLES:

Your growth strategy probably doesn't involve taking on another entity's legal entanglements. Proper due diligence can help uncover legal filings, liabilities and even criminal action that might not have been disclosed up front in merger or acquisition negotiations.

3

COMPANIES IN FOREIGN JURISDICTIONS MIGHT PLAY BY DIFFERENT RULES:

Proper due diligence can help you avoid becoming partnered with an organisation that treats bribes, kickbacks and other illegal activity as "business as usual." Such conduct will affect your own organisation in several ways, including causing harm to finances and reputation while also having obvious legal consequences.

4

CULTURAL DIFFERENCES CAN CAUSE BUSINESS PROBLEMS:

International expansion is a key goal among many larger organisations. Mergers and acquisitions have failed, however, due to cultural clashes among employees. The preparation process should include a compatibility factor that takes cultural and social differences into account.

5

YOU MIGHT ABSORB NEW CREDIT RISK:

An organisation that is overextended, has claimed bankruptcy or is faced with debtor filings can become a serious detriment to your business. Comprehensive financial investigations will uncover these financial risks and help you move forward in a prudent fashion.

6

TRANSPARENCY IS KEY:

The terms of a merger or acquisition should be clearly spelled out and communicated clearly before finalising any deal. Discrepancies or misunderstandings can cause discontent among leaders and employees at either party (or both), which can cause the merger or acquisition to fail. Also, anti-bribery and anti-corruption policies should be implemented at this stage to determine any risk factors for the transaction.

7

FRAUD IS A RISK IN MERGERS AND ACQUISITIONS:

One of CRI Group's clients, a multinational corporation engaged in the provision of medical equipment and supplies, was looking to merge with a company based in the Middle East. CRI Group's due diligence experts helped the client avoid becoming entangled with what turned out to be a fraudulent business run by an alleged criminal. Merging with such an entity can result in severe economic loss and a potentially damaged reputation.

8

DATABASE CHECKS ARE IMPORTANT...

In the hands of the right experts, database checks are an enormous tool for conducting thorough due diligence. These can include local and regional business records, certifications, compliance records, criminal and court records and other documents and data. Some private services aggregate such records to make it easier to quickly find and review the information needed.

9

BUT SO ARE "BOOTS ON THE GROUND":

Skilled due diligence professionals know how to find data that large services just don't capture. Some records might only be accessible in their local principality. Certain broad results might require a deeper drill-down, including actions such as bankruptcy or civil or criminal cases against an entity. What really happened, and how are such cases likely to be resolved? Who are the main actors involved?

10

CONDUCT BACKGROUND CHECKS:

The principle players in a merger/acquisition should be vetted to help screen for fraud. Conducting thorough background checks on owners, directors and CEOs can help uncover any criminal records and other important information. Transparency in knowing who you are dealing with is key during the due diligence process.

MANAGING RISKS WITH EMPLOYEE BACKGROUND CHECKS / SCREENING

How do you know the candidate you just offered a role to is the ideal candidate? Are you 100% sure you know that everything they're telling you is the truth? 90%? They showed you a diploma, how do you know it's not photoshopped? Did you follow the correct laws during your background checks process?

Background checks and necessary screenings are vital to avoid horror stories and taboo tales that occur within HR, your business or even your brand – simply investing in sufficient screening can save you time, money and heartbreak.

CRI Group has developed EmploySmart™, a robust new pre-employment background screening service to avoid negligent hiring liabilities. Ensure a safe work environment for all – EmploySmart™ can be tailored into specific screening packages to meet the requirements of each specific position within your company. We are a leading worldwide provider, specialised in local and international employment background screening, including pre-employment screening and post-employment background checks.

GET A FREE QUOTE NOW!

FRAUD FACT:
Stretching employment dates is the most commonly seen form of resume fraud. Enhancing job titles and responsibilities, faking credentials, fabricating reasons for leaving the previous job, and unexplained gaps and periods of "self-employment" are other top methods of deception. Source: CRI Group survey, 2019.

TIP FOR SUCCESS:
58% of hiring managers said they've caught a lie on a resume; one-third (33%) of these employers have seen an increase in resume embellishments post-recession.

Source: CareerBuilder.com.

BACKGROUND SCREENING: ESSENTIAL CHECKS

Pre-employment background checks should dig deep enough (within the rules of local laws and regulations) to asses every detail of a job candidate's claims and credentials, to confirm that the claims match with the facts. **CRI Group's team of experts examine all of the following details of a potential employee:**

IDENTITY:

Some job candidates will actually fabricate a new identity, especially if they have something to hide. Proper screening can verify name, addresses, phone numbers, national ID numbers and other identifying information to confirm that they are who they claim to be.

EDUCATION & CREDENTIALS VERIFICATION:

Verification is needed to confirm school grades, degrees and professional qualifications.

CREDIT CHECKS & BANKRUPTCY CHECKS:

As permitted by local laws, financial and credit history should be reviewed, as fraud statistics have shown financial distress to be a key red flag for fraudulent behavior. Has the candidate claimed bankruptcy? Have they dissolved prior companies or are they faced with debtor filings?

CRIMINAL HISTORY:

International criminal records searches are critically important, and should include any convictions for the applicant in the requested jurisdictions.

PREVIOUS EMPLOYMENT VERIFICATION:

Background checks will verify past employers, locations of past employment, dates employed, salary levels, reasons for leaving, position titles, gaps in employment history and pertinent contact information.

TOP 10 THINGS EVERY ORGANISATION SHOULD KNOW ABOUT BACKGROUND SCREENING

1. Some job candidates will actually fabricate a new identity:

This is especially true if they have something to hide, such as a criminal background. Proper screening can verify names, addresses, phone numbers, national ID numbers and other identifying information to confirm that they are who they claim to be.

2. Credit and financial history should be reviewed:

Fraud statistics have shown financial distress to be a key red flag for fraudulent behavior. Has the candidate claimed bankruptcy? Have they dissolved prior companies or are they faced with debtor filings? An individual's financial history should be checked to the degree that is permissible by local laws.

3. Previous employment needs to be confirmed:

Background checks will verify past employers, locations of past employment, dates employed, salary levels, reasons for leaving, position titles, gaps in employment history and pertinent contact information.

4. Stretching employment dates is a major problem:

Speaking of previous employment, CRI Group's survey found that the top form of résumé fraud is stretching employment dates. This can cover gaps in employment, or make it seem they have more experience in certain positions than they actually do.

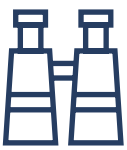
→ **Know how to protect your company from bad hiring decisions. Download the brochure, "EmploySmart: Smarter Background Checks Today for a Better Workforce Tomorrow."**

5. Some candidates present fake education credentials:

Verification is needed to confirm school grades, degrees and professional qualifications. Claiming a degree that was never earned is one of the most common fabrications. Certifications, assessments, awards – all of these can be fabricated or fraudulently claimed by a candidate in an effort to make themselves look more qualified for a position than they actually are.

6. International criminal records searches are critically important:

Criminal background checks should include any convictions for the applicant in the requested jurisdictions. Depending on their history, your business and employees could be at risk from a bad actor who intentionally hides their criminal past.



7. Checking (and verifying) references is important:

A job seeker might provide an employment reference that gives a shining recommendation – but the contact turns out to be their close friend. This type of deception can hide the true nature and work record of the candidate.

8. Formalise your background screening policy:

What is your company's current, written policy for hiring new employees? Having the process detailed in writing will help make it a regular part of your business practice.

9. Make sure someone owns the process:

Ultimately, who has the responsibility of vetting new hires? All of those who are involved in hiring should also be involved in the implementation of a due diligence solution that includes background checks.

10. Don't skip post-employment screening:

Proper due diligence doesn't just apply to prospective new hires. It should also be used to periodically evaluate your current workforce. Examine the various roles and personnel at your organisation, and consider a policy that addresses risk areas with background checks.

BACKGROUND SCREENING – FREQUENTLY ASKED QUESTIONS (FAQS)

WHY CONDUCT PRE-EMPLOYMENT BACKGROUND CHECKS?

In order to protect the company from various potential risks, a background check is considered an imperative pre-employment screening step before making a hiring decision. Most of the time, companies assume that applicants are telling the truth on their resumes – but what if they are not? These checks are essentially an investigation into a person's character – inside and outside of their professional lives. Some checks you probably already carry out in-house, such as: candidate's qualifications (documents provided), work history (with a reference check), right to work in the country and even a quick social media presence scan.

WHAT ARE SOME OF THE POTENTIAL CONSEQUENCES OF A BAD HIRING DECISION?

An organisation faces risks related to productivity, financial cost, time, reputation, and safety when it fails to properly screen candidates and hires underqualified or dishonest employees. Potential consequences include:

- Attrition and wasted hiring budgets
- Theft or embezzlement
- Damaged employee relations and morale
- Endangerment of employees, clients and business associates
- Lost productivity
- Litigation
- Public scandals and negative publicity

Source: hrzone.com

WHAT ADVANTAGES DOES PROPER BACKGROUND SCREENING PROVIDE AN ORGANISATION?

No organisation can afford to have employees on staff who aren't what they claim to be. Even a seemingly innocent embellishment can indicate more background problems under the surface, and the potential for future problems down the road. A robust background screening process provides an extra layer of security that helps to avoid hidden costs of making hiring mistakes – costs like loss of productivity, wasted budgets, damaged employee relations, negative publicity or other major consequences.

WHAT ARE THE MOST COMMON FABRICATIONS FOUND ON RÉSUMÉS?

There are many ways to embellish one's résumé, but these are the most common:

- Stretching dates of employment
- Omitting past employment
- Faking credentials
- Fabricating reasons for leaving the previous job
- Providing fraudulent references

HOW DOES BACKGROUND SCREENING UNCOVER FABRICATIONS IN EMPLOYMENT HISTORY?

Proper background screening will examine job titles, beginning and ending dates for each job listed, and will sometimes verify with the previous employer the stated salary and job duties. This is critical in maintaining a safe and effective work force, as a candidate who misrepresents their past experience may lack the proper training and expertise to conduct their job functions.

In some cases, such as manufacturing or construction jobs (for example) this can be dangerous. Fabrications also show dishonesty and increase risk of fraud and other behaviour that puts an employer at risk.

HOW ARE EDUCATION AND PROFESSIONAL CREDENTIALS VERIFIED?

Job candidates may claim to have received a degree they actually did not earn. Or, they may claim a different degree (that is required for a position) than they actually earned. Expert background screeners will verify all educational degrees from the university or college directly. This also includes confirming that the institution is legitimate and not a "diploma mill."

Background screening also includes checking professional licenses and credentials. Investigators will verify these with the issuing body to confirm that the license or credential is held by the candidate and is current/in good standing.

HOW DOES THE GENERAL PROTECTION DATA REGULATION (GDPR) AFFECT BACKGROUND SCREENING?

The GDPR is a set of privacy rules issued by the European Union. The provisions change the way organisations can process background checks, most notably in screening for criminal records. Companies must be aware of the new rules and follow expert advice to stay within its guidelines.

Among the guidelines that must be followed, an organisation must have a written document defining how it will handle criminal records, how it retains those records, and how (and when) they are deleted. To dismiss these guidelines or follow them incorrectly can mean running afoul of the law.

WHAT OTHER LAWS CAN AFFECT BACKGROUND SCREENING?

Every country and jurisdiction has its own laws governing privacy and record-collecting. It is important to work with experts that are familiar with the laws and regulations in the region(s) where you are screening candidates. For example, in the Middle East, background screening industry professionals must adhere to strict local data protection requirements, such as DIFC Data Protection, ADGM Data Protection and QFC Data Protection regulations, to process consensually based personal information.

Dubai International Financial Centre (DIFC) Data Protection standards allow for the processing of sensitive personal information, such as criminal history, with signed consent from the data subject for employee due diligence requirements. As a DIFC-licensed entity, CRI Group (as well as other reputable background screening firms) must maintain

MIDDLE EAST BACKGROUND SCREENING: COMPLIANCE WITH PRIVACY LAWS

In every region and jurisdiction in the world, there are different regulations that govern what background screeners can and can't do in regards to providing pre- and post-employment screening services. The laws in the United States, for example, are not the same as those that affect investigations in the Middle East. The concern over individual privacy and data protection are hot discussion items globally. Companies that engage background screening firms for the Middle East need to make sure those investigators are following all rules and regulations in regards to privacy – or else they might face liability along with the screening provider.

READ MORE

strict adherence to the region's Data Protection Law in order to fulfil our ongoing DIFC licensed status.

HOW OFTEN SHOULD I SCREEN EMPLOYEES?

Employees should be screened at regular intervals to reveal any new information relevant to the business. That's why CRI Group's background investigations services also include:

- Employee monitoring & risk management
- Data protection compliance
- Employee testing & confidentiality
- Employee risk management
- Post-employment background checks

WHY SHOULD I CONTRACT A THIRD-PARTY VENDOR IF I HAVE AN IN-HOUSE TEAM?

You may have the capabilities to carry the above services; however, to perform a full in-depth background screening service for candidates and employees at all levels, you need a considerable amount of manpower and skills – and it can be an all-consuming task.

A third-party vendor such as CRI® with a global network, that works with companies across the Americas, Europe, Africa, and Asia-Pacific, is a one-stop international risk management, background screening and due diligence solutions provider that brings true value to you and your team. By contracting you can benefit from the following:

1. Cost control & savings
2. Time savings / response time
3. Customer service / quality control
4. Expertise & core competency
5. Technology & know-how

WHAT OTHER CHECKS CAN A THIRD-PARTY VENDOR EXECUTE BETTER THAN MY IN-HOUSE TEAM?

From senior executives to shop-floor employees, a full in-depth background check should include:

- Address verification (physical verification)
- Identity verification
- Previous employment verification
- Education & credential verification
- Local language media check
- Credit verification & financial history (where publicly available)
- Compliance & regulatory check
- Civil litigation record check
- Bankruptcy record check
- International criminal record check
- Integrity due diligence … and more.

WHAT IS THE BEST WAY TO EVALUATE PROFESSIONAL BACKGROUND SCREENING FIRMS?

Reputable firms will have typically have a long track record as leaders in providing background screening services. They will also have a global footprint that demonstrates expertise in the various laws and regulations in different areas of the world. CRI® has been offering comprehensive EmploySmart services for over 30 years across more than 80 countries, with a network of more than 175 local network of operatives, researchers and analysts.

EDUCATION & EMPLOYMENT VERIFICATION TRENDS IN THE APAC REGION

The biggest investment today that a business can make is in their new employees, as with each new hiring, they invest time, training, and resources. Background screening is important because it protects the company's reputation, brand, and biggest asset – its people. The trend of background screening is rising over the last few years in the APAC region, with an increased number of check types and a subsequent increase in discrepancy rates.

READ MORE

WHAT IS EmploySmart™?

CRI Goup's EmploySmart™ pre-employment background screening is a process that analyzes a job candidate's claims and credentials, and digs beyond the surface to make sure the facts match up.

An EmploySmart™ background check will investigate a candidate's background based on criteria determined by their prospective or current employer. A check of a candidate's background may include identity, employment, academic and professional, credit history, civil litigation, criminal and police verifications, media search and compliance database, regulatory register and white-collar crime check.

WHY CR®?

CRI® is a leading worldwide provider of specialised international employment background screening, including pre-employment screening and post-employment background checks.

The advantages of using our team of EmploySmart™ background screening experts include the following:

- Fast turnaround times
- Global coverage
- Expertise in compliance
- Data integrity
- Expert investigators
- Strict data protection laws
- Conducting investigations since 1990

WHAT TRAINING STANDARDS AND CREDENTIALS DOES CRI GROUP HAVE?

CRI® implemented ISO 27001:2005 (Information Security Management System), the only company in Middle East and Asian region with BS 102000:2013 Code of practice for the provision of investigative services; BS 7858:2012 Security screening of individuals employed in a security environment.

HOW LONG DOES IT TAKE TO CONDUCT A BACKGROUND CHECK?

Background checks typically take 2-3 days to process and to receive back from the outside contracted agency. A few exceptions may take up to 2 weeks. Rarely, a background check may take longer, 3 to 4 weeks. Please allow additional processing time for each background check in the event of a delay.

A delay can occur for either of the following reasons:

- The information has been entered incorrectly by the applicant or the requestor into the vendor's system.
- The county or district listed for a background check in researching whether the applicant has any criminal felony or misdemeanor charges is delayed in providing a response to the vendor.

HOW MUCH DOES IT COST TO CONDUCT A BACKGROUND CHECK?

That will depend on the scope. Please contact us for a free consultation.

→ **Have more questions? Download our eBook, "FAQ: Employee background screening."**

Get answers to frequently asked questions about background checks / screening cost, guidelines, check references etc. This eBook of compiled list of background screening related questions taken as a whole, is the perfect primer for any HR professional, business leader and companies looking to avoid employee background screening risks. It provides the tools and knowledge needed to make the right decisions.

DOWNLOAD NOW!

WHY BACKGROUND SCREENING? BECAUSE THE NUMBERS DON'T LIE

Want to know what types of red flags are most often found on résumés and employment applications? Based on recent pre- and post-employment screening engagement, CRI Group's EmploySmart™ experts provide insights into where companies are most vulnerable in the hiring process. **Out of all background screening cases conducted by CRI Group between January-June this year (2020), our operations team found that total number of detected discrepancies was as high as 17.6%.** The following were found in recent background screening checks:

2%
Claiming a fake degree

2.33%
Incorrect education degree details

1.27%
Civil litigation records

1.5%
Criminal records

0.85%
Fake certificates

1.27%
Fake address

2.33%
Adverse media

0.85%
Bankruptcy records

4.5%
Incorrect employment details

0.85%
Negative references

When someone intentionally provides false information their résumé, they are committing résumé fraud – usually in the hopes of gaining a competitive edge in the hiring process. "There are even business services out there that will knowingly assist candidates with changing their résumé in this way, such as offering advice on how to hide employment gaps or how to add false information that looks realistic. Some will even provide fake transcripts and fake letters of recommendation" (HR Daily Advisor, 2018).

→ **Want to dive deeper into the numbers? Read "Background Screening Red Flags: Numbers Don't Lie" to learn more.**

BACKGROUND SCREENING RED FLAGS: NUMBERS DON'T LIE

Want to know what types of red flags are most often found on résumés and employment applications? CRI Group's EmploySmart™ experts provided some statistics on their latest pre- and post-employment screening engagements, and they give insights into where companies are most vulnerable in the hiring process.

READ MORE

CASE STUDIES: FAKES & FORGERIES FROM APPLICANTS

Employee background screening is a critical tool for companies to ensure they are choosing the best personnel for their organisation. And if you think verifying an employee's or candidate's education credentials is just a formality, wait until you hear about these cases.

INVESTIGATION FOUND 5 OUT OF 18 DEGREES TO BE FAKE

CRI Group's investigators recently conducted background screenings of employees who were working for a multinational organisation operating in Pakistan. While verifying education credentials as part just one of the aspects of a thorough screening process, the investigators immediately noticed red flags and initiated detailed checks of the education degrees claimed by the subjects.

In this case, CRI Group screened 18 degrees claimed from a single university. By contacting the university and conducting an examination of documents and records, CRI Group found an astounding 5 of them (27.7%) to be fake and/or forged.

There is likely a similarly large percentage of employees that are performing duties in various organisations without carrying relevant degree or certifications. There is a possibility that many of the employees are performing their tasks in companies without holding relevant past professional experience, and some may have been involved in suspicious activities in their past which could result in huge monetary loss for the companies where they are currently employed.

FAKE REFERENCES

An applicant claimed to be a holder of a university degree. When CRI Group conducted its local education verification process, the university named by the candidate reported that the applicant's degree was 'fake and forged.' The applicant also provided a reference letter, apparently signed by the university's Deputy Controller of Examination (Dy COE) — confirming his education record and asking to re-check his record with the university.

However, further investigations showed that the reference letter was also fake, and the signatory was not, nor had ever been, the Dy COE of the university. Another fake and forged degree was revealed when CRI Group investigated the applicant's BBA — as there was no conferment of said degree.

A CRIMINAL AMONG THEM

In another pre-employment verification of an applicant, CRI Group uncovered disturbing details. When the applicant's previous employers were contacted, one of them reported that the applicant was hired without any prior experience, was trained for a couple of months, and then terminated due to committing cash embezzlement as well as participating in harassment and workplace violence. A second employment verification revealed his termination, as he caused a financial loss to the company.

In the end, some job candidates will seek an advantage through fraudulent means. More troubling is the fact that in certain cases, the hidden truth might even include criminal behavior. It is important for any organisation to verify information provided by individuals they seek to hire.

→ **Don't let this happen at your organisation. Get a quote for background screening today!**

WHY CRI® GROUP?

Since 1990, Corporate Research and Investigations Limited “CRI Group” has safeguarded businesses from fraud and corruption, providing insurance fraud investigations, employee background screening, investigative due diligence, third-party risk management, compliance and other professional investigative research services. CRI ® Group’s expertise will add to the diverse pool of business support services available within your region

INVESTIGATIVE RESEARCH

ANTI-CORRUPTION & REGULATORY INVESTIGATIONS
ASSET SEARCH & RECOVERY
FRAUD RISK & INSURANCE INVESTIGATIONS
IP INFRINGEMENT INVESTIGATIONS
INTERNAL INVESTIGATIONS & CONFLICT OF INTEREST
FINANCIAL INVESTIGATIONS & FORENSIC ACCOUNTING

BUSINESS INTELLIGENCE

MARKET RESEARCH & ANALYSIS
COMMERCIAL INVESTIGATIONS

COMPLIANCE SOLUTIONS

INVESTIGATIVE DUE DILIGENCE
CORPORATE SECURITY & RESILIENCE
THIRD-PARTY RISK ASSESSMENT
ANTI-MONEY LAUNDERING
INTEGRITY DUE DILIGENCE

DueDiligence360™
Partners to TRUST

BACKGROUND INVESTIGATIONS

VENDOR & 3RD PARTY SCREENING
PERSONNEL VETTING & PRE- EMPLOYMENT SCREENING
EMPLOYEE INTEGRITY DUE DILIGENCE

EMPLOYSMART™
Smarter Background Checks Today for a Better Workforce Tomorrow

CERTIFICATION & TRAINING

ISO 37001 ANTI-BRIBERY & ANTI-CORRUPTION MANAGEMENT SYSTEMS
ISO 37301 COMPLIANCE MANAGEMENT SYSTEMS
ISO 31000 RISK MANAGEMENT SYSTEMS
ISO 37002 WHISTLEBLOWING MANAGEMENT SYSTEMS
ISO 37000 GUIDANCE FOR THE GOVERNANCE OF ORGANISATIONS
ANTI-MONEY LAUNDERING

ABAC ANTI-BRIBERY ANTI-CORRUPTION CENTER OF EXCELLENCE

WHY WORK WITH US?

- CRI Group has one of the largest, most experienced and best-trained integrity due diligence teams in the world.
- We have a flat structure which means that you will have direct access to senior members of staff throughout the due diligence process.
- Our multi-lingual teams have conducted assignments on thousands of subjects in over 80 countries, and we’re committed to maintaining and constantly evolving our global network.
- Our Risk Management solutions are easily customisable, flexible and we will tailor our scope to address your concerns and risk areas; saving you time and money.
- Our team of more than 50 full-time analysts is spread across Europe, Middle East, Asia, North and South America and is fully equiped with the local knowledge to serve your needs globally.
- Our extensive solutions include due diligence, employee pre & post background screening, business intelligence and compliance, facilitating any decision-making across your business no matter what area or department.

Zafar I. Anjum, Group Chief Executive Officer
e: zanjum@CRIgroup.com | **t:** +971 50 9038184
Zafar, Group CEO of Corporate Research and Investigations Limited (CRI Group), has been building a 30 years’ career in the areas of anti-corruption, fraud prevention, protective integrity, security, and compliance. Possessing both industry expertise and an extensive educational background (MS, MSc, CFE, CII, CIS, MICA, Int. Dip. (Fin. Crime), CII, MIPI, MABI), Zafar Anjum is often the first certified global investigator on the scene when multi-national EMEA corporations seek to close compliance or security gaps.

Global Leader in Risk Management,
Background Screening & Due Diligence Solutions

37th Floor, 1 Canada Square,
Canary Wharf,
London, E14 5AA,
United Kingdom
t: +44 203 927 5250
e: london@CRIgroup.com

LET'S TALK

If you'd like to discuss your business needs, we'd love to hear from you.

EMEA HEAD OFFICE
United Kingdom
Corporate Research & Investigations Ltd.
37th Floor, 1 Canada Square,
Canary Wharf, London, E14 5AA,
United Kingdom
t: +44 203 927 5250
e: london@crigroup.com

MIDDLE EAST
UAE — Dubai
Corporate Research & Investigations Ltd.
917, Liberty House, DIFC P.O. Box 111794,
Dubai, U.A.E.
t: +971 4 3589884 | +971 4 3588577
toll free: +971 800 274552
e: cridxb@crigroup.com

UAE — Abu Dhabi
Corporate Research & Investigations Ltd.
Office No: 3509, 35th Floor Al Maqam Tower, ADGM Square, Al Maryah Island, Abu Dhabi, U.A.E
t: +971 2 4187568
e: criadgm@crigroup.com

Qatar
Corporate Research & Investigations LLC — QFC Branch
Office No. 130, 1st Floor, Al – Jaidah Square,
63 Airport Road, PO Box: 24369, Doha, Qatar
t: +974 4426 7339 | +974 7406 6572
e: doha@crigroup.com

NORTH AMERICA
U.S.A.
Corporate Research & Investigations LLC
445 Park Avenue, 9th Floor New York,
NY 10022, United States of America
t: +1 212 745 1148
e: newyork@crigroup.com

Canada
Corporate Research & Investigations Ltd.
540, 439 University Avenue,
5th floor Toronto ON, M5g 1Y8, Canada
t: +1 437 836 3223
e: toronto@crigroup.com

SOUTH AMERICA
Brazil
Corporate Research & Investigations LLC
Paulista Building 2064/2086 Paulista Avenue,
14th floor, São Paulo 01310-928 Brazil
t: +55 11 2844 4290
e: brazil@crigroup.com

ASIA
Malaysia
Corporate Research & Investigations LLC
Lot 2-2, Level 2, Tower B, The Troika,
19 Persiaran KLCCM, 50450 Kuala Lumpur, Malaysia
t: +60 32178 6133
e: malaysia@crigroup.com

Singapore
Corporate Research & Investigations (Pte.) Ltd.
1 Raffles Place, #19-07, Tower 2, One Raffles Place,
Singapore 048616
t: +65 9723 5104
e: singapore@crigroup.com

Pakistan — Islamabad
Corporate Research & Investigations (Pvt.) Ltd.
Level 12, #1210,1211, 55-B, Pakistan Stock Exchange (PSE) Towers, Jinnah Avenue,
Blue Area, Islamabad, Pakistan
toll free: +92 (51) 080 000 274
t: +92 (51) 111 888 400
e: pakistan@crigroup.com

Pakistan — Karachi
Corporate Research & Investigations (Pvt.) Ltd.
BRR Towers 13th Floor, I.I Chundrigar Road,
Karachi 74000 Pakistan
t: +92 (51) 111 888 400
e: pakistan@crigroup.com

Scan & find out more about CRI Group or go to:
crigroup.com/about

info@crigroup.com