Financial institutions
Energy
Infrastructure, mining and commodities
Transport
Technology and innovation
Life sciences and healthcare

NORTON ROSE FULBRIGHT

Asia Pacific insights

Business ethics and anti-corruption

Part of the global regulation and investigations group

Issue 11 / January 2017

In this issue:

From the editor

Many thanks for reading Issue 11 of our *Asia Pacific Insights* into Business ethics and anti-corruption matters in the new year 2017.

As the year 2016 wound down to a close, we look back at what has been widely termed the year of disruption and examine some significant enforcement activities and developments which may signal upcoming changes to the compliance landscape in the new year.

China remains an important jurisdiction to consider when managing anti-corruption risks. A large number of FCPA investigations are focused on activity in China. In the Nu Skin case, my US and China-based colleagues delve into an SEC settlement where a fine was imposed following an investigation which involved the use of "charitable donations" to a charity associated with a Chinese government official. In another China-related article, Barbara Li and Olivia Yang review the new Cyber Security Law that will have important implications for businesses operating in China.

In a multi-jurisdictional comparative analysis, Abigail McGregor, Paul Sumilas, Jeremy Lua and I consider the rising tide against senior management personal liability under various regimes for anti-corruption offences – including the use of "books and records" and anti-money laundering provisions – to ensure that those who turn a blind eye to corrupt activities do not escape the force of the law. The convergence of the US, Australian and Singapore regimes suggests that the rheotoric on senior personal liability is being backed up by action.

Finally, Jason Hungerford and Paul Sumilas review a compliance milestone in the highly anticipated standard for anti-bribery management systems – ISO 37001 – and scrutinize its effectiveness and value to an organization.

As we look forward to 2017, I hope our legal analysis and thought pieces continue to provide you with useful perspective and insight to support you in your work.

Wilson Ang
Partner
Tel +65 6309 5392
wilson.ang@nortonrosefulbright.com

Business ethics and anti-corruption in Asia Pacific

Norton Rose Fulbright advises clients across the globe on all matters relating to business ethics and anti-corruption. Within Asia Pacific, we have acted in major corruption investigations and have a track record of advising on complex, cross-border matters. We are amongst the largest global legal practices in the region. Our team operates across offices in Bangkok, Beijing, Hong Kong, Jakarta, Shanghai, Singapore, Tokyo, Brisbane, Melbourne, Perth and Sydney.
The quarterly review *Business ethics and anti-corruption: Asia Pacific insights* explores the impact of anti-corruption developments in the Asia Pacific region and offers practical insights in response to topical issues.

See also
Business ethics and anti-corruption world
A global bulletin published by Norton Rose Fulbright LLP

Contents

SEC fines Nu Skin to settle FCPA charges

On September 20, 2016, Nu Skin Enterprises, Inc. (Nu Skin) paid US$765,688 to settle allegations by the US Securities and Exchange Commission (SEC) that Nu Skin violated the accounting provisions of the US Foreign Corrupt Practices Act (FCPA) in connection with a charitable donation.[1] Specifically, the conduct relates to payments made by Nu Skin's Chinese subsidiary, Nu Skin (China) Daily Use And Health Products Co. Ltd. (Nu Skin China) to a charity tied to a high ranking official in the Chinese Communist party.[2] Nu Skin China allegedly made the payment in an effort to end an investigation by the Chinese Administration for Industry and Commerce (AIC) into Nu Skin China's marketing and sales practices. The resolution underscores the importance of caution and diligence in making charitable donations in foreign countries.

1 SEC Charges Nu Skin Enterprises, Inc. with FCPA Violations, U.S. Securities and Exchange Comm'n (Sept. 20, 2016), https://www.sec.gov/litigation/admin/2016/34-78884-s.pdf.

2 Nu Skin Enterprises, Inc., Exchange Act Release No. 78884, at *2 (Sept. 20, 2016).

Facts

The AIC had been investigating whether Nu Skin China had been conducting business activities in a particular city without the necessary licenses. In an effort to influence the AIC's investigation, a Nu Skin China employee contacted the Communist party official, who was also the former boss of the head of the AIC branch investigating Nu Skin China, and requested the name of a charity to which Nu Skin China could donate. The official suggested a charity that was created by an entity with which the official was previously associated.

After the discussion with the official, the AIC informed Nu Skin China that there was enough evidence to file charges that would result in a fine of RMB2.8 million (approximately US$431,088). Nu Skin China offered to "donate some money instead of [paying] a fine" to avoid any charges. Senior personnel at Nu Skin China also requested that the official personally intervene in the matter in exchange for a RMB1 million donation to the charity. Soon after the charitable donation was made, the AIC notified Nu Skin China of its decision to neither charge nor fine the company.

The parent corporation identified the donation as a potential FCPA issue before it occurred and recommended that its Chinese subsidiary consult with U.S. counsel. U.S. counsel recommended that the subsidiary include anti-corruption language in the donation agreement. The parent corporation reviewed the draft of the anti-corruption provisions, but they were removed by the subsidiary just prior to execution.

Key takeaways

This settlement highlights a number of key issues for companies subject to the FCPA

- **Charitable donations are back in the crosshairs:** This is the second time that the SEC has brought an enforcement action based entirely on a charitable donation. Companies need to carefully scrutinize charitable donations in foreign countries to maintain compliance with the FCPA. They should always determine why the donation is being made and who outside the company requested it. Donations requested by foreign government officials should not be approved unless the company can prove it has no matters before the foreign government that the official may influence. The conclusions should be documented in advance of the donation.

- **Instilling a compliance culture:** Multinational companies must not only embrace the "tone at the top" message that US regulators identify as a key element of a compliance program, but also ensure that the proper tone permeates further down in the organization. This resolution demonstrates that the U.S. regulators are not excusing U.S. public companies when the parent corporation is asking the right questions. The parent corporation took appropriate action by requiring Nu Skin China to consult with external U.S. counsel regarding the adequacy of the donation documentation. But the subsidiary ignored that advice and removed the anti-corruption terms from the donation agreement, without the knowledge of parent personnel. The regulators are holding U.S. companies responsible for the unauthorized actions of subsidiary employees. U.S. companies must follow up to make sure its anti-corruption instructions were followed.

- **Geographic risk:** China continues to be a hot spot for corruption and a focus for the US regulators – in 2016 alone, the SEC has brought over 10 actions based on misconduct in China. As this case shows, even companies taking appropriate steps, such as engaging external counsel to assist on corruption-related matters, must take special care in the region. In this regulatory environment, companies must consider whether to conduct anti-corruption audits and reviews of their Chinese operations.

For more information contact:

Michael Edney
Partner, Washington, DC
Tel +1 202 662 0410
michael.edney@nortonrosefulbright.com

Sun Hong
Partner, Shanghai
Tel +86 21 6137 7020
hong.sun@nortonrosefulbright.com

Kevin James Harnisch
Partner, Washington, DC
Tel +1 202 662 4520
kevin.harnisch@nortonrosefulbright.com

Paul Sumilas
Senior associate, Singapore
Tel +65 6309 5442
paul.sumilas@nortonrosefulbright.com

Ilana Beth Sinkin
Associate, Washington, DC
Tel +1 202 662 4651
ilana.sinkin@nortonrosefulbright.com

China cyber security: New law increases security regulation over cyberspace

On November 7, 2016, the Standing Committee of China's National People's Congress (NPC) voted to pass the Cyber Security Law. Its draft has gone through three rounds of readings and it will become effective from June 1, 2017. This legislation provides for the Chinese government's supervisory jurisdiction over cyberspace, defines security obligations for network operators and enhances the protection over personal information. It also establishes a regulation regime in respect of critical information infrastructure and imposes data localisation requirements for certain industries.

In this briefing, we outline the key changes it will bring about and discuss the implications for businesses in China.

Key aspects of the Cyber Security Law

Network operators

The Cyber Security Law requires that network operators must comply with stringent cyber security obligations. These include having to comply with

- A graded protection system for network security
- Security protection obligations so as to protect networks from disturbance, damage or unauthorised access and to prevent network data from being divulged.

In particular, network operators are required to adopt technical measures for monitoring and recording network operation status and network security incidents, and to keep network logs for at least six months. In addition, network operators are obliged to provide technical support and assistance to public security authorities and national security authorities for security and crime investigation.

Under the Cyber Security Law, it is compulsory for network operators to verify the identity of users when providing services (such as landline and mobile subscription, Internet access and domain name registration), and not to provide such services until users have sufficiently disclosed their identity. If there is a cyber intrusion or breach, network operators are obliged to delete personal information illegally collected or make corrections to it at the request of the person to whom the personal data relates.

Key network equipment and specialised network security products

Products and services providers shall comply with the compulsory requirements of relevant national standards. It is provided in the Cyber Security Law that "Key Network Equipment" and "Specialised Network Security Products" must be either certified or tested by a licensed security certification institution in order to ensure compliance with relevant national and industry standards. Products or services which fall within the scope of "Key Network Equipment" and "Specialised Network Security Products" are not allowed to be released into the China market unless they have passed the certification or testing process. The government will formulate and promulgate the catalogue of Key Network Equipment and Specialised Network Security Products.

Critical information infrastructure facilities

An important aspect of the Cyber Security Law is that it introduces the concept of Critical Information Infrastructure Facilities. According to the Cyber Security Law, Critical Information Infrastructure Facilities are broadly defined to cover a wide range of sectors including energy, transportation, electricity, water, gas, financial institutions, medical/ healthcare, and social security.

The Cyber Security Law requires that procurement of network products and services for the Critical Information Infrastructure Facilities shall pass a security assessment conducted by China Administration of Network together with other relevant governmental agencies under the State Council if the network products and services involved may affect the national security. The products/services providers are also required to sign a confidentiality agreement to specify the responsibilities for network security and confidentiality undertaking. It is also important to note that personal data and important business data generated or collected in China by the operators of Critical Information Infrastructure Facilities must be stored in China and transfer of such data abroad is allowed if

- There is a business need
- Security assessment is passed according to the rules issued by CAC and other relevant governmental agencies.

Protection of personal data

The Cyber Security Law is the first legislation at the national law level which establishes the legal principles for protection of personal data. In the past, data privacy is regulated by administrative rules, judicial interpretations, government policies and non-binding industry guidelines.

The Cyber Security Law provides that network operators must safeguard the secrecy of personal data collected and the collection and use of personal data must follow the principles of legality, propriety and necessity and data collectors must follow the legal requirements in terms of giving the notice and obtaining the consent. In case of a data breach incident, the data collectors shall report to the authority and affected users should also be contacted. Companies and individuals who are directly in charge can be fined up to RMB100,000 for failure to comply.

Fighting against cyber crime

Compared with the previous drafts, the final version of the Cyber Security Law reinforces the provisions in relation to crackdown against cyber fraud and cyber crime. The Cyber Security Law takes a strong stance against cyber fraud and cyber crime by imposing criminal, administrative and legal penalties against individuals and entities that commit cyber fraud and cyber crime.

Implications for businesses

The issuance of the Cyber Security Law appears to be in line with recent regulatory movements in China, following the promulgation of the National Security Law, the Measures for Administration of Mobile Apps, and the Regulations for Administration of Online Publishing Services. It demonstrates Chinese government's intention to strengthen the regulation of Internet activities and safeguard the security of cyber space.

The Cyber Security Law contains provisions which could have significant implications for companies doing business in China and companies are advised to understand the requirements in the Cyber Security Law to ensure that their business operations in China will comply with the Cyber Security Law when the Law takes effect from June 1, 2017.

For example, business entities which collect personal information from China will need to abide by the rules under the Cyber Security Law in handling personal information. If the business is relation to the Critical Information Infrastructure Facilities, special care must be taken in relation to data localisation requirement and the security assessment procedure. Data residence requirements may be challenging for multinational enterprises, if they need to transfer data cross-border in their business operations.

Another issue is that some language used in the Cyber Security Law is fairly generic and vague and further implementing rules are yet to be issued. This could create ambiguity and uncertainty as to how the Law will be interpreted and implemented in practice. For example, it is not known at present what equipment would fall into the category of "Key Network Equipment" and "Specialised Network Security Products" and it is not clear according to what criteria or procedures the security assessment will be conducted for the Critical Information Infrastructure Facilities. We expect that clarifications and guidance will be formulated by the Chinese authorities and we will continue to monitor and provide updates.

To subscribe for updates from our Data Protection Report blog, visit the email sign-up page.

For more information contact:

Barbara Li
Partner, Beijing
Tel +86 10 6535 3130
barbara.li@nortonrosefulbright.com

Olivia Yang
Associate, Beijing
Tel +86 10 6535 3161
olivia.yang@nortonrosefulbright.com

This time it's personal: Senior management liability in "books and records" offences

"Senior managers who choose to turn a blind eye towards the corrupt practices of their companies and the employees they supervise may find themselves personally liable for allowing the company's books to be altered to conceal the corrupt nature of the payments made – even if it could not be shown that they had actually engaged in the payment of bribes."

Corruption is by nature a secretive economic crime that is both difficult to detect and prove. As both the bribe giver and recipient are liable for the offence of bribery, there is little incentive for any party to a corrupt transaction to report the offence to the authorities or to fully cooperate in any investigation. Conversely, the parties may be more inclined to collude and conceal their involvement in the corrupt transaction. The difficulty in detecting and proving corruption is further complicated where a corporate entity is involved. In such cases involving the corporatisation of bribery, complex corporate structures and creative accounting practices may be employed to conceal the involvement of the individuals, especially those occupying senior positions in the company.

Nevertheless, recent cases in Singapore have shown that Singapore authorities are prepared to deploy a range of prosecutorial techniques so as to bring senior managers to account for their role in corrupt schemes through false accounting and money-laundering offences. This approach shows a striking similarity with the US-style "books and records" offences often used by US prosecutors in complex bribery schemes, and the new false accounting offences recently enacted in Australia which will bolster the anti-bribery toolbox of the Australian Federal Police.

ST Marine

In PP v Han Yew Kwang, Han Yew Kwang (Han), a former deputy president at ST Marine, was prosecuted for conspiring with a number of colleagues, who were all senior executives at ST Marine at the material time, to pay bribes to employees of ST Marine's customers in order to obtain business from these customers. An integral part of this scheme involved disguising the bribes as bogus entertainment expenses which were paid out from petty cash vouchers as approved by the senior management of ST Marine, i.e. the accused and his co-conspirators. It is pertinent to note that Han and his colleagues were not the ones who carried out the payment of the bribes. Rather, they approved the fraudulent petty cash vouchers, which they knew were not genuine entertainment expense claims, that were presented to them.

Even though Han and a number of his co-accused admitted their involvement and cooperated in the course of investigations, it was evident that proving the individual acts of bribery was difficult. This was because investigations were hampered by the fact that key witnesses and the receivers of the bribes were mainly located overseas.

Nevertheless, this difficulty was surmounted by the use of section 477A of the Penal Code Cap. 224 (section 477A), which criminalises the falsification of a company's accounts by a clerk or servant of the company with intent to defraud. Given that the bribes were essentially paid out of petty cash payment vouchers falsely recorded as "entertainment expenses", this approach had the effect of bringing the accused and his conspirators to account for their role in the corrupt scheme, i.e. for approving the individual fraudulent payments, in addition to the general conspiracy to pay bribes.

Questzone

The authorities adopted a similar tactic in the prosecution of Thomas Philip Doerhman (Doerhman) and Lim Ai Wah (Lim), who were sentenced to 60 and 70 months jail respectively on 1 September 2016, for falsifying accounts under section 477A and money laundering offences under the Corruption, Drug Trafficking and other Serious Crimes (Confiscation of Benefits) Act Cap. 65A (CDSA). Doerhman and Lim, who were both directors of Questzone Offshore Pte Ltd (Questzone), were prosecuted for conspiring with a third individual, Li Weiming (Li), in 2010 to issue a Questzone invoice to a Chinese telecommunications company seeking payment of US$3.6 million for a fictitious sub-contract on a government project in a country in the Asia-Pacific. Li was the chief representative for the Chinese company in that country. A portion of the monies paid out by the Chinese company to Questzone pursuant to its invoice was then subsequently redistributed by Doerhman and Lim to Li and the then Prime Minister of that Asia-Pacific country in 2010.

Even though no corruption charges were brought under the Singapore Prevention of Corruption Act against the parties, it is plainly conceivable that Questzone functioned as a corporate conduit for corrupt payments to be made. On the facts, some key witnesses were overseas – with Li having absconded soon after proceedings against him commenced. The use of section 477A and money-laundering charges under the CDSA allowed the prosecution to proceed against Doerhman and Lim as they only needed to prove that the invoice was false, in respect of the section 477A charge; and that the monies paid out pursuant to the invoice – which would be proceeds of crime or property used in connection with criminal conduct – were transferred to Li and the then Prime Minister of the Asia-Pacific country, in respect of the money-laundering offences.

US and Australian approach: "books and records"

The use of false accounting offences to prosecute senior management for their involvement in corrupt transactions is well established in the US. The Securities and Exchange Commission (SEC) is known to utilise the "books and records" provision in the Foreign Corrupt Practices Act (FCPA) to prosecute senior managers in listed entities for their role in the corrupt transactions. The relevant provision requires listed entities in the US to keep books and records that fairly and accurately reflect the transactions of the corporation. Therefore, a scheme involving the doctoring or manipulating of company records in order to conceal the corrupt transactions would cause the company to be in violation of this provision. Senior management who engage in or otherwise permit such conduct could be found similarly liable.

As far back as 2009, the SEC has used the books and records provisions aggressively to charge individuals. In the Nature's Sunshine case, the CEO and CFO of the company were charged with FCPA violations for failure to adequately supervise employees to make and keep accurate books and records and implement an adequate set of internal controls, despite not having direct knowledge or involvement in the bribery scheme. In a more recent example, the SEC charged Ignacio Cueto Plaza (Cueto), the former CEO of LAN Airlines S.A. (LAN), for his role in authorizing US$1.15 million in payments to a consultant pursuant to a sham consulting contract. The SEC alleged that Cueto "understood that it was possible the consultant would pass some portion of the [payment] to union officials" in an effort to resolve a dispute between LAN and its employees. Although unable to prove that a bribe payment occurred, the SEC stated

> *"The payments were made pursuant to an unsigned consulting agreement that purported to provide services that Cueto understood would not occur. Cueto authorized subordinates to make the payments that were improperly booked in the Company's books and records, which circumvented LAN's internal accounting controls."*

In another recent example, the SEC charged Jun Ping Zhang (Zhang), the former CEO and Chairman of Harris Corporation's (Harris) Chinese subsidiary CareFx China, for his role in facilitating a bribery scheme that provided illegal gifts to Chinese officials in exchange for business. Pursuant to the scheme, Zhang authorized and approved false expense claims that were used to provide gifts to officials. The SEC charged Zhang with violations of both the anti-bribery and accounting provisions of the FCPA, alleging

> *"[Zhang] was Harris' gatekeeper at CareFx China, but he nonetheless authorized false expense claims that he knew were going to be used to provide gifts to government officials. Moreover, Ping helped his subordinates at CareFx China hide the bribe scheme from Harris auditors and employees."*

In a move that will bring the Australian anti-corruption regime closer to the US and Singapore approach, new offences involving false dealing with accounting documents came into effect on March 1 2016. Under the new law, it is an offence for an individual or corporation to intentionally or recklessly facilitate, conceal or disguise in their accounting documents an occurrence of bribery, corruption or loss to a person that was not legitimately incurred. Importantly, proof that a benefit (not legitimately due) was actually received or given by the accused or another person is not required. This overcomes an evidentiary limitation that has historically been difficult for prosecutors to overcome.

It's personal: liability of senior executives under scrutiny

Senior managers who choose to turn a blind eye towards the corrupt practices of their companies and the employees they supervise may find themselves personally liable for allowing the company's books to be altered to conceal the corrupt nature of the payments made – even if it could not be shown that they had actually engaged in the payment of bribes.

The approach adopted by the SEC, which focuses on the complicity of senior executives and their failure to ensure that the company maintains accurate books and records and implements appropriate internal controls, should not be surprising in light of the memorandum titled "Individual Accountability for Corporate Wrongdoing" issued in September 2015 by the US Assistant Attorney General, Sally Yates, to all US Department of Justice (DOJ) prosecutors and civil litigators. The "Yates Memo" is largely seen as a signal of intent by the DOJ to pursue and punish individuals for their role in corporate crime, in response to prior criticism that not enough had been done to hold individuals to account for their decisions which led to the financial crisis of 2007-2009.

This approach of targeting individuals in general, and senior executives in particular, was echoed in Singapore by Attorney-General VK Rajah SC (A-G Rajah) in an opinion editorial in November 2015, where he urged corporates to adopt a culture of compliance in order to combat commercial crime. In a portentous statement threatening to pierce the corporate veil, A-G Rajah warned that there was "no certainty of escape from liability" for those seeking to hide behind complex corporate structures.

Senior management cannot act in conscious disregard or be wilfully blind to corrupt practices in their organisations. The specific targeting of individuals by the authorities, through the use of "books and records" type and anti-money laundering offences, puts senior executives on notice of the need for them to prevent, detect and properly respond to corporate wrongdoing – and to set the right tone from the top.

As far as liability is concerned, this time it's personal.

An earlier version of this article was first published on *Thomson Reuters Accelus Regulatory Intelligence and Compliance Complete*.

For more information contact:

Wilson Ang
Partner, Singapore
Tel +65 6309 5392
wilson.ang@nortonrosefulbright.com

Abigail McGregor
Partner, Sydney
Tel +61 2 9330 8742
abigail.mcgregor@nortonrosefulbright.com

Paul Sumilas
Senior associate, Singapore
Tel +65 6309 5442
paul.sumilas@nortonrosefulbright.com

Jeremy Lua
Associate, Singapore
Tel +65 6309 5336
jeremy.lua@nortonrosefulbright.com

But does it really work? The value of ISO certification of anti-bribery compliance

The highly-anticipated ISO standard for anti-bribery management systems – ISO 37001 – was recently published. The standard and its guidance represent the outcome of an arduous process, where stakeholders from many nations and representing a range of interests agreed a set of principles that organisations of all sizes (whether public, private or not-for-profit) can use to design anti-bribery management programmes. The ISO does not intend or purport to create new ground, but rather consolidates existing guidance from regulators, intergovernmental organisations and NGOs.

Organisations might consider obtaining ISO certification for any range of reasons. First and foremost, such a certification can indicate to a company's customers, business partners, investors and any others exposed to the company's risk profile that the organisation's programme meets baseline standards.

However, companies considering certification should be mindful that an ISO 37001 certification means that an anti-bribery management programme of a certain design exists, with all of the constituent parts prescribed by ISO; it does not mean that the programme really works. This is an important point, as any government agency looking to take enforcement action against an organisation for bribery and corruption related offences will inevitably undertake its own assessment of whether that organisation's compliance programme is genuinely effective in its day-to-day application.

ISO 37001 in summary

In terms of content, ISO 37001 defines bribery by reference to the laws applicable to each organisation and prescribes various actions, measures and controls that would be familiar to experienced legal, compliance and risk professionals. These include

- Conducting a risk assessment to determine the risks faced by the organisation
- Providing related training for all relevant employees and business associates
- Conducting appropriate due diligence to assess bribery risks
- Top management leadership and commitment
- Providing appropriate resources for the operation of the anti-bribery management system
- Implementing appropriate financial and commercial controls to mitigate the risk of bribery
- Having whistle-blowing procedures in place
- Monitoring and testing the programme's effectiveness on a regular basis.

ISO certification can be a useful indication to external stakeholders that these elements exist within an organisation. For the business partner who requests information about a company's anti-bribery management programme, ISO certification could be shorthand for describing the various elements in place.

Further, regulators who want to encourage a compliance culture in jurisdictions with less enforcement history than the United States or United Kingdom may point to ISO 37001 as guidance for local organisations. Because ISO37001 is a global commercial standard, it may be better received than standards promulgated by the US or UK regulators, whose extraterritorial reach is sometimes perceived as unreasonable

Genuinely effective?

Anti-bribery management programmes have two main aims

1. to mitigate the risk and incidence of corruption within an organisation

2. to provide a credible response to prosecutors when, despite best efforts, a corrupt act occurs.

Programmes that achieve those two aims are those that actually work, rather than just exist.

The message frm relevant authorities is unambiguous: only truly effective anti-bribery management programmes merit consideration in terms of penalty mitigation or, where applicable, an affirmative defence. In fact, the UK Government Guidance on Corporate Prosecutions[1] lists an ineffective compliance programme as an aggravating factor that should encourage a decision to prosecute. Similar language appears in the UK Deferred Prosecution Agreements Code of Practice.[2] A key takeaway from the Standard Bank DPA is that ineffective anti-bribery programmes will not be considered "adequate procedures, despite the moving parts that may exist.[3]

US authorities ask "three basic questions: Is the company's compliance programme well designed? Is it applied in good faith? Does it work?".[4] US regulators often give some weight to a respondent's compliance programme, but mitigation is only awarded in cases where the programme is truly effective – and where the alleged corrupt activity took place despite the company's best efforts.

What is a corporate to do?

ISO certification could certainly be a valuable exercise for any organisation looking to ascertain whether its programme – or at least its plan for developing the programme – hits all the right marks. Seeking certification should not, however, direct company resources away from focussing on meeting the standards regulators set: is the programme mitigating the risk and incidence of corruption, and is it providing a credible response when impropriety nonetheless occurs?

Achieving these goals – as opposed to a certification – is hard work and takes planning, expertise and cultural change management. Reflecting this, the ISO standard notes in its appendix that senior managers must have "genuine intent" and a "genuine commitment to prevent, detect and address bribery in relation to the organisation's business".[5] This matches various guidance documents issued by the authorities, such as the UK Ministry of Justice Bribery Act Guidance,[6] the FCPA Resource Guide[7] and the US Federal Sentencing Guidelines.[8]

The dangers of an over-reliance on certification were highlighted earlier this year when Australian journalists alleged that Monaco-based Unaoil had helped various multi-national companies secure government licences using improper payments. Unaoil had previously been certified by a well-known due diligence provider. The matter is now subject to a number of criminal inquiries by authorities including the SFO, and the press has labelled the agent, "The intermediary that allegedly bribed the entire oil industry".[9]

Ensuring that your anti-bribery management programme really works takes genuine review and assurance: not just an auditing process, but substantive transaction testing to ensure that legal risks are being appropriately identified and mitigated, that processes are being followed and that the correct decisions are being made by businesses, legal and compliance personnel. Such an outcomes-based assessment provides metrics and management information to executives and boards, which enables a company to determine with confidence whether their programme really works. The same can be done, albeit with more qualitative feedback, with respect to development of ethical culture and training effectiveness. What dilemmas are facing your managers, and how effectively does their reflex meet the challenge? Is your training programme changing hearts and minds, and how can you do better? Is your message being heard?

Real commitment and action is the challenge in any organisation and

1 See page 7, available here: https://www.sfo.gov.uk/publications/guidance-policy-and-protocols/codes-and-protocols/

2 See page 5, available here: https://www.sfo.gov.uk/publications/guidance-policy-and-protocols/deferred-prosecution-agreements/

3 For further information about the Standard Bank DPA, please see Norton Rose Fulbright's prior client alert

4 See page 56, available here: https://www.sec.gov/spotlight/fcpa/fcpa-resource-guide.pdf

5 See paragraph A.3.1., available here: http://www.iso.org/iso/catalogue_detail?csnumber=65034

6 See in particular Principle 2, available here: https://www.justice.gov.uk/downloads/legislation/bribery-act-2010-guidance.pdf

7 See page 56, available here: https://www.sec.gov/spotlight/fcpa/fcpa-resource-guide.pdf

8 See § 8B2.1(b), U.S. Sentencing Guidelines, available here: http://www.ussc.gov/sites/default/files/pdf/guidelines-manual/2014/CHAPTER_8.pdf

9 http://www.forbes.com/sites/jwebb/2016/07/26/serious-fraud-office-moves-against-unaoil-the-intermediary-firm-that-bribed-the-entire-oil-industry/#6d8b5aad435c

the key to effective anti-bribery management programmes. The new ISO standard gives corporates a set of tools by which they can meet that challenge, but whether those tools are deployed effectively is a matter of real testing and assurance.

Norton Rose Fulbright was delighted to be represented as the only legal practice on the UK based BSi Anti-Bribery Committee which worked on the ISO standard on anti-bribery (ISO 37001). This followed our earlier work on the British Standards Institute's panel in connection with the drafting of the first British Standard on Anti-Bribery (BS 10500).

For more information contact:

Jason Hungerford
Partner, London
Tel +44 20 7444 2474
jason.hungerford@nortonrosefulbright.com

Paul Sumilas
Senior associate, Singapore
Tel +65 6309 5442
paul.sumilas@nortonrosefulbright.com

Stuart Neely
Associate, London
Tel ++44 20 7444 3289
stuart.neely@nortonrosefulbright.com

Contacts

Asia

China
Sun Hong
Tel +86 21 6137 7020
hong.sun@nortonrosefulbright.com

Hong Kong
Alfred Wu
Tel +852 3405 2528
alfred.wu@nortonrosefulbright.com

India
Sherina Petit
London
Tel +44 20 7444 5573
sherina.petit@nortonrosefulbright.com

Japan
Eiji Kobayashi
Tel +81 3 5218 6810
eiji.kobayashi@nortonrosefulbright.com

Singapore
Wilson Ang
Tel +65 6309 5392
wilson.ang@nortonrosefulbright.com

Thailand
Somboon Kitiyansub
Tel +662 205 8509
somboon.kitiyansub@nortonrosefulbright.com

Sarah Chen
Tel +662 205 8518
sarah.chen@nortonrosefulbright.com

Australia
Abigail McGregor
Melbourne
Tel +61 3 8686 6632
abigail.mcgregor@nortonrosefulbright.com

Global

Head of business ethics and anti-corruption
Sam Eastwood
Tel +44 20 7444 2694
sam.eastwood@nortonrosefulbright.com

Global head of investigations
Chris Warren-Smith
Tel +44 20 7444 5992
chris.warren-smith@nortonrosefulbright.com

Global co-heads of regulation and investigations
Martin Coleman
Tel +44 20 7444 3347
martin.coleman@nortonrosefulbright.com

Lista M Cannon
Tel +44 20 7444 5991
lista.cannon@nortonrosefulbright.com

Global resources

Our office locations

People worldwide

7000+

Legal staff worldwide

3500

Offices

50+

Key industry strengths

- Financial institutions
- Energy
- Infrastructure, mining and commodities
- Transport
- Technology and innovation
- Life sciences and healthcare

Europe

- Amsterdam
- Athens
- Brussels
- Frankfurt
- Hamburg
- London
- Milan
- Monaco
- Moscow
- Munich
- Paris
- Piraeus
- Warsaw

United States

- Austin
- Dallas
- Denver
- Houston
- Los Angeles
- Minneapolis
- New York
- Pittsburgh-Southpointe
- St Louis
- San Antonio
- San Francisco
- Washington DC

Canada

- Calgary
- Montréal
- Ottawa
- Québec
- Toronto
- Vancouver

Latin America

- Bogotá
- Caracas
- Rio de Janeiro

Asia Pacific

- Bangkok
- Beijing
- Brisbane
- Hong Kong
- Jakarta[1]
- Melbourne
- Port Moresby (Papua New Guinea)
- Perth
- Shanghai
- Singapore
- Sydney
- Tokyo

Africa

- Bujumbura[3]
- Cape Town
- Casablanca
- Dar es Salaam
- Durban
- Harare[3]
- Johannesburg
- Kampala[3]

Middle East

- Abu Dhabi
- Bahrain
- Dubai
- Riyadh[2]

Central Asia

- Almaty

1 TNB & Partners in association with Norton Rose Fulbright Australia
2 Mohammed Al-Ghamdi Law Firm in association with Norton Rose Fulbright (Middle East) LLP
3 Alliances

NORTON ROSE FULBRIGHT

Norton Rose Fulbright

Norton Rose Fulbright is a global law firm. We provide the world's preeminent corporations and financial institutions with a full business law service. We have more than 3500 lawyers and other legal staff based in more than 50 cities across Europe, the United States, Canada, Latin America, Asia, Australia, Africa, the Middle East and Central Asia.

Recognized for our industry focus, we are strong across all the key industry sectors: financial institutions; energy; infrastructure, mining and commodities; transport; technology and innovation; and life sciences and healthcare.

Wherever we are, we operate in accordance with our global business principles of quality, unity and integrity. We aim to provide the highest possible standard of legal service in each of our offices and to maintain that level of quality at every point of contact.