Asia Compliance Risks and Mitigation Strategies

August 15, 2023

GIBSON DUNN

Kelly S. Austin
Partner, Gibson Dunn

Oliver Welch
Partner, Gibson Dunn

Bonnie Tong
Associate, Gibson Dunn

Presenters

Kelly S. Austin
Partner
Hong Kong Office
Tel: +852 2214 3788
Fax: +852 2214 3710
KAustin@gibsondunn.com

Oliver D. Welch
Partner
Hong Kong Office
Tel: +852 2214 3716
Fax: +852 2214 3710
OWelch@gibsondunn.com

Bonnie Tong
Associate
Hong Kong Office
Tel: +852 2214 3762
Fax: +852 2214 3710
BTong@gibsondunn.com

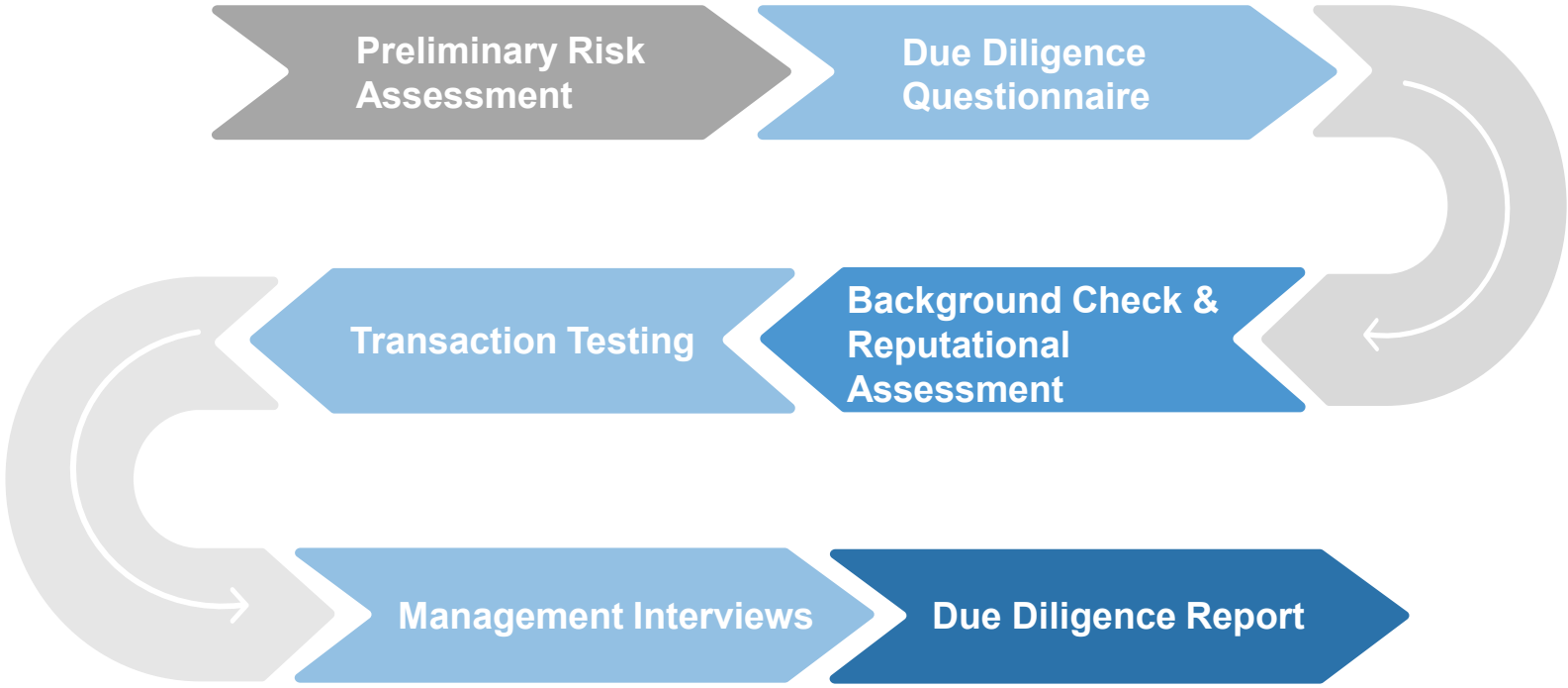
Today's Agenda

01	How to Conduct Compliance Due Diligence: A Risk-Based Approach
02	Compliance Due Diligence: Key Risk Areas
03	Diligence Considerations in M&A Transactions
04	Internal Audit: Key Issues and Case Studies
05	Compliance Expectations and Key Risk Areas
06	Recommended Best Practices

How to Conduct Compliance Due Diligence: A Risk-Based Approach

01

Overview of Compliance Due Diligence Steps



Preliminary Risk Assessment

Nature and size of the relationship

- Role and strategic importance of third party.
- If M&A, majority investment or minority investment, Board representation, ability to nominate key functional leaders.

Geographic risks

- Emerging markets, such as China, India, Turkey, and Southeast Asia, are generally considered to have a higher risk of public corruption.
- Consult the Corruption Perceptions Index published by Transparency International.

Industry risks

- High-risk industries: mining, healthcare, infrastructure, energy, defense, telecommunications.

Other factors

- Government touchpoints.
- Reliance on third parties.
- Adverse media.

Purpose: The preliminary risk assessment is an initial review of available information about the third party and relationship, and is meant to inform the scope and depth of subsequent due diligence activities.

Sources: Target company's website, securities filings, media searches, discussions with the deal team, Investment Committee memorandum.

Due Diligence Questionnaire

A standard due diligence questionnaire should cover the third party's:

go-to-market strategy	compliance policies
key customers	compliance resources
government touchpoints	key regulators/licenses
use of agents	charitable donations
financial controls	historical issues

The Questionnaire should include comprehensive definitions of:

government officials	agents or third parties
government customers	the Target

Practical Tip #1

- Tailor templates to the third party's sector and country and to the findings of the preliminary assessment. The size and resulting interest of the transaction may also impact the amount of information the Target is willing to share.

Practical Tip #2

- Coordinate with teams working on other due diligence streams (e.g., financial due diligence, legal due diligence, and tax due diligence) to avoid duplication and to ensure information sharing.

Practical Tip #3

- Be prepared to ask follow-up questions. Due diligence often requires several rounds of queries following the initial questionnaire.

Practical Tip #4

- After submission of the questionnaire, consider having a discussion with your point-of-contact within the third party to clarify or prioritize any questions.

Background Check and Reputational Assessment

Depending on the risk profile of the proposed third party or transaction, counsel may engage a third-party vendor to conduct a background check and reputational assessment on the target entity, the promoters, the directors, members of the target's key management team, controlling shareholders or founders.

Public record checks

- Typical for all transactions regardless of size or risk
- Searches for adverse media
- Sanctions screening
- Politically Exposed Persons screening
- For lower risk and smaller transactions, we may have capability to handle these checks ourselves.

Discreet source inquiries

- Usually reserved for larger (controlling interest) or higher risk transactions
- Industry sources
- Former employees
- Journalists and analysts that have knowledge of the target

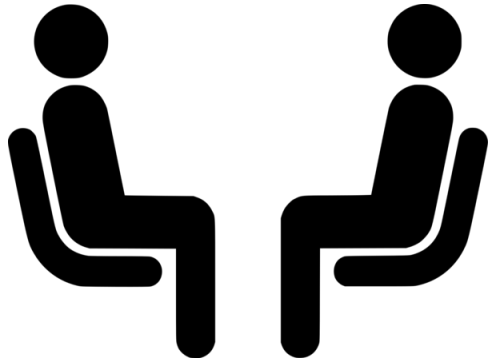
Practical Tip

- Factor in the time needed to commission a background check. Public record checks require at least 1~2 weeks turnaround time; discreet inquiries take at least 3~4 weeks.

Executive and Management Interviews

When

- Whenever practicable, consider conducting interviews with key leaders after receipt of responses to the due diligence questionnaire, background check report and transaction testing results to allow follow-up on specific findings. In some instances it may be appropriate to speak with certain management team members at the outset to assist with the preliminary risk assessment.



Who

- CEO, CFO, General Counsel, Chief Compliance Officer, Head of Sales, Government Affairs, Operations, Promoters, Directors.

Topics

- Follow-up questions or concerns resulting from the due diligence steps, third party's compliance culture, effectiveness of the compliance program.

Approach

- Never shy away from asking tough questions, but remember you will likely work with these individuals post-close. Management will likely be speaking with others conducting due diligence, so ensure your questions are focused.

Due Diligence Documentation

Introduction and Background

- Provide detail on the target, including services and goods provided, key markets, go-to-market strategy, and key customers. If M&A, describe the proposed transaction, including monetary investment, resulting ownership stake, board seats, rights to designate or veto management appointments.

Methodology

- Provide an *exhaustive* list of all due diligence and mitigation steps.

Factual Findings

- Summarize key findings of the due diligence questionnaire, background checks, transaction testing, management interviews and other due diligence steps.

Country and Sector Risk Profile

- Briefly summarize risks inherent in the jurisdictions and sectors in which the target operates. Check TI/CPI ranking and recent news reports, and FCPA enforcement actions involving companies in the same sector.

Risk Assessment

- Summarize observations and give the proposed relationship a risk designation (high risk, medium risk, moderate risk).

Recommendations

- Provide any proposed remedial actions. Ensure they are practical and in line with expectations and your negotiation position.

Compliance Due Diligence: Key Risk Areas

02

Key Risk Areas

Watch for the following when assessing a third party's risk profile.

Compliance Policies and Training	• Lack of a robust anti-corruption policy; lack of clear guidelines on gifts and T&E expenses; lack of clear guidelines on interactions with government officials. • Lack of regular training or communications on code of conduct or other compliance policies. • Lack of effective implementation of compliance policies.
Government Touchpoints and Interactions	• Government contracts; participation in public tenders. • Nature of business requires extensive interactions with regulators; weak L&P process. • Partnerships or alliances with government and SOEs. • Ongoing matters pending approval from a government authority. • Gifts, travel, entertainment, sponsorships or speaker fees provided to government officials.
Third-Party Relationships	• Use of third parties (e.g., distributors) in go-to-market activities without sufficient transparency. • Use of third parties (e.g., customs agent, liaisoning agent) in government interactions. • Lack of a third-party qualification program. • Lack of regular monitoring of third parties. • Lack of contractual protections in third-party agreements.

Key Risk Areas (cont'd)

Financial Controls	• Insufficient or unrelated supporting documentation for transactions. • Lack of sufficient scrutiny on employee reimbursement and cash advances. • Inaccurate descriptions of company or employee expenses in company records.
Charitable Contributions	• Lack of due diligence on recipients. • Donations that benefit a government official who has oversight over the target's business. • Lack of a proper approval process for donations.
Investigation & Monitoring	• Lack of a reporting mechanism for employees to report potential violations. • Lack of an internal audit function or functioning investigation process. • Lack of a compliance risk assessment program.
Prior or Ongoing Compliance Issues	• Ongoing internal or government investigations. • Historical violations of anti-corruption laws by the target entity or its promoters/management. • No disciplinary actions for employees who violated anti-corruption laws. • Historical enforcement actions for violations of tax, labor, regulatory and environmental laws.
Response to Due Diligence Efforts	• Responses to the questionnaire that contain information inconsistent with other documents that you obtain from the third party. • Refusal by the target entity to provide information as part of the due diligence process. • Refusal by the target to acquiesce to basic anti-corruption compliance representations or covenants in the transaction documents.

Diligence Considerations in M&A Transactions

03

Importance of Pre-Acquisition Compliance Due Diligence

Successor liability poses significant risks.

- Under principles of successor liability, an acquirer can inherit the FCPA/Bribery Act liability of a target.
- U.S. courts recognize theories that can hold an acquiror liable for the past acts of an acquired entity.
- Recent corporate FCPA enforcement actions have involved successor liability issues.

Collateral consequences can undermine the purpose of the transaction.

- Financial penalties can erode anticipated revenue and growth.
- Key personnel may need to be replaced, which may damage the acquiror's business.
- Both the acquiror and acquiree may receive significant negative publicity and reputational harm.
- The existing business model may no longer be viable when the acquiror stops non-compliant practices post acquisition. Remediation of anti-corruption violations by the target company could require termination of lucrative contracts, important customer relationships, or key third parties.

A Cautionary Tale

Pre-Investment Conduct Results In Wipeout of Investment Value.

Parent: eLandia

Year: 2009

Target: LatinNode, a telecom services provider.

Conduct: In August 2007, during a post-closing financial integration review, eLandia discovered evidence that Latin Node had paid approximately $2.25 million in bribes to Honduran and Yemeni government officials between March 2004 and June 2007. eLandia voluntarily reported the payments to the DOJ.

Result: eLandia's entire $26+ million investment in Latin Node was reportedly nearly wiped out due to the inflated acquisition price of a corrupt company and investigation costs. eLandia paid a $2 million fine in connection with DOJ's inquiry and placed Latin Node into bankruptcy.

A "cautionary tale" of what can happen when an acquirer conducts "little, if any, [FCPA] due diligence."

— Former DOJ FCPA Unit Chief (Nov. 17, 2009)

Due Diligence Obligations

Credit for Conducting FCPA Due Diligence.

- DOJ and SEC will give meaningful credit to companies who conduct thorough risk-based compliance due diligence on acquisition targets, and, in appropriate circumstances, may decline to bring enforcement actions against companies that discover misconduct in acquired entities through due diligence.

According to DOJ/SEC Guidance, sufficient due diligence many include:

- Review of the target's sales and financial data, its customer contracts, and third-party and distributor agreements.
- Performing a risk-based analysis of the target's customer base.
- Performing an audit of selected transactions entered into by the target.
- Engaging in discussions with the target's key executives and functional leaders regarding corruption risks, compliance efforts and corruption-related issues that have surfaced in the past.

Transaction Testing

A deep-dive review of the target entity's high-risk accounts, carried out by a forensics firm.

Example: A PRC Pharmaceutical Company

Process:

- **Step 1**: In order to preserve privilege, outside counsel engages a forensics firm to conduct the transaction testing. The forensics firm will be acting under the direction of legal.
- **Step 2**: The forensics firm issues a written document request asking for trial balances, general ledgers, a list of government customers, information relating the target entity's financial controls, and other data.
- **Step 3**: The forensics firm selects sample transactions and requests the target entity to gather supporting documents, such as accounting vouchers, contracts, bank transfer records, employee expense reports, etc.
- **Step 4**: The forensic firm performs an onsite review of the supporting documents and conducts confirmatory discussions as necessary.
- **Step 5**: The forensic firm prepares and issues a draft report to counsel.

M&A Risk Mitigation

Tailored Anti-Corruption Representatives and Warranties

- Tailor anti-corruption provisions based on due diligence findings and risk assessment.
- Be careful with "materiality" language or knowledge qualifiers. There is no materiality standard in the FCPA.

Audit Rights

- Provision obligating the target to comply with a compliance-related audit or investigation initiated by the client.

Conditions Precedents

- Example: "Before the closing date, the Target shall adopt the following compliance policies."

Post-Closing Requirements

- Example: "Within three months following the closing date, the Target shall establish a compliance committee."
- Included in the shareholder's agreement and, often, append a detailed compliance plan.

Compliance Certifications

- Key leaders within the target sign a separate document certifying that they will abide by all applicable laws, including anti-corruption laws.

Internal Audit: Key Issues and Case Studies

04

Internal Audit's Constituencies and Responsibilities

A company's internal audit team plays a number of important roles and has responsibilities to various constituencies within and outside a company.

Multiple constituencies

- Board and Audit Committees
- Business management
- External auditors and regulators

Multiple responsibilities

- Ensure accuracy of the company's financial statements
- Evaluate effectiveness of the company's risk management, internal and financial controls, and governance processes
- Identify key business risks and communicate them to management
- Liaison with external auditors

U.S. and UK Regulatory Guidance Regarding Internal Audit

Regulators in both the U.S. and UK recognize the crucial role played by the internal audit team in ensuring a company's internal controls are regularly evaluated and findings are communicated to key stakeholders.

U.S. Department of Justice

- DOJ's guidance manual for federal prosecutors instructs them to consider "whether internal audit functions [are] conducted at a level sufficient to ensure their independence and accuracy," and whether companies engage in sufficient audits and other activities to ensure their compliance programs are up to date and do not grow "stale."

U.S. Securities and Exchange Commission

- SEC staff attorneys are to consider "the existence of compliance procedures to prevent misconduct" and a company's "ability to detect misconduct and prompt remediation" in assessing whether to pursue an enforcement action.

Joint DOJ/SEC Guidance

- The *FCPA Resource Guide* jointly issued by both agencies provides that a company's internal audit program should scale up commensurate with its risk profile and encourages "targeted audits" of key risk areas to identify potential weaknesses.

UK Ministry of Justice

- MOJ's guidance regarding the procedures companies should put in place to prevent bribery provides that a company with an effective compliance program "monitors and reviews procedures designed to prevent bribery by persons associated with it and makes improvements where necessary."

Recent Enforcement Actions Highlighting Internal Audit Findings

Recent FCPA enforcement actions have highlighted the role of a company's internet audit team and focused on audit warnings of potential issues that were inadequately addressed.

Novartis (2020)

- The SEC highlighted internal audit findings of control deficiencies in clinical trials carried out by Novartis's Greek subsidiary, as well as indications that the trials were promotional rather than scientific in nature.

Cardinal Health (2020)

- The SEC alleged that the compliance department of the company's Chinese subsidiary conducted an audit of expenses paid out of a marketing account and identified evidence of non-compliance with Cardinal China's compliance policies. Additionally, U.S.-based executives received an internal report claiming marketing employees were using these funds to pay government officials in China.

Stryker Corp. (2018)

- The SEC alleged that the company's internal controls were insufficient to detect the risk of improper payments in India, China, and Kuwait. Among other issues, the SEC alleged that an internal forensic review of Stryker's Indian subsidiary identified no supporting documentation for many high-risk transactions, and that Stryker's Chinese subsidiary used sub-distributors that were not vetted, approved, or trained as required by company policy.

Panasonic (2018)

- Internal audit identified payments to a government official as high risk; nevertheless, the company allegedly continued to make payments to the official. Internal audit also identified a number of "critical risk" and "high risk" deficiencies in the use of certain third-party providers; management allegedly failed to address these issues.

Recent Enforcement Actions Citing Internal Audit Failures

In other recent FCPA cases, the government has cited internal audit failures in support of its charges.

Herbalife Nutrition Limited (2020)

- In 2016, after receiving an internal audit report showing excessive hospitality expenses by Herbalife employees in China, a member of Herbalife's Board of Directors wrote to Herbalife's Audit Committee and the Head of Internal Audit questioning these expenses. The Head of Internal Audit allegedly dismissed the board member's concern and opined that those findings were within "tolerance."

Fresenius Medical Care (2019)

- The resolution documents alleged that Fresenius's legal, compliance and internal audit functions failed to detect and prevent bribery in certain countries, particularly in West Africa, despite numerous red flags. However, the documents also noted that internal audit did identify certain issues relating to the company's dealings with foreign officials in Mexico and Spain.

Mobile TeleSystems (2019)

- The resolution documents cited MTS's failure to implement adequate internal accounting controls and to enforce the controls it had in place. Among other deficiencies, MTS was cited for lacking a sufficient internal audit function to ensure corporate assets were not used to bribe foreign officials, and failed to conduct adequate internal audits to detect and prevent criminal activity.

Legal Professional Privilege

Definition: The privilege (or right) of a client not to disclose confidential communications between client and attorney that were made for the purpose of seeking or providing legal assistance or advice.

Purpose

- Ensure open and honest communication between clients and attorneys; and
- Promote public interest in observation of law and administration of justice.

Legal professional privilege protects communications, not facts

- The privilege applies in the United States and, in various forms, in common law jurisdictions such as Australia, New Zealand, India, Hong Kong, Singapore and the UK.

Special Privilege Considerations for Internal Audit

Although a company's internal audit team is often well-positioned to proactively identify potential corruption risks worthy of further investigation, special care should be taken to ensure compliance audits are conducted at the direction of counsel and are protected by privilege.

- Generally speaking, internal audit reports and work papers are not protected by privilege:
  - Attorney-client privilege does not attach if the audit is not directed by counsel.
  - Work product protection does not apply if the audit was conducted in the ordinary course of business rather than "in anticipation of litigation."

- The UK's "legal advice privilege" and "litigation privilege" similarly do not tend to protect internal audit reports and work papers.

- Given the significant weight regulators give to internal audit findings, sensitive audits related to potential regulatory or litigation issues are increasingly being conducted at the direction of counsel.

- Legal should confirm that internal audit is working at the direction of counsel and set out the scope of the review in a formal communication:
  - *Legal and Outside Counsel have been asked to provide legal advice to the company with respect to the level of compliance with the company's policies and applicable laws and regulations. In order to ascertain the facts necessary to provide such advice, we have asked you to assist us by performing certain audit and information gathering tasks. You will be acting under our direction during the course of this review.*

- For audits being conducted at the direction of counsel, internal audit's workstream should function outside of the ordinary course of business. Internal audit should report up exclusively through in-house and/or external legal functions.

Special Privilege Considerations for Internal Audit

Best Practices for Compliance Reviews

- Escalate potential policy, legal or regulatory compliance issues to legal as soon as they surface. Ask for guidance early and often.
- Keep audit issue summaries and reports strictly factual. Avoid conclusions especially when referring the matter to another group, i.e. compliance. Avoid hyperbolic statements (*substantial risk, clear violation, material impact*), legal language (*anti-competitive, bid rigging, FCPA*) and technical terms that may be taken as conclusive findings.
- Do not reach legal or policy conclusions.
- Label documents appropriately. For example, internal audit work papers should be stored separately and labeled "Prepared at the Direction of Counsel." When a document contains information that is confidential, proprietary, or privileged, mark it as such. Documents not in final form should be labeled as drafts.
- Remember to keep the information you acquire as part of a privileged review confidential. Check with legal if you need to share information with someone outside the internal audit and legal teams.
    - Internal audit can work with counsel to develop a non-privileged summary of findings to ensure that lessons learned are broadly disseminated in the company.
- Be careful when drafting corrective and remedial actions. Can the company effectively implement what you are recommending? Who will own the action items?

Key Risk Areas for Companies Doing Business in Asia

05

Overview of Key Risk Areas

Although companies need to be mindful of and prepared to prevent a wide range of anti-corruption risks, they should be especially mindful of the following.

Third-Party Risks

- The use of third-party wholesalers, distributors, marketing professionals, or consultants is a common risk area.
- Companies must be mindful of these risks and employ strong due-diligence processes to qualify and monitor vendors.

State-Owned and –Controlled Customers

- Employees of state-owned enterprises qualify as “foreign officials” under the FCPA and have been a persistent source of liability for companies in the technology sector.
- Companies need to be especially mindful of promotional gifts, sponsorships, and sponsored events offered to government officials, as well as the size and terms of discounts and rebates offered to SOE customers.

Charitable Donations and Grants

- Donations and grants to state-affiliated parties are governed by the FCPA, and companies must take precautions to ensure these types of payments are put to appropriate use.

Emerging Market Risks

- Given its significant operations in high-risk countries, companies must be mindful of both corruption risks and relevant legal requirements in every jurisdiction in which it operates.

Third-Party Risks

Issues involving third parties have been at the core of recent enforcement actions conducted by the SEC, the DOJ, and local enforcement agencies.

- High-risk third parties may include sales agents, consultants, PR/marketing firms, event organizers, distributors, logistics providers, joint venture partners, local counsel, and customs brokers.
- The DOJ and SEC will impose direct liability upon companies based on improper activities of third-party agents where companies have actual knowledge or purposefully avoid actual knowledge of the activities.
- The UK Bribery Act holds companies strictly liable for bribery by their subsidiaries, employees, or third-party agents absent adequate procedures.

Red flags relating to third-party agents include:

- Third-party consultants that are in a different line of business than that for which they are being engaged.
- Excessive payments to third-party agents or consultants.
- Lack of supporting paperwork and other documentation for services performed.
- Third-party consulting agreements that include only vaguely described services.

Government Customers

Among the most significant sources of risk in dealing with government customers are promotional gifts, business hospitality, or sponsored events, and discounts or rebates offered to customers.

Gifts, Hospitality and Sponsored Events

- While gifts or other benefits to government customers may be legitimate, companies also may face significant corruption risk associated with such arrangements.
- U.S. regulators have brought several FCPA enforcement actions including allegations of this nature.
- **"Red flags" to be mindful of in this space include:**
  - Lavish benefits (such as tickets to the World Cup and related hospitality) to government customers who are in a position to influence decisions affecting the company's business; and
  - Conference sponsorship, often with a disproportionate amount of the travel budget dedicated to tourism activities.

Rebate and Discount Programs

- Discounts may be acceptable when provided for certain competitive or other documented business reasons, but discounts may also lead to bribery-related concerns and implicate the FCPA.
- DOJ and the SEC have regularly pursued companies for providing inflated, above-market discounts to third-party distributors that enabled the distributors to make improper payments to government customers.

Charitable Contributions and Government Grants

Particularly given the surge of philanthropic activity during the COVID-19 pandemic, companies should be very mindful of potential compliance risks relating to contributions of money or products to government agencies or charities and non-profits with government affiliations.

- Even charitable contributions or other philanthropic or humanitarian efforts can run afoul of the FCPA if they indirectly benefit foreign officials and appear tied to a company's business interests.
- Charitable contributions are closely scrutinized by government regulators, and have been the basis for FCPA enforcement actions.
  - For example, U.S. pharmaceutical company ***Schering-Plough*** paid $500,000 to resolve allegations arising from improperly-recorded donations to a Polish non-profit focused on castle restoration whose founder and director was a Polish government official involved in healthcare procurement.

Red flags to be mindful of in this space include:

- Recipients affiliated with government officials in a position to influence relevant business decisions.
- Contributions that differ significantly in value or kind from the typical practices of the company (or subsidiary).
- Contributions to entities with activities that are hard to discern or inconsistent with the company's mission.
- Contributions conditioned upon or otherwise related to the purchase of companies' products.

Recommended Best Practices

06

Regular Risk Assessment and Re-evaluation

Internal audit plans must be constantly reviewed and refreshed in order to ensure that the company's program is consistent with regulatory expectations and industry best practices.

Risk factors that companies should consider in designing and updating their internal audit plan include:

- The location of its operations, particularly those located in high-risk jurisdictions.
- The regulatory landscape in which it operates.
- The types of clients and business partners it deals with.
- The nature and extent of its interactions with government entities and officials.
- Recent changes in relevant regulations or regulatory guidance.
- Case studies involving companies in similar industries.
- Recent internal audit and investigation observations.

Managing Third-Party Risks

Use of third parties is an inevitable part of doing business in an emerging market. Pre-engagement screening, as well as close monitoring, can help offset the decreased transparency and control that comes with using agents and intermediaries.

Best practices for controlling and minimizing third-party risks include:

- ***Involve legal and compliance*** in contract negotiations/drafting to ensure that services are specifically and accurately described and allow for an efficient control (e.g., finance) to assess whether the services have actually been rendered and whether prices are reasonable in light of those services and are in line with market rates.
- Include ***audit rights with a trigger in third-party agreements*** to allow for audits when indicated.
- Identify the specific ***functions that are prone to corruption*** and handled by third parties.
- Use a risk-based approach to periodically select third parties for an ***audit review***.
- Conduct ***specific training for employees*** working with third parties and with end-customers.
- Understand ***interaction between sales force in emerging markets, involved third parties (e.g., distributors, agents) and end-customers***, and conduct function-specific compliance training with these employees.
- Understand whether ***margins of intermediaries are passed on to end-customers*** by reviewing publicly available tender materials or conducting audit reviews.
- Ensure that ***rebates, credit notes, and other payments*** provided to the third party are made to the contracting entity, including identifying any offshore arrangements.

Questions?

Our Offices

Abu Dhabi
Al Sarab Tower, Floor 11
ADGM Square, Al Maryah Island
Abu Dhabi, United Arab Emirates
+971 (0) 2 234 2600

Beijing
Unit 1301, Tower 1
China Central Place
No. 81 Jianguo Road
Chaoyang District
Beijing 100025, P.R.C.
+86 10 6502 8500

Brussels
Avenue Louise 480
1050 Brussels
Belgium
+32 (0)2 554 70 00

Century City
2029 Century Park East
Los Angeles, CA 90067-3026
+1 310.552.8500

Dallas
2001 Ross Avenue
Suite 2100
Dallas, TX 75201-6912
+1 214.698.3100

Denver
1801 California Street
Suite 4200
Denver, CO 80202-2642
+1 303.298.5700

Dubai
Building 5, Level 4
Dubai International Finance Centre
P.O. Box 506654
Dubai, United Arab Emirates
+971 (0)4 318 4600

Frankfurt
TaunusTurm
Taunustor 1
60310 Frankfurt
Germany
+49 69 247 411 500

Hong Kong
32/F Gloucester Tower, The Landmark
15 Queen's Road Central
Hong Kong
+852 2214 3700

Houston
811 Main Street, Suite 3000
Houston, Texas 77002-6117
+1 346.718.6600

London
Telephone House
2-4 Temple Avenue
London EC4Y 0HB
England
+44 (0) 20 7071 4000

Los Angeles
333 South Grand Avenue
Los Angeles, CA 90071-3197
+1 213.229.7000

Munich
Hofgarten Palais
Marstallstrasse 11
80539 Munich
Germany
+49 89 189 33-0

New York
200 Park Avenue
New York, NY 10166-0193
+1 212.351.4000

Orange County
3161 Michelson Drive
Irvine, CA 92612-4412
+1 949.451.3800

Palo Alto
1881 Page Mill Road
Palo Alto, CA 94304-1125
+1 650.849.5300

Paris
16, avenue Matignon
75008 Paris
France
+33 (0)1 56 43 13 00

San Francisco
555 Mission Street
San Francisco, CA 94105-0921
+1 415.393.8200

Singapore
One Raffles Quay
Level #37-01, North Tower
Singapore 048583
+65.6507.3600

Washington, D.C.
1050 Connecticut Avenue, N.W.
Washington, D.C. 20036-5306
+1 202.955.8500

Appendix

China: Data Protection Development

China: Data Protection Development

Implementation of Data Protection Laws

- Article 38 of the ***Personal Information Protection Law*** sets out three ways that a personal information processor may transfer personal information outside the PRC: (1) passing an official data security assessment, (2) obtaining a personal information protection certification from an officially designated certification body, or (3) executing a contract incorporating standard contract clauses with the data recipient.
- The ***Measures for Security Assessment of Cross-border Data Transfer*** (effective September 1, 2022) specify when a personal information processor must apply for an official data security assessment (e.g., processing sensitive information of 10,000 or more persons), as well as the procedure and the criteria of the assessment.
- The ***Implementing Regulation on Personal Information Protection Certification*** (November 2022) sets out the standards and procedures for issuing a personal information protection certificate, including the certificate for cross-border data transfer.
- The ***Measures for the Standard Contract for Cross-Border Transfer of Personal Information*** (effective June 1, 2023, with a six-month grace period) allows a company to transfer personal information outside China subject to a set of standard contractual clauses, which require a data processor inside China to inform data subjects about the data recipients outside China, the purpose of the data transfer, and obtain the data subjects' consent to the transfer.
- ***Local governments and courts*** have issued numerous guidance documents and illustrative cases relating to the PIPL.

Guiding Cases for Personal Information Protection Under PRC Criminal Law

- In December 2022, the Supreme People's Court published four guiding cases under PRC Criminal Law Art. 253(1), which penalizes "obtaining, selling or providing personal information." The cases make clear that protected personal information includes facial recognition information, a PRC ID card number, a WeChat identifier, and a mobile phone number.

Establishment of the National Data Bureau

- In March 2023, China's National People's Congress approved the establishment of the National Data Bureau, a national agency to oversee data-related regulatory matters in an effort to overhaul the current regime where multiple agencies share oversight.