


Crises and threats



When it comes to managing threats, taking action is key. Sooner is better than later.

“There cannot be a crisis next week.
My schedule is already full.”

Henry Kissinger

Seven critical threats. A thousand critical details.

No one wants to spend time dealing with crises, which makes it all the more surprising that so many companies fail to prepare for them. That's what this guide is about - getting prepared for critical threats your company might encounter so they're less likely to turn into crises that destroy value.

The major critical threats facing companies investing in China today are familiar to most business executives. They fall into seven broad areas, each of which brings a unique set of risks.

- intellectual property theft
- fraud
- money laundering
- corruption
- disputes
- integrity
- data protection

Staying ahead of critical threats requires a kind of preparedness many companies don't want to spend time on. With so much to manage today, it's easy to put off thinking ahead about things that might become crises tomorrow. Sometimes deferring action can make sense - but often it doesn't.

This guide outlines the major areas of critical threats and initial steps to consider for mitigating them. It also includes checklists you can use when you find yourself confronting a crisis. In our experience, companies concerned about the potential damage of these types of threats will want to take action now.

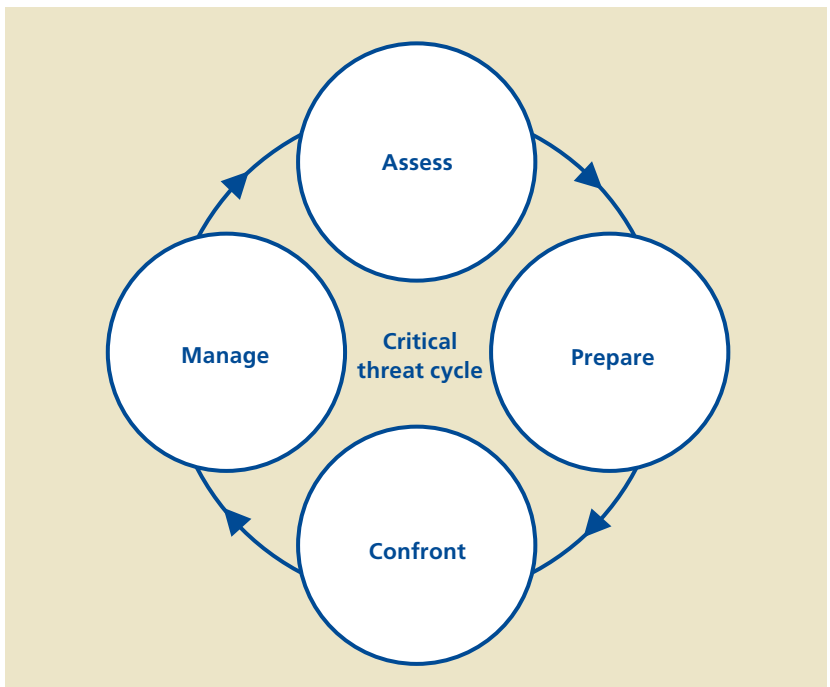
Crises and threats

	Risk	Major areas of exposure	First things
	Intellectual property theft	<ul style="list-style-type: none"> • License to operate • Rights and licenses • Royalties 	<ul style="list-style-type: none"> • Take stock of your intellectual property • Perform value assessment • Conduct risk review
	Corporate fraud	<ul style="list-style-type: none"> • Employee embezzlement • Conflicts of interest • Fraudulent financial reporting • Procurement fraud 	<ul style="list-style-type: none"> • Implement anti-fraud programs and controls • Preservation of evidence • Secure information at risk • Secure assets at risk • Develop ethical culture
	Money laundering	<ul style="list-style-type: none"> • Proceeds of crime • Terrorist financing 	<ul style="list-style-type: none"> • Conduct risk assessment • Implement compliance programs • Conduct integrity due diligence • Carry out training & accountability
	Corruption	<ul style="list-style-type: none"> • Bribes and kickbacks • Economic extortion • Facilitation payments 	<ul style="list-style-type: none"> • Implement anti-corruption programs and controls • Conduct vendor and partner due diligence
	Disputes	<ul style="list-style-type: none"> • Management distraction • Quality of settlement offers • Calculating losses 	<ul style="list-style-type: none"> • Develop a strategy with your legal team • Engage an independent and objective expert • Have resources in place that can move quickly
	Integrity	<ul style="list-style-type: none"> • Professional reputation • Undisclosed business affiliations • Criminal history 	<ul style="list-style-type: none"> • Get to know your potential business partners • Conduct integrity due diligence
	Data protection	<ul style="list-style-type: none"> • Litigation • Technology fraud • Electronic discovery • Intellectual property 	<ul style="list-style-type: none"> • Develop and implement a policy • Understand your data universe • Identify go-to crisis management resources • Prepare and maintain a crisis management plan

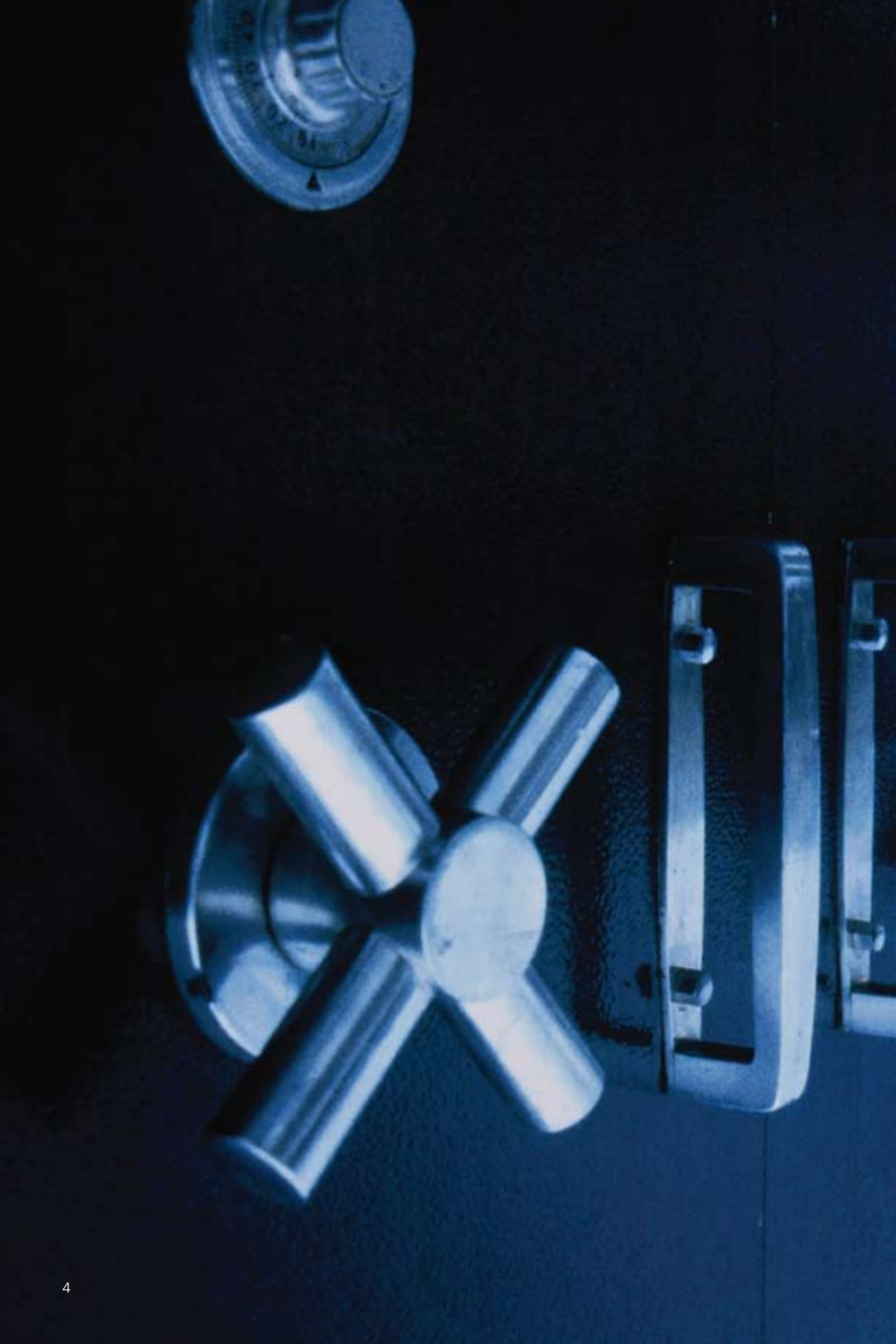
Crises and threats

Business is filled with risks that can destroy value in a heartbeat. We call them critical threats. An accounting error. A missing laptop. An unsubstantiated fraud allegation. Even small things can snowball, and the next thing you know, it's front page news, your share price is tumbling - and your phone is ringing off the hook.

Instead of worrying about critical threats, take steps to mitigate and manage them. Start with a thorough assessment of your exposure in each area and work your way around the critical threat cycle to make sure you're covered.



Managing critical threats requires two things. Getting prepared, and responding when things go wrong. Many of the actions you should take to prepare for threats are the very same actions that make them less likely.



Safeguarding value. Reducing risk.

Intellectual property is like hard currency in many industries. Protecting it is critical, particularly in China where intellectual property abuses are rife. Yet many companies lack a clear understanding of exactly what their intellectual property is - and more to the point, what it's worth.

That inattention creates risks of theft, loss and sacrificed revenue - as well as the potential for costly legal actions. Simply put, when intellectual property is compromised, whether by theft or carelessness, your business can lose value instantly.

Avoiding this risk requires knowing what your intellectual property is, where it is and what it's worth. Only then can you start developing controls to protect it - and keep crises from happening.

Many companies feel their intellectual property is sufficiently managed when their lawyers register patents, trademarks and the like. But the truth is, that's only a small piece of the intellectual property puzzle. A disciplined program of monitoring and controls is necessary to maximize the value and minimize the risks of theft and loss.

Crises and threats

Intellectual property theft

First things

- Take stock of your intellectual property across the enterprise and by business line. Define it, catalogue it and keep your inventory current.
- Assess the value of your intellectual property. Document your valuations completely
- Don't go overboard protecting everything. Some intellectual property is not worth the cost of tight control - while other intellectual property can make or break your company. You have to know which is which

Essential capabilities

Managing the threat of intellectual property loss requires a 360-degree approach by a team with competencies in several specialized areas. Between your in-house resources and your outside advisors, make sure you have each of these capabilities covered:

- Intellectual property licensing
- Strategic alliance structuring
- Counterfeit and grey market tracking
- Due diligence
- Patents, copyrights, trademarks and trade secrets
- Intellectual property valuation
- Royalty and revenue recovery

Intellectual property is like real property - just harder to track

Intellectual property is an intangible product that has commercial value. The value of intellectual property is the amount of money someone would spend to create what he could steal from you instead. In some industries, that value is measured in billions of dollars.

Examples of intellectual property include:

- Customer lists
- Industrial designs
- Permits, mineral rights, licenses
- Environmental studies
- Agreements and contracts
- Patents, know-how, trade secrets
- Trademarks and brands
- Business processes
- Product pricing models

Many companies focus only on the threat of their own intellectual property being stolen. But that cuts both ways. For example, sometimes companies accidentally find themselves in possession of intellectual property that belongs to others - knowledge and trade secrets of competitors that come into your business with new personnel. When you're thinking about risks related to intellectual property, don't overlook your exposure because of this kind of infiltration.



No wiggle room

Sarbanes-Oxley and its global reverberations have made financial statement integrity an iron maiden of corporate accountability. There's not an inch of wiggle room - and errors can be fatal.

But fraud does happen - despite your best intentions - and it must be found. The risks are simply too high. Even the hint of irregularity can wipe out value in an instant. Whether it's the cost of litigation or the cost of losing investor confidence, the threats are real and serious.

Preparedness in the area of financial statements starts with an effective fraud risk assessment - and ends with disciplined controls. It also includes a detailed plan for managing crises in the event they cannot be forestalled. The plan should provide specific guidance for securing evidence and for internal and external communications.

First things

- Assess the 'tone at the top' to make sure your leadership sets the standard for integrity
- Assess fraud risks against current controls. Determine the level of exposure arising from each category of risk
- Evaluate your exposure to major fraud scenarios, including external, internal and collusive fraud
- Pay special attention to the risk of management overriding controls
- Update your crisis communications plan
- Identify go-to resources for support on short notice
- Ensure you have an ethics policy in place
- Set up a whistle-blower scheme

Essential capabilities

Assessing financial statement integrity goes far beyond number crunching. Sometimes it even comes down to detective work - sifting through email archives - or asking the tough questions that no one really wants to answer. Make sure your team is fully prepared to deal with strategic and technical issues in each of these areas:

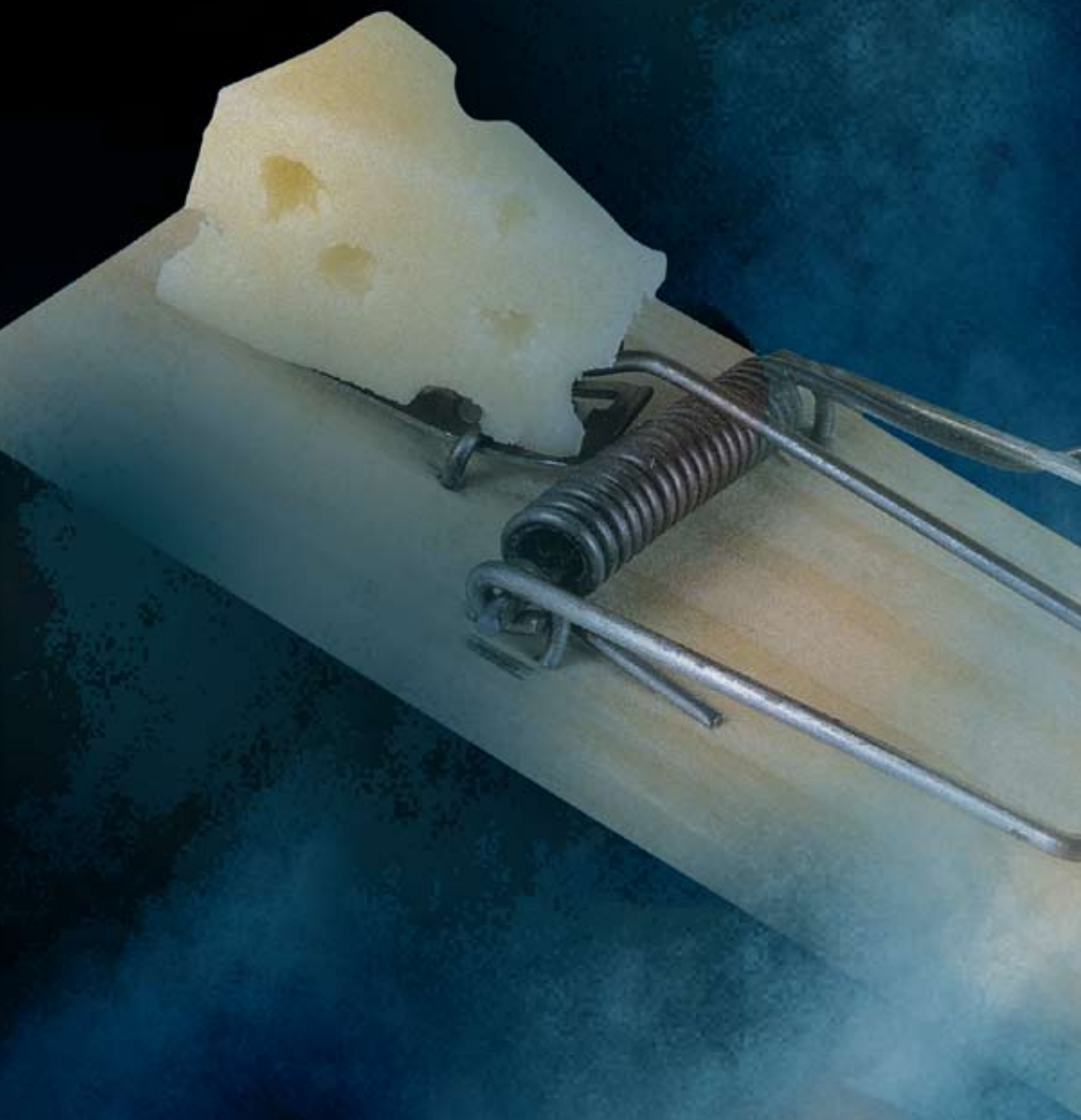
- Diagnostics for assessing fraud risk exposure
- Advanced technology for detecting financial statement anomalies
- Data mining
- Loss quantification
- Fraud awareness training
- Forensic accounting
- Evidence gathering, securing and preserving

Keeping needles out of haystacks

Fraud costs businesses and their stakeholders millions of dollars every year in China, but finding it can sometimes seem like an impossible task. With evidence well-hidden among millions of discrete transactions spread out around the world, it's a lot like finding a needle in a haystack. That's why it makes so much sense to try to deter fraud from happening in the first place..

An anti-fraud program has five elements: a formal fraud risk assessment process, a comprehensive control environment, specified anti-fraud control activities, a fraud-focused information and communication program, and thorough monitoring activities. Each of these elements must be addressed at the highest level of your organization.

Beyond protecting the business from the cost of fraud and addressing regulatory requirements, many organizations regard this as an opportunity to communicate to stakeholders that they are doing everything possible to protect against the risk of fraud. An effective anti-fraud program can preserve your assets and reputation, while demonstrating due diligence to regulators. In the event of a regulatory action, an effective compliance program will also go a long way to reducing potential fines and showing that management did all it could to avoid problems.



It all comes out in the wash

Governments around the world, including in China, are taking an increasingly proactive approach to the prevention of money laundering. Like it or not, that's the world we're operating in - and companies involved in financial services, insurance, real estate, accountancy, brokerage, gaming and precious metals have to take these new requirements seriously. The personal and corporate risks are simply too high to ignore.

No business, cash-intensive or not, is immune from becoming the unwitting accomplice of money launderers. These challenges are compounded for global companies with multiple legal and regulatory requirements, languages, systems and business cultures.

As the international community moves toward tighter regulations and more aggressive enforcement, companies operating in global markets face new responsibilities to identify, report and prevent money laundering activities, no matter where in the world they do business.

First things

- Establish, test and monitor enterprise-wide policies and procedures
- Maintain a strong control culture.
- Designate a Chief Anti-Money Laundering Officer
- Identify who you'll depend on for external counsel in each jurisdiction
- Build in continuous improvement to reflect changing legislation
- Identify resources for conducting electronic transaction look-backs.
- Stress-test your capabilities to detect risk
- Develop a comprehensive incident management plan
- Test your detection framework to make sure it actually works
- Organize extensive training programs to enhance employees' AML awareness and vigilance

Essential capabilities

As money launderers have become increasingly sophisticated, so too must the management of this critical threat. Conducting effective forensic investigations and evaluation of compliance frameworks involving electronic data, in particular, requires advanced technology, deep experience and these specialized capabilities:

- Risk assessments at the enterprise and business unit level
- Protocols for responding to regulatory orders
- Drafting and enhancing policies and procedures
- "Know your customer" program and enhanced due diligence
- Training, compliance assessments, forensic analysis
- Advanced data mining technology
- Chain of custody controls
- Investigations
- Internal investigations
- Credible remedial action plans and implementation support

No room for error

While all the critical threats covered in this book are significant, the threat of money laundering is uniquely troublesome. Perhaps it's the association with illegal drugs or terrorism, perhaps it's the implication of organized crime. Whatever the reason, suspicion of money laundering can destroy personal and corporate reputations faster than almost any other threat. Even the hint of involvement can send your stock price into a tailspin. When a money-laundering crisis begins to emerge, there is no room for error. That means you have to be prepared well in advance. Know exactly who your team will be and how everyone will respond.

Most important of all, recognize the fact that regulations related to money laundering are becoming more and more complex. International businesses need to be aware of laws that can reach over borders and financial systems causing unexpected impacts and publicity.

In today's zero tolerance corporate climate, taking responsibility to safeguard your organization, its employees, directors and shareholders from the fallout of possible criminal and civil fines and penalties is essential.



The world is watching

Foreign companies doing business in China, especially U.S. companies and U.S. listed companies are confronted by the formidable challenge of determining whether cross-border operations and transactions are untainted by corruption.

The stories are legendary - bribery, possession, money laundering and more. In some countries, these practices are business as usual. Which is all the more reason to take this issue seriously.

A new salesperson for a business unit in Shanghai greases the wheels to get a deal done. A production manager in Guangzhou bribes officials to get materials delivered on time. It's an age-old practice with many names - and it's a sure fire way to destroy the value and reputation of any company.

Some argue that the chances of getting caught are slim. That doesn't matter, because the consequences of getting caught are enormous. Your company can be liable for punitive damages, your officers and directors face personal and criminal risk, governments can impose sanctions and your company can be prohibited from getting future contracts.

First things

- Know your agents in China. Understand what you're paying them - and why
- FCPA controls imbedded into the control infrastructure
- Monitor all documentation related to payments and transactions.
- If something seems unusual, don't hesitate to investigate. If something seems too good to be true, it probably is
- Periodic company internal audit of entertainment expenses
- Insist on including right to audit clauses in all contracts
- Train teams so that they are knowledgeable of common vehicles for risk (promotional programs, donations etc)
- Commissions and bonus are in expected and reasonable ranges
- FCPA specific education packages available

Essential capabilities

If your leadership behaves in accordance with ethical, legal and moral guidelines, that will go a long way toward instilling integrity throughout the organization. Beyond that, be sure you have your fingers on the pulse of all potential risks around corrupt practices, especially related to M&A. Don't cut corners on any of these capabilities:

- Risk assessment related to corporate structures
- Analysis of existing contracts and relationships
- Investigations of reputation and integrity of principals
- Corporate culture assessment
- Assessment of internal controls and compliance programs
- Evidence preservation

The long arm of the law

The recent surge in prosecutions by the U.S. Department of Justice and enforcement actions by the Securities and Exchange Commission under the Foreign Corrupt Practice Act of 1977 ("FCPA") has forced companies to carefully examine whether they have effective policies and procedures in place to manage FCPA related risks.

FCPA deals with bribery and accounting. Its bribery provisions apply to U.S. public and private companies, U.S. citizens, and U.S. and foreign companies registered with the SEC. Accounting provisions apply to U.S. and foreign companies registered with the SEC, as well as foreign subsidiaries and affiliates of issuers.

Many countries have attached more and more importance to foreign corruption prevention and enforced counterpart laws and regulations to the FCPA.

High-stakes conflicts

Corporations operating in China face ever increasing threats of litigation and related business disputes. Competitors, customers, shareholders, regulators and even employees pose risks ranging from law suits to contract enforcement and more. When these kinds of disputes flare up, speed, discipline and clear-eyed professionalism become the essential ingredients for effective resolution.

Companies today may encounter disputes in many areas, but five categories of disputes are especially complex: business interruption insurance, buy-sell disputes, joint venture disputes, construction disputes and intellectual property disputes. Each of these brings with it a host of technical issues that require involvement by specialized counsel and experts.

But the challenges go beyond complexity: disputes can become emotional roller coasters, too. This combination of complexity and passion can lead to high drama that may cloud decision making and effective action. That's one reason companies engage balanced teams of advisors for dispute management. Legal experts. Damage quantification experts. Forensic investigators. Expert witnesses. Economists. Whoever and whatever it takes to make the case - that's what your team should bring to the table. By engaging a diverse group of professionals, you can be more confident that every angle is being covered and minimize the hazards of "group think".

Major areas of high-stakes conflicts	
Critical threats and opportunities	
Business interruption insurance	<ul style="list-style-type: none"> • Design risk management for new facilities • Loss accounting • Establishing the “as was” replacement cost • Negotiating with insurers
Buy-sell disputes	<ul style="list-style-type: none"> • Early issues identification • Arbitrator selection • Documentation of positions
Intellectual property disputes	<ul style="list-style-type: none"> • Discovery • Deposition preparation • Settlement strategies • Trial preparation
Construction disputes	<ul style="list-style-type: none"> • Ensure maximum recoverable damages • Accelerating claims and payments • Mitigating risk • Identifying fraudulent activity
Joint venture disputes	<ul style="list-style-type: none"> • Design protective measures for joint venture agreements • Retain control of intelligent property and know-how • Expert determination of buy-out values • Process to maintain documentary evidence of malpractice and oppression

First things

- Establish a methodology for tracking early indicators of potential disputes
- Build a team of advisors who can hit the ground running on short notice
- Create a dispute resolution plan that includes evidence preservation and documentation
- Line up experts early

Essential capabilities

Expert management of disputes requires experience in areas as diverse as tax, information technology, insolvency, corporate finance, mergers and acquisitions, compensation, accounting and auditing, computer forensics and corporate governance. Other specialized capabilities include:

- Arbitration
- Expert testimony
- Assessing risk and damage exposure
- Business and asset valuations
- Forensic investigations
- Business insurance analysis
- Royalty recovery
- Construction disputes
- Securities litigation support

You need the truth

In the pressure-cooker environment surrounding high-stakes disputes, it's easy to start believing your own press. But if you get too caught up in winning, you may find yourself pushing for all-or-nothing solutions that can increase risks. Especially when people driving the process are entrenched with personal agendas that might conflict with the corporate goals.

Sometimes disputes are not about winning or losing at all. Sometimes they're about settling to minimize risk and damage. And sometimes they're simply about avoiding protracted litigation that can distract your leadership team from staying focused on the business. To balance all these potential conflicts, the first thing you'll need is a clear view of the truth.

Getting that view requires the right investigative and analytical tools in the hands of experienced advisors who won't sugarcoat the facts. So when you finally come face to face with the big questions, you'll have complete confidence in the answers.



Mitigate the risks of the unknown

Entering into any new business relationship carries a significant degree of risk of the unknown. But this is particularly so in emerging economies such as China where inadequate corporate governance, corruption, weak enforcement of intellectual property rights and immature dispute resolution mechanisms are common place.

The existence of such issues necessitates conducting due diligence on a potential business partner before committing to an acquisition, transaction or relationship. However, this process should not merely comprise an evaluation of legal and financial positions but should also involve looking at 'off-balance sheet' risks related to integrity and reputation. These could include the source of the target company's seed capital, its track record in similar ventures to that planned, the nature of any political connections that its principals might have, their reputation within the industry, and an understanding of any civil or criminal proceedings that they may have been involved in.

Finding out after the event that your new business partner has a criminal conviction or a reputation for paying bribes to government officials is often too late. That is why integrity due diligence is a key part of the risk mitigation process and can help you avoid costly mistakes, regulatory sanction and damage to reputation.

First things

- Identify business background, affiliations, professional reputation of key principals
- Ascertain existence of significant political connections
- Explore past litigation and regulatory history of company and key principals
- Identify any convictions for or allegations of the key principal's involvement in illegal or unethical activities
- Provide overview of company's history and origins of its seed capital
- Gain insight into management competence and industry reputation

Essential capabilities

Know who you are dealing with up front. The information that you uncover may not necessarily be a deal killer but if it is you'll be glad you found out about it before completing the transaction.

- Pre-transactional integrity due diligence
- Vendor/supplier due diligence
- CEO/senior management background checks

Making the complex understandable

The complexity and volume of business-related data in today's corporate climate means businesses are under ever increasing pressure to understand the data captured during day-to-day business activities. This data is useless until it is analyzed and transformed into business information. In some instances there are standard tools for analyzing transactional business data. However quite often the analysis involves accessing many different data sources to make informed decisions about business strategies and solve complex problems. Analytic & Forensic Technology helps businesses by using technology to bring new levels of clarity, integrity and insight to cut through the fog.

Analytic & Forensic Technology is based upon the premise that in order to make decisions you must understand your field of play and have a clear vision of your options. The techniques used by our team are founded on forensic methodology and the understanding that data, is volatile and needs to be analyzed using appropriate tools and people.

Discovery and litigation support inevitably involve managing large amounts of electronic information, such as email, electronic files and financial data. Traditional filtering techniques such as "de-duplication" are becoming less effective as data sizes increase. By using advanced search and review methodology combined with scalable technology platforms we are able to find, produce and validate the relevant data you are looking to suit your schedule.

Crises and threats

Data protection

Data, often on a huge scale, is the life blood of most businesses, and without it you cannot function effectively. However, in order to fully understand this data companies need to work across multiple sources such as spreadsheets, proprietary databases, ERPs, marketing, HR and customer information. Data analytics can streamline your view of this data and provide meaning and clarity to your company information to help solve complex business issues.

Discovery and data analytics also play an integral role in fraud investigations, helping to capture, analyze and report relevant findings for later production in court. It is through complex analysis of computer systems and provision of technical reports that evidence can be provided to make sense of an otherwise incomprehensible issue. Computer forensics analysis is a methodology that underpins all IT investigations work. It provides a framework to work within and can produce the 'smoking gun' document that will make or break your case.

First things

- Have an information policy in place, and provide training relating to this policy
- Understand your data universe. i.e. know where the information resides in your organization
- Identify go-to crisis management resources
- Prepare and maintain an IT incident response plan and ensure this fits with your business continuity plan

Essential capabilities

Specialized knowledge and skill sets are needed when it comes to Analytic Forensic Technology issues. Deep expertise and professional knowledge combined with relevant experience are essential in the analysis of critical information. This is a highly specialized area that goes way beyond general IT departments.

- Forensically sound methodology and specialized equipment for data acquisition that results in court-admissible evidences
- Ability to recover data from a wide variety of computer equipment to meet international standards
- Ability to analyze large volumes of electronic information in a timely manner
- Identify relevant information that is crucial to a case
- Producing comprehensive reports from complex transactions and large data sets that provide a clear and full picture

Ready or not

Every business faces critical threats - and some of them can become crises no matter how well a company prepares. Whether you're working to recover damages in a dispute or preserve your reputation in the face of a government inquiry, sure-footedness and expert knowledge are critical to success.

Fortunately, the same actions that will help your company avoid crises will also help you manage them if things escalate. Those actions require having a clear view of the road ahead, putting an experienced team into place, getting an early start on gathering evidence and documentation, and understanding what you can and cannot do in any particular situation.

When it comes to addressing critical threats, many companies do not have the required expertise in house. That means they must turn to outside advisors who can work together to preserve value and manage threats effectively.

That's where we can help.

Contact details for Deloitte's China Practice

Beijing

Deloitte Touche Tohmatsu CPA Ltd.
Beijing Branch
8/F Deloitte Tower
The Towers, Oriental Plaza
1 East Chang An Avenue
Beijing 100738, PRC
Tel: +86 10 8520 7788
Fax: +86 10 8518 1218

Dalian

Deloitte Touche Tohmatsu CPA Ltd.
Dalian Branch
Room 1503 Senmao Building
147 Zhongshan Road
Dalian 116011, PRC
Tel: +86 411 8371 2888
Fax: +86 411 8360 3297

Guangzhou

Deloitte Touche Tohmatsu CPA Ltd.
Guangzhou Branch
26/F Teemtower
208 Tianhe Road
Guangzhou 510620, PRC
Tel: +86 20 8396 9228
Fax: +86 20 3888 0119 / 0121

Hong Kong SAR

Deloitte Touche Tohmatsu
35/F One Pacific Place
88 Queensway
Hong Kong
Tel: +852 2852 1600
Fax: +852 2541 1911

Macau SAR

Deloitte Touche Tohmatsu
19/F The Macau Square Apartment H-N
43-53A Av. do Infante D. Henrique
Macau
Tel: +853 2871 2998
Fax: +853 2871 3033

Nanjing

Deloitte Touche Tohmatsu CPA Ltd.
Nanjing Branch
Room B, 11/F Golden Eagle Plaza
89 Hanzhong Road
Nanjing 210029, PRC
Tel: +86 25 5790 8880
Fax: +86 25 8691 8776

Shanghai

Deloitte Touche Tohmatsu CPA Ltd.
30/F Bund Center
222 Yan An Road East
Shanghai 200002, PRC
Tel: +86 21 6141 8888
Fax: +86 21 6335 0003

Shenzhen

Deloitte Touche Tohmatsu CPA Ltd.
Shenzhen Branch
13/F China Resources Building
5001 Shennan Road East
Shenzhen 518010, PRC
Tel: +86 755 8246 3255
Fax: +86 755 8246 3186

Suzhou

Deloitte Business Advisory Services
(Shanghai) Limited
Suzhou Branch
Suite 908, Century Financial Tower
1 Suhua Road, Industrial Park
Suzhou 215021, PRC
Tel: +86 512 6289 1238
Fax: +86 512 6762 3338

Tianjin

Deloitte Touche Tohmatsu CPA Ltd.
Tianjin Branch
30/F The Exchange North Tower
189 Nanjing Road
Heping District
Tianjin 300051, PRC
Tel: +86 22 2320 6688
Fax: +86 22 2320 6699

Deloitte provides audit, tax, consulting, and financial advisory services to public and private clients spanning multiple industries. With a globally connected network of member firms in 140 countries, Deloitte brings world-class capabilities and deep local expertise to help clients succeed wherever they operate. Deloitte's 165,000 professionals are committed to becoming the standard of excellence.

Deloitte's professionals are unified by a collaborative culture that fosters integrity, outstanding value to markets and clients, commitment to each other, and strength from cultural diversity. They enjoy an environment of continuous learning, challenging experiences, and enriching career opportunities. Deloitte's professionals are dedicated to strengthening corporate responsibility, building public trust, and making a positive impact in their communities.

Deloitte refers to one or more of Deloitte Touche Tohmatsu, a Swiss Verein, and its network of member firms, each of which is a legally separate and independent entity. Please see www.deloitte.com/cn/en/about for a detailed description of the legal structure of Deloitte Touche Tohmatsu and its member firms.

Deloitte's China practice provides services through a number of legal entities and those entities are members of Deloitte Touche Tohmatsu (Swiss Verein).

We are one of the leading professional services providers in the Chinese Mainland, Hong Kong SAR and Macau SAR. We have over 8,000 people in ten offices including Beijing, Dalian, Guangzhou, Hong Kong, Macau, Nanjing, Shanghai, Shenzhen, Suzhou and Tianjin.

As early as 1917, we opened an office in Shanghai. Backed by our global network, we deliver a full range of audit, tax, consulting and financial advisory services to national, multinational and growth enterprise clients in China.

We have considerable experience in China and have been a significant contributor to the development of China's accounting standards, taxation system and local professional accountants. We also provide services to around one-third of all companies listed on the Stock Exchange of Hong Kong.

These materials and the information contained herein are provided by Deloitte Touche Tohmatsu and are intended to provide general information on a particular subject or subjects and are not an exhaustive treatment of such subject(s).

Accordingly, the information in these materials is not intended to constitute accounting, tax, legal, investment, consulting, or other professional advice or services. The information is not intended to be relied upon as the sole basis for any decision which may affect you or your business. Before making any decision or taking any action that might affect your personal finances or business, you should consult a qualified professional adviser.

These materials and the information contained therein are provided as is, and Deloitte Touche Tohmatsu makes no express or implied representations or warranties regarding these materials or the information contained therein. Without limiting the foregoing, Deloitte Touche Tohmatsu does not warrant that the materials or information contained therein will be error-free or will meet any particular criteria of performance or quality. Deloitte Touche Tohmatsu expressly disclaims all implied warranties, including, without limitation, warranties of merchantability, title, fitness for a particular purpose, noninfringement, compatibility, security, and accuracy.

Your use of these materials and information contained therein is at your own risk, and you assume full responsibility and risk of loss resulting from the use thereof. Deloitte Touche Tohmatsu will not be liable for any special, indirect, incidental, consequential, or punitive damages or any other damages whatsoever, whether in an action of contract, statute, tort (including, without limitation, negligence), or otherwise, relating to the use of these materials or the information contained therein.

If any of the foregoing is not fully enforceable for any reason, the remainder shall nonetheless continue to apply.