PECB Insights

ANTI-BRIBERY AND COMPLIANCE:
TOOLS FOR SUSTAINABLE BUSINESS

LEADERSHIP   STANDARDS   EXPERTISE   TECHNOLOGY   BUSINESS & LEISURE   TRAVEL   SUCCESS STORY   OPINION   BOOKS   INNOVATION

In This Issue

"If corruption
is a disease,
transparency is
a central part of
its treatment."

KOFI ANNAN,
FORMER UN SECRETARY GENERAL
& NOBEL PEACE PRIZE LAUREATE

Anti-Bribery and the COVID-19 Pandemic: How to Prove a Bribery Charge?

✎ **BY ROBIN M SINGH, MS(LAW), MBA, MS(IT), GLEG (US PRIVACY LAW), CCEP-I, CFE, HCCP**

The ongoing COVID-19 pandemic has resulted in wide-scale disruption of all aspects of life. While governments and individuals continue to grapple with the devastating effects of the virus, they also face the challenges of corruption.

This article takes a closer look at the link between COVID-19 and the increased risk of bribery in different sectors, and the elements required to prove a bribery charge in the US.

The pandemic and corruption: What is the link?

It is widely known, as well as studied by many experts of the field that corruption has existed for thousands of years and the earliest records of bribery date back to 3000 B.C. Studies show that natural disasters increase corruption in public sectors across developed and developing countries.

The frequency of natural disasters significantly impacts the level of corruption in developed countries. During these times, owing to shifting priorities, organizations face the risk of deprioritizing their key objectives of business integrity, transparency, and whistleblowing. The uncertainties posed by the ongoing COVID-19 crisis led businesses across sectors and industries to focus on disaster recovery, business continuity, and client/employee welfare over integrity.

While the pandemic has stressed out organizational infrastructures in many ways, the crisis has encouraged poor behavior among clients, third parties, and employees across sectors such as healthcare, pharmaceuticals, oil and gas, and others.

Healthcare

Corruption in healthcare is not a new phenomenon. Estimations show that while $7.35 trillion was being spent annually across the world on healthcare before the pandemic crisis, $455 billion was lost to corruption.

Massive resources that were mobilized in response to the pandemic created immense opportunities for corruption. In addition, corruption prevention mechanisms have been suspended owing to the emergency.

Corruption risk undermines the trust of the public in public institutions while supplies and resources get squandered, blocking their flow to people who need them the most. From falsification of certificates for medical equipment, unnecessary intermediaries to delivery of lower quality equipment, bribery and kickbacks were rampant in the healthcare system.

Transparency International's survey of Asian nations reveals that bribery rates were the highest in the past year. While utility services topped the list where citizens faced the highest corruption in India, public health services were the second in the list. Apart from India, some of the Asian countries that had a high bribery rate include Indonesia, Sri Lanka, Bangladesh, Malaysia, Japan, and Vietnam.

Oil and gas

Oil and gas or other extractive industries have always been vulnerable to corruption and the most common of them being paying bribes to win contracts. One of the factors that increases the corruption risk is the complex relationships the companies have with government officials and multiple third parties across

An anti-fraud company based in Germany surveyed 58 countries and found that a majority experienced corruption with respect to access or purchase of PPE (personal protective equipment). According to another report, irregularities were the norm in coronavirus response-related government contracts across dozens of countries.

the world. Secondly, these companies often look for natural resources in emerging markets that may lack the infrastructure, stability, and regulatory environments.

The OECD (Organisation for Economic Cooperation and Development) Foreign Bribery Report from 2014 finds that 53% of foreign bribery cases in the sector involved CEOs or corporate management. While intermediaries were involved in three out of four bribery cases (marketing and sales agents, distributors, local consulting companies, and so on), in 57% of cases, bribes were paid to secure public procurement contracts. Bribes were offered, given, or promised frequently to employees of state-owned or public enterprises, custom officials, and defense and health officials.

The full impact of the pandemic in the oil and gas industry remains to be seen. However, according to the Natural Resource Governance Institute, the falling demand, the oil price shock, disrupted supply, and reduced commodities' prices combine to increase the risk of corruption in the sector.

Both private and national oil companies are facing pressure across the world to cut costs. From shuttering off key projects, layoffs slowed down, or shutting production to financial losses, oil companies are going through an unprecedented crisis. Consequently, executives may opt to reduce budget allocation to compliance and anti-corruption measures and compliance (such as due diligence, project monitoring, public reporting, staff training).

The second risk relates to cutting corners with regulators facing the challenge of monitoring the companies' behavior during the pandemic. Complying with health, labor, safety, and environmental regulations is expensive, which can prompt struggling companies to side-step obligations or attempt to bribe regulators, or exploit weaknesses within regulatory enforcement.

Pharmaceuticals

Corruption instances in pharmaceuticals and medical supply procurement are bountiful across the countries during the pandemic. Dubious contracts have been awarded to procure N95 face masks, testing kits, and PPE kits. In Brazil, for instance, face masks were purchased from a supplier close to the President. These masks were 67% costlier than other supplier bids.

Corrupt activities and kickbacks are also quite common when it comes to the procurement of essential medicines. Apart from improper bidding procedures, bribes for inspectors and kickbacks for referrals are common in public procurement. Many high-profile cases in recent times have highlighted the widespread proliferation of bribes and kickbacks in the industry. Pharmaceutical companies bribe doctors to influence their decisions over prescriptions and consequently, procurements. For instance, Novartis paid $678 million to settle a corruption lawsuit in 2020. The firm was found to have spent over $100 million for its extensive kickback program to influence doctors to prescribe its medicines.

Anti-bribery legislation in the US

The Foreign Corrupt Practices Act (FCPA) of 1977 is the main anti-bribery legislation in the US. The law prohibits companies and individuals from offering corrupt payments directly or indirectly to foreign officials or entities. However, the FCPA does not cover employees and officials of the federal and state governments in the US.

Domestic bribery is covered in 18 U.S.C. § 201 that was enacted in 1962. The statute prohibits individuals and companies in the US from offering bribes of any kind to public officials to influence an official act. An overlapping statute is the mail and wire fraud statute (18 U.S.C. § 1346) that defines honest services fraud that prohibits corrupt schemes intended to deprive another of their right to honest services.

Additionally, the US is also a member of the UN Convention against Corruption, OECD Anti-Bribery Convention, and Inter-American Convention against Corruption. Apart from these, many states have their own anti-bribery laws and limitations on gift and hospitality offered to government officials.

Proving bribery

18 USC Section 201 has two parts: Section 201(b) criminalizes bribery, while Section 201(c) prohibits receiving or payment of gratuities. To prove bribery took place under Section 201(b), quid pro quo (bribe offered in exchange for a favor) has to be established, while this is not a requirement under the gratuities provision.

To secure a conviction for the one who paid a bribe under Section 201(b), it has to be proven that a bribe (something of value) was promised, offered, or given to a public official to influence an official act. To obtain the conviction of the one who received bribe, it has to be proven that a public official agreed, accepted, or solicited to accept bribe in return of "being influenced".

For gratuities conviction, the only aspect to be proven is that bribe has been willingly offered or given "because or for any official act". It is not necessary to show that there was intent to influence any official act with the bribe.

At a basic level, the only thing that has to be proven in charges of bribery is that an agreement took place between the concerned parties that a favor would be provided in exchange for cash or something of value.

While a written agreement may not be required to prove the same, prosecutors have to establish that the agreement actually took place. For instance, a recorded phone conversation where a politician agreed to receive bribe from a party could constitute evidence. A video of an officer accepting cash from a driver before letting the latter go is also evidence.

Typically, the prosecution relies on paper evidence in cases of bribery for proving intent. These can include receipts, bank statements, text messages, and emails in addition to any evidence gathered from recorded phone conversations and wire taps.

In cases where there is no paper or recorded evidence, prosecutors may also provide evidence of the defendant's flashy lifestyle. Circumstantial evidence may also be enough to show that bribe happened. For instance, there could be evidence that shows a contract was opened for bidding and a meeting between the concerned parties happened. Sometime later, the official offering the contract goes on an expensive vacation that they earlier could not afford as their financial records show during the investigation. The argument here will be that there is circumstantial evidence to show the official was offered and accepted a bribe from the one who secured the contract.

Subpoenas are another way of gathering evidence, while whistleblowers are often the initiators of the bribery charges.

Whistleblowers are offered protection as well as incentives under the FCPA such as monetary awards that range from 10 to 30% of the amount of bribe collected. Retaliation against whistleblowers is also prohibited and penalized.

The person who accepted the bribe must be a public official such as federal employees or elected officials. The one who offers the bribe must be offering cash, promise of support, something of value, or another type of favor. The other key element for proving bribery is that the person who receives the bribe does a favor in return for the bribe such as voting in favor of law. It must be proven that the public official or the person receiving the bribe has the authority to carry out the favor and that the one who bribed had a specific intent.

In addition, proof is required of a causal relationship between the official act and the bribe that is not simply a suspicious coincidence. Solicitation of bribe is also a crime even if it does not result in receiving a valuable gift.

Conclusion

The pandemic crisis has created exigent circumstances that raise the risk of bribery within the country and FCPA issues. Extended national lockdown across the country has increased pressure on businesses to procure supplies and raise revenue. Sectors such as life sciences, pharmaceuticals, healthcare, and allied businesses are at significant risk for anti-bribery regulation violations.

With factories remaining closed or operating at minimal levels in response to the COVID-19 situation, many multinational companies are faced with the scarcity of their traditional sources of labor, goods, and raw materials. While minimizing the negative impacts on their revenue, companies need to revamp their due diligence practices to meet the demands of the new circumstances. Given the extent of the financial impact of lockdowns, the risk of bribery and corruption remains high as businesses or individuals seek to influence government officials in this regard.

Laws that cover bribery are utilized to punish the one offering the bribe as well as the one who receives it. Defendants (the ones charged with taking bribe) can include government officials, elected representatives, board members, police officers, sports officials, labor union officers, and business leaders.

For any individual or entity, a bribery charge can mean a huge reputational and business risk. If the charges are proven, the penalties including jail time and fines can be severe. Consulting a white-collar crime attorney is the crucial step in proving or defending yourself against a bribery charge.

Robin M Singh
Ms(Law), MBA, Ms(IT), GLEG (US Privacy Law), CCEP-I, CFE, HCCP

in

Robin has received the "Top 50 Smart Leaders" award across the Middle East in the field of Healthcare Ethics and Compliance and the "40 under Forty" Maverick award by the national association of valuators, the USA for Compliance, and Investigations. He has worked across jurisdictions such as UAE, Kuwait, Oman, Singapore, and India; and even in high-risk jurisdictions such as Afghanistan. He has assisted major entities and many of them fortune 500 companies to swim through the regulatory, ethical, and privacy-related dilemmas.He has developed client-adaptive programs and dealt with a wide range of engagements relating to ethics, privacy, compliance, and anti-bribery/anti-fraud framework. He has authored more than 25 papers/articles across various international journals and magazines. He was instrumental in setting up the Regulatory Affairs Compliance and Privacy Program in the Healthcare Government Entity and is currently working with committees to address queries associated with his field of expertise during the time of the pandemic.

Enjoyed Reading this Article?

Join our upcoming Anti-Bribery Conference scheduled for May 17-20, 2021. Register for FREE and attend the conference for more insights on related topics.

The Leadership Illusion: Are You As Ethical As You Believe You Are?

✎ BY MICHAEL BRET HOOD

If you were the Chief Executive Officer (CEO) of a networking and cybersecurity organization and you learned about employees who were knowingly utilizing third parties to pay bribes to government officials, what would you do if such payments clearly violated Canada's Corruption of Foreign Public Officials Act (CFPOA)? Would you turn your head and allow the practice to continue as long as the payments brought in significant revenues? More likely, you would choose to end the practice immediately. Yet, if you were the leader of your organization and had to make such a choice, the decision you think you would make is not likely to match the decision that you actually would make.

The previous statement is certainly not meant to detract from your integrity or ethicality, but rather, it reflects how your brain operates in ways that we don't always consciously recognize, especially as you move up the organizational hierarchy. It has been estimated that approximately 95% of your daily decisions are made automatically and without conscious thought. Before you go any further in this article, take a moment and think about how you would answer the following questions:

> Do you rank in the top 10%, top 25%, top 50%, or the bottom 50% when assessing your leadership ability as compared to your organizational colleagues?

> On a scale of one to ten with one being absolutely unethical, ten being absolutely ethical, and five in the middle, rate your own ethicality on this numeric scale.

How do you think that your colleagues and executives would have answered those questions? The case highlighted in the first paragraph involved a Juniper Networks, Inc. senior manager who learned about a secret slush fund that was being used by employees to facilitate bribes that earned

government contracts yet did nothing of substance to stop the illegal behavior. If posed the same questions about leadership and ethicality, how do you think the senior manager would have responded?

Organizations spend millions of dollars each and every year on leadership and compliance efforts, yet despite the substantial investment, reports of unethical behavior emerge frequently. Typically, the excuses provided for such leadership and ethical failures involve the bad seed or the deviant employee, but if you were to dig further, you might find that the people and the leaders who committed the unethical transgressions were very similar to you. Illusory superiority is your natural tendency to rate yourself, when compared to others, in a much more favorable way than what may be true. Participants in one of our leadership development classes are asked this question and told to move to the designated corner of the room that matches their response.

Statistically, there should be half of the people in the corner of the room identified as the bottom 50%, but how many participants do you think would actually walk to that corner? There have never been more than just a few.

As you think about your answer to that question, is it possible that illusory superiority can or has affected you? Confidence is an important part of being a leader, but as you gain power and prestige in an organization, there are deleterious effects that occur to your leadership, including overconfidence. By the time you become an executive leader, research has shown that you will become very overconfident in your judgments, your risk acceptance, and in your decision-making. Therefore, what may seem to be an easy ethical decision as you look at it from your perspective could easily be different from the perspective of someone who has a vested interest in the decision outcome.

Max Bazerman and Ann Tenbrunsel, in their book "Blind Spots: Why We Fail to Do What's Right and What to Do about It", introduce a concept they refer to as the "Want Self" and the "Should Self."

> **"The "Want Self" describes the side of you that's emotional, affective, impulsive, and hot-headed. In contrast, your "Should Self" is rational, cognitive, thoughtful, and cool-headed."**

As much as you like to believe that your decision-making is rational and thoughtful, emotions and impulse play a significant role. "When time comes to make a decision, our thoughts are dominated by thoughts of how we want to behave; thoughts of how we should behave disappear." The "Want Self," in conjunction with illusory superiority, often leads to bounded ethicality, the tendency for organizational pressures and psychological processes to cause us to engage in ethically questionable behavior that is inconsistent with our own values and preferences.

Illusory superiority also causes you to overestimate your ethicality. In the second bulleted question, you answered at the beginning of this article, did the number you picked to represent your ethicality go below a seven? If not, you would be the same as approximately 99% of the people who are asked this question in one of our ethics courses. In a matter of minutes, the interactive session provokes enough self-assessment that the participants realize they are not nearly as ethical as they believe themselves to be. What allows you to overestimate your ethicality is your ability to rationalize your decisions.

If you were to think about a time where you said or did something you regretted, can you recall the conversation that occurred almost instantaneously in your mind after the mistake? As soon as you thought about how you shouldn't have said or done whatever it was, the word "but" was inserted into your thoughts followed by your rationalization/ justification. When you or your followers deviate from ethical or compliance rules, your brain will automatically start to produce the excuses you need in order for you to maintain the belief that you are an ethical person. A leader who understands how easily people can rationalize their behaviors can pursue a more active approach when attempting to create an ethical organizational culture.

One of the methods your brain uses to alter and transform the dimensions of your decisions is through the use of euphemisms, a mild term used in place of another word that could be considered offensive or abrasive. Instead of paying a bribe to a foreign official, you offer a "grease payment." Instead of intentionally lying about something, you are providing "alternative facts." Euphemisms have long served as a means for you to camouflage decisions, behaviors, and thoughts which make you and your followers uncomfortable. "Euphemisms send a powerful informal signal about an organization's values to its employees: As long as you disguise and hide your unethical behavior, we will accept it, and indeed even encourage it." (Bazerman, M. & Tenbrunsel, A., 2011).

In order to improve your ethical leadership, being consciously aware of the power of euphemisms can lead to deeper discussions to determine the true context of their origin. For example, when you hear a follower use a euphemism in conversation, you could engage the follower in a more nuanced discussion to see if you can determine the reason why your follower chose to deploy the softer language. Simply hearing a follower use words such as collateral damage, creative accounting, and the like can give a clear indication of discomfort in the follower's actions, decisions, and/or behaviors. Likewise, taking the time to self-assess when you catch yourself deploying euphemisms can also lead to important discoveries about your true feelings, behaviors, and thoughts.

Another common technique to neutralize and rationalize unethical behavior in organizations is referred to as social proof, a psychological and social process for copying and adopting the actions and behaviors of others as social norms. If you think about the very first day you arrived in your organization, do you remember looking to others to see how you were supposed to dress, talk, and behave? Social cues from other organizational members, especially leaders, sets the tone for others and informally gives

direction on what is or isn't acceptable behavior within the organization. "Carrying messages that are heard but not seen, informal cultures represent the unofficial messages regarding ethical norms within the organization. It is through informal mechanisms that employees learn the 'true values' of the organization." (Bazerman, M. & Tenbrunsel, A., 2011).

If you contrast the Juniper Networks, Inc. case with a recent CFPOA filing against Imex Systems in Toronto, the leaders in that organization self-reported the bribery payments of their employee. When the executives of IMEX Systems chose to self-report, there was a message sent to the employees about tolerance for unethical acts such as paying bribes. If you were an employee of IMEX System's or Juniper Networks, Inc., what kind of message would you take from either company's action/inaction and how would it affect the formal and informal culture of each organization?

Employee goals are another method where leaders can influence the ethical behavior of the organization. While goals are certainly useful in establishing and measuring expected performance for your followers, leaders who create vague and unclear goals could inadvertently lead their people down the slippery slope. "Architects of reward systems often fail to consider how efforts to accomplish a target goal will cause decision-makers to ignore ethical problems in other areas." (Bazerman, M. & Tenbrunsel, A., 2011). Leaders who ignore these indirect effects can cause their followers to fall victim to the false consensus effect, your tendency to overestimate how acceptable and common your own behavior is in a society.

Nazir Karigar was a Canadian citizen employed by Cryptometrics Canada who was trying to obtain a $100 million security contract with Air India and was convicted of violating the CFPOA. During his trial, Karigar presented the defense that it was commonplace to offer bribes in India. The allegation of bribery as a cultural norm is an example of how bounded ethicality and the false consensus effect can directly lead to unethical behavior. By framing his decision to bribe government officials in the context of "everyone is doing it", Karigar saw his decision as standard behavior within the society, when the inverse was true.

Salespeople are frequently tasked with contradictory goals; generate a certain amount of sales while also acting in accordance with compliance procedures. When people face competing goals, it causes stress, which allows rationalizations that mute ethical obligations. "The rationalizations not only facilitate future wrongdoing but dull awareness that the act is, in fact, wrong. Indeed, if the rationalizations become a shared resource in the

organization's culture, they may pave the way toward defining the practice as 'business as usual' – the way things work." ([Vikas, A. et al.](#)). Organizations and leaders that openly clarify their stance on unethical behavior such as corruption and follow that clarification with appropriate action lessen the chance that the informal culture will send the message that "business as usual does not include bribery or other unethical behavior.

If you are like others, you probably have underestimated the difficulties of being a leader. You, although we don't like to admit it, are equally capable of rationalizing unethical behavior as anyone else. In order to fight against the natural reactions to increased organizational power such as overconfidence and illusory superiority, understanding your tendencies to overestimate your abilities and your ethicality can lead to decisions and behaviors you never imagined nor intended. Your integrity is only as good as your actions and whether you realize it or not, your followers are watching… and learning.
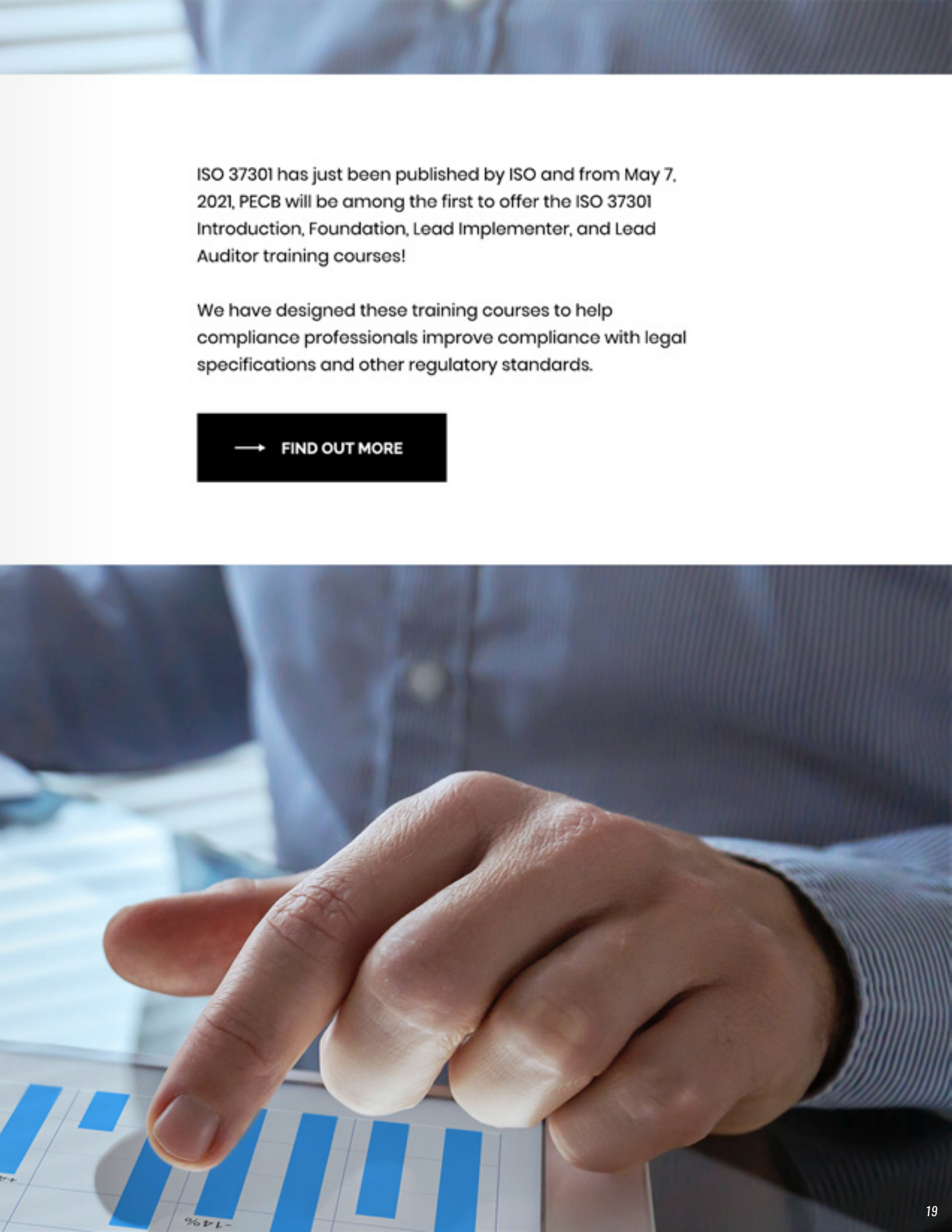
Michael Bret Hood
Director at 21st Century Learning & Consulting, LLC

in

After serving for 25 years as a Special Agent in the FBI, Michael "Bret" Hood became the director of [21st Century Learning & Consulting, LLC](#). Bret serves as an adjunct professor of leadership and ethics at the University of Virginia. Bret received two FBI Director Awards for Leadership Development for his work on executive leadership development programs. He offers leadership, ethics, and implicit bias trainings around the world and was recently named the James R. Baker Speaker of the Year by the Association of Certified Fraud Examiners.

ISO 37301:2021 Compliance Management Systems Training Courses

ISO 37301 has just been published by ISO and from May 7, 2021, PECB will be among the first to offer the ISO 37301 Introduction, Foundation, Lead Implementer, and Lead Auditor training courses!

We have designed these training courses to help compliance professionals improve compliance with legal specifications and other regulatory standards.

⟶ FIND OUT MORE

Out of the Box

New standard for compliance management makes everyone a winner.

The regulatory landscape is constantly changing and organizations need systems in place to ensure they keep up. But complying with laws and regulations can be so much more than just ticking a box: it can be the result of a deeply entrenched culture of integrity and good ethics. All of which is a recipe for business success. A compliance management system is a way of getting there and a new standard has just been published to help.

ISO 37301, Compliance management systems – Requirements with guidance for use, provides everything an organization needs to know to develop, implement, maintain and improve an effective compliance management system. It replaces ISO 19600:2014, Compliance management systems — Guidelines.

Howard Shaw, Chair of the ISO technical committee that developed the standard, said compliance is not just about avoiding fines and should not be limited to one department. It is everyone's affair.

"Organizations want to work and collaborate with companies they can trust," he said.

"And trust is built on a company culture of doing the right thing, where every employee contributes because they understand and believe in the importance of it. Central to this is good leadership and clear values, which have to come from the top."

In this way, ISO 37301 recommends the involvement of senior management and advocates compliance as a principle of good governance. It also recommends integrating compliance management right across the organization, to be embedded in its financial, risk, quality, environmental and health and safety management processes as well as its operational requirements and procedures.

The benefits of implementing ISO 37301 are expected to include not only a reduced risk of fines due to non-compliance, but enhanced reputation and credibility, providing greater confidence to clients and other stakeholders and increased business opportunities.

The standard can also be integrated into an organization's other management systems, such as ISO 37001 for anti-bribery or ISO 9001 for quality, thus increasing efficiencies, effectiveness and productivity.

Disclaimer: PECB has obtained permission to publish the articles written by ISO.

CREATING A CULTURE OF COMPLIANCE:

How to Build a Robust Anti-Bribery Compliance Program

✎ **BY NICO SNYMAN**

Bribery is a widespread phenomenon. It raises serious social, moral, economic, and political concerns, undermines good governance, hinders development, and distorts competition. It erodes justice, undermines human rights and is an obstacle to reducing poverty. It also increases the cost of doing business, introduces uncertainties into commercial transactions, increases the cost of goods and services, diminishes the quality of products and services, which can lead to loss of life and property, destroys trust in institutions, and interferes with the fair and efficient operation of markets.

Governments have made progress in addressing bribery through international agreements such as the Organization for Economic Co-operation and Development Convention on Combating Bribery of Foreign Public Officials in International Business Transactions and the United Nations Convention against Corruption and through their national laws.

In most jurisdictions, it is an offense for individuals to engage in bribery and there is a growing trend to make organizations, as well as individuals, liable for bribery. However, the law alone is not sufficient to solve this problem. Organizations have a responsibility to proactively contribute to combating bribery.

This can be achieved by implementing a robust Anti-Bribery Management System (ABMS), and through leadership commitment to establishing a culture of integrity, transparency, openness, and compliance. The nature of an organization's culture is critical to the success or failure of an ABMS. The ABMS and supporting management systems help an organization to avoid or mitigate the costs, risks, and damage of involvement in bribery, to promote trust and confidence in business dealings, and to protect its reputation.

This article reflects good practice and can be used in all jurisdictions. It is applicable to small, medium, and large

organizations in all sectors, including public, private, and not-for-profit sectors. The bribery risks an organization can face vary according to factors such as the size of the organization, the locations, and sectors in which the organization operates, and the nature, scale, and complexity of the organization's activities.

1. LEADERSHIP AND TONE AT THE TOP

Governance body and board oversight

Any organization with a Governing Body (GB)/Board of Directors (BoD) has the fiduciary responsibility to demonstrate leadership and commitment with respect to the ABMS by:

> Approving the organization's AB policy

> Ensuring that the organization's strategy and AB policy are aligned

> At planned intervals, receiving and reviewing information about the content and operation of the organization's ABMS

> Requiring that adequate and appropriate resources needed for effective operation of the anti-bribery management system are allocated and assigned

> Exercising reasonable oversight over the implementation of the organization's ABMS by top management and its effectiveness

Thus, a GB/BoD shall be directly liable for any bribery uncovered under their watch. There is no hiding away.

Top management, Exco's, and Manco's

The top management, whether it is the Executive Committee (Exco) or Management Committee (Manco) has the following responsibilities, depending on the role:

> Ensuring that the ABMS, including policy and objectives, is established, implemented, maintained, and reviewed to adequately address the organization's bribery risks

> Ensuring the integration of the ABMS requirements into the organization's processes

> Deploying adequate and appropriate resources for the effective operation of the ABMS

> Communicating internally and externally regarding the anti-bribery policy

> Communicating internally the importance of an effective ABMS and of conforming to the anti-bribery management system requirements

> Ensuring that the ABMS is appropriately designed to achieve its objectives

> Directing and supporting personnel to contribute to the effectiveness of the ABMS

> Promoting an appropriate AB culture within the organization

> Promoting continual improvement

> Supporting other relevant management roles to demonstrate their leadership in preventing and detecting bribery as it applies to their areas of responsibility

> Encouraging the use of reporting procedures for suspected and actual bribery

> Ensuring that no personnel will suffer retaliation, discrimination, or disciplinary action for reports made in good faith, or on the basis of a reasonable belief of violation or suspected violation of the organization's AB policy, or for refusing to engage in bribery

Compliance function

The GB/BoD and top management have the obligation to appoint an AB Compliance Function (ABCF). This function is responsible and has the authority for:

> Overseeing the design and implementation of the ABMS by the organization

> Providing advice and guidance to personnel on the ABMS and issues relating to bribery

> Ensuring that the ABMS conforms to the organization's own requirements, the requirements of the stakeholders, and the global best practices (ISO 37001)

> Reporting on the performance of the ABMS to the GB/BoD and top management and other compliance functions, as appropriate

The ABCF must be adequately resourced and assigned to person(s) who have the appropriate competence, status, authority, and independence. The ABCF must have direct and prompt access to the GB/BoD and top management if any issue or concern needs to be raised in relation to bribery or the ABMS.

The top management can assign some or all of the ABCF to persons external to the organization. If it does, it must ensure that specific personnel have responsibility for, and authority over, those externally assigned parts of the function.

Delegated decision-making

Decision-making is critical to implementing an ABMS. The ABCF must obtain the Delegation of Authority (DoA) for the making of decisions in relation to which there is a more-than-low risk of bribery, the organization shall establish and maintain a decision-making process or set of controls which requires that the decision process and the level of authority of the decision-maker are appropriate and free of actual or potential conflicts of interest. A critical part of the DoA is to review and implement continuous improvement strategies to empower the ABCF and the ABMS continuously. This is not a one-time exercise.

2. UNDERSTANDING THE ORGANIZATIONAL CONTEXT

Understanding the organization and its context

Every organization is different, and one-size-fits-all methodologies do not work in the real world. As part of the continuous improvement strategy and to fully understand the context the organization functions within, issues critical to its purpose and that affect its ability to achieve the objectives of its ABMS must be identified and then assessed.

These issues will include, without limitation, the following factors:

> The size, structure, and delegated decision-making authority of the organization

> The locations and sectors in which the organization operates or anticipates operating

> The nature, scale, and complexity of the organization's activities and operations

> The organization's business model

> The entities over which the organization has control and entities which exercise control over the organization

> The organization's business associates

> The nature and extent of interactions with public officials

> Applicable statutory, regulatory, contractual, and professional obligations and duties

Understanding the needs and expectations of stakeholders

Stakeholders are directly or indirectly part of any organization. One must understand the definition of stakeholders, prior to reading this further. Stakeholders are persons or organizations that can affect, be affected by, or perceive themselves to be affected by a decision or activity (ISO 73).

Every organization implementing an ABMS must determine:

> The stakeholders that are relevant to the ABMS, through a stakeholder analysis process. This shall include the Power/Influence matrix analysis of every stakeholder.

> The relevant requirements of these stakeholders. In identifying the requirements of stakeholders, an organization can distinguish between mandatory requirements and non-mandatory expectations of, and voluntary commitments to stakeholders.

Bribery risk assessment

Anti-Bribery Risk Assessment (ABRA) is the departure point in understanding the risks pertaining to bribery. The ABRA must include the following as a minimum requirement:

> Establish criteria (low, medium, high) for evaluating the level of bribery risk, which shall consider the organization's policies and objectives

> Identify the bribery risks the organization might reasonably anticipate, given the factors listed in the internal and external context analysis

> Analyze, assess, and prioritize the identified bribery risks

> Evaluate the suitability and effectiveness of the organization's existing internal controls (IC) to mitigate the assessed bribery risks

> As part of the continuous improvement strategy, these assessments must be reviewed on a regular basis so that changes and new information can be properly assessed based on timing and frequency defined by the organization or in the event of a significant change to the structure or activities of the organization.

It must be understood that the ABRA is an official document and can form part of any criminal, civil, or discipline process, thus, it must be conducted by competent AB specialists. It must also be signed off by the top management and the GB/BoD.

The intention of the ABRA is to enable the organization to form a solid foundation for its ABMS. This assessment identifies the bribery risks that the management system will focus on, the bribery risks deemed by the organization to be a priority for bribery risk mitigation, control implementation, and allocation of anti-bribery compliance personnel, resources, and activities.

3. CREATING AN ANTI-BRIBERY ORGANIZATIONAL CULTURE

Due diligence

Where the organization's ABMS has assessed a more-than-low bribery risk in relation to specific categories of transactions, projects, or activities, planned or ongoing relationships with specific categories of business associates, or specific categories of personnel in certain positions, the organization shall assess the nature and extent of the bribery risk in relation to specific transactions, projects, activities, business associates, and personnel falling within those categories.

The ABMS shall include any due diligence necessary to obtain sufficient information to assess the bribery risk. The due diligence shall be updated at a defined frequency, so that changes and new information can be properly taken into account.

The purpose of conducting due diligence on certain transactions, projects, activities, business associates, or personnel is to further evaluate the scope, scale, and nature of the more-than-low bribery risks identified as part of the organization's risk assessment. It also serves

the purpose of acting as an additional, targeted control in the prevention and detection of bribery risk, and informs the organization's decision on whether to postpone, discontinue, or revise those transactions, projects, or relationships with business associates or personnel.

Projects, specific transactions, and activities must be focused upon. The following are factors that the organization may find useful to evaluate:

a. Structure, nature, and complexity (e.g., direct or indirect sale, level of discount, contract award, and tender procedures)

b. Financing and payment arrangements

c. Scope of the organization's engagement and available resources

d. Level of control and visibility

e. Business associates and other third parties involved (including public officials)

f. Links between any parties in point e. above and public officials

g. Competence and qualifications of the parties involved

h. Client's reputation

i. Location

j. Reports in the market or in the press

Business associates are usually a due diligence focus and must include factors which the organization may find useful to evaluate:

> Whether the business associate is a legitimate business entity, as demonstrated by indicators such as corporate registration documents, annual filed accounts, tax identification number, listing on a stock exchange

> Whether the business associate has the qualifications, experience, and resources needed to conduct the business for which it is being contracted

> Whether and to what extent the business associate has an anti-bribery management system in place

> Whether the business associate has a reputation for bribery, fraud, dishonesty, or similar misconduct, or has been investigated, convicted, sanctioned, or debarred for bribery or similar criminal conduct

> The identity of the shareholders (including the ultimate beneficial owner(s)) and top management of the business associate, and whether they have a reputation for bribery, fraud, dishonesty, or similar misconduct

Anti-bribery controls and business associates

In relation to business associates not controlled by the organization for which the bribery risk assessment or due diligence has identified a more-than-low bribery risk, and where anti-bribery controls implemented by the business associates would help mitigate the relevant bribery risk, the organization shall implement procedures as follows:

> The organization shall determine whether the business associate has anti-bribery controls in place which manage the relevant bribery risk.

> Where a business associate does not have anti-bribery controls in place, or it is not possible to verify whether it has them in place:

  • Where practicable, the organization shall require the business associate to implement anti-bribery controls in relation to the relevant transaction, project or activity.

  • Where it is not practicable to require the business associate to implement anti-bribery controls, this shall be a factor taken into account in evaluating the bribery risk of the relationship with this business associate and the way in which the organization manages such risks.

Gifts, hospitality, donations, and similar benefits

Any organization needs to be aware that gifts, hospitality, donations, and other benefits can be perceived by a third party (e.g., a business competitor, the press, a prosecutor, or judge) to be for the purpose of bribery even if neither the giver nor the receiver intended it to be for this purpose.

A useful control mechanism is to avoid as far as possible any gifts, hospitality, donations, and other benefits which could reasonably be perceived by a third party to be for the purpose of bribery.

The benefits referred to could include, for example:

> Gifts, entertainment, and hospitality
> Political or charitable donations
> Client representative or public official travel
> Promotional expenses
> Sponsorship
> Community benefits
> Training
> Club memberships
> Personal favors
> Confidential and privileged information

A robust gifts and hospitality procedure must be implemented by the organization and be designed to:

> Control the extent and frequency of gifts and hospitality by:

  • A total prohibition on all gifts and hospitality; or

  • Permitting gifts and hospitality, but limiting them by reference to such factors as:

    - A maximum expenditure (which may vary according to the location and the type of gift and hospitality)

    - Frequency (relatively small gifts and hospitality can accumulate to a large amount if repeated)

    - Timing (e.g., not during or immediately before or after tender negotiations)

    - Reasonableness (taking account of the location, sector, and seniority of the giver or receiver)

    - Identity of recipient (e.g., those in a position to award contracts or approve permits, certificates, or payments)

    - Reciprocity (no one in the organization can receive a gift or hospitality greater than a value which they are permitted to give.)

    - The legal and regulatory environment

> Require approval in advance for gifts and hospitality above a defined value or frequency by an appropriate manager

> Require gifts and hospitality above a defined value or frequency to be made openly, effectively documented (e.g., in a register or accounts ledger), and supervised

Raising concerns

Raising concerns or implementing a whistleblowers policy is a critical step in changing the culture of any organization on route to ABMS maturity. The organization shall implement procedures which:

> Encourage and enable persons to report in good faith or on the basis of a reasonable belief attempted, suspected, and actual bribery, or any violation of or weakness in the anti-bribery management system, to the anti-bribery compliance function or to appropriate personnel

> Except to the extent required to progress an investigation, require that the organization treats reports confidentially, to protect the identity of the reporter and of others involved or referenced in the report

> Allow anonymous reporting

> Prohibit retaliation, and protect those making reports from retaliation, after they have in good faith, or on the basis of a reasonable belief, raised or reported a concern about attempted, actual, or suspected bribery or violation of the anti-bribery policy or the ABMS

> Enable personnel to receive advice from an appropriate person on what to do if faced with a concern or situation which could involve bribery

Through inductions, training, and awareness programs, the organization shall ensure that all personnel are aware of the reporting procedures and are able to use them, and are aware of their rights and protections under the procedures.

Investigating and dealing with bribery

Appropriate procedures on how to investigate and deal with any issue of bribery, or violation of anti-bribery controls, which is reported, detected, or reasonably suspected, must be developed and implemented. How an organization investigates and deals with a particular issue will depend on the circumstances.

Every situation is different, and the organization's response should be reasonable and proportionate to the circumstances. A report of a major issue of suspected bribery would require a far more urgent, significant, and detailed action than a minor violation of anti-bribery controls. The suggestions below are for guidance only and should not be taken as prescriptive.

The ABCF should preferably be the recipient of any reports of suspected or actual bribery or violation of anti-bribery controls. If the reports go in the first instance to another person, the organization's procedures should require that the report is passed on to the compliance function as soon as possible. In some cases, the compliance function will itself identify a suspicion or violation.

The procedure should determine who has responsibility for deciding how the issue is investigated and dealt with. When any issue is identified, top management or the compliance function (as appropriate) should assess the known facts and potential severity of the issue. If they do not already have sufficient facts on which to decide, they should start an investigation.

The investigation should be carried out by a person who was not involved in the issue. It could be the compliance function, internal audit, another appropriate manager, or an appropriate third party. The person investigating should be given appropriate authority, resources, and access by top management to enable the investigation to be effectively carried out. The person investigating should preferably have had training or prior experience in investigating. The investigation should promptly establish the facts and collect all necessary evidence by, for example:

> Making inquiries to establish the facts

> Collecting all relevant documents and other evidence

> Obtaining witness evidence

> Where possible and reasonable, requesting reports on the issue to be made in writing and signed by the individuals making them

Once the investigation is completed, and/or has sufficient information to be able to make a decision, the organization should implement appropriate follow-up actions. Depending on the circumstances and the severity of the issue, these could include one or more of the following:

> Terminating, withdrawing from, or modifying the organization's involvement in, a project, transaction, or contract

> Repaying or reclaiming any improper benefit obtained

> Disciplining responsible personnel (which, depending on the severity of the issue, could range from a warning for a minor offense to dismissal for a serious offense)

- Reporting the matter to the authorities
- If bribery has occurred, taking action to avoid or deal with any possible consequent legal offenses

4. ANTI-BRIBERY MATURITY ASSESSMENTS

The Anti-Bribery Maturity Model (ABMM) outlines Key Anti-Bribery Indicators (KABI) and activities that comprise a sustainable, repeatable, and mature anti-bribery management system program.

ABMM is not a generic maturity model which one can obtain from the internet, if available. It is a specifically designed model to address the Key Anti-Bribery Indicators (KABI) as required by the organization and its unique environment it operates in.

Taking the unique designed ABMM maturity assessment, organizations benchmark how in line their current anti-bribery management practices are with the KABI.

This provides a clear and understandable road map, with milestones and performance indicators to the organization to be used for the duration of the implementation period. This is in short, the GPS directions of achieving the objectives.

Without the ABMM, most organizations run around, waste time, implement unnecessary structures and processes, and over complicate the ABMS.

As experts in this field, Crest Advisory Africa (CAA) has implemented various ABMSs across the globe due to our speed of implementation and the outcome of years of building and understanding these models.

5. RECOMMENDATIONS

The following are some recommendations on how to create a culture of compliance and have a robust compliance program:

- Contact the experts to conduct an ABMM assessment to determine where you are and where you need to be
- Develop the road map to implement and grow in maturity
- Create the strategy you need to follow to achieve the culture change and to build a robust ABMS
- Build and implement an open, transparent, and integrated training and awareness program to improve the competencies across the organization
- Empower the AB compliance function to conduct a comprehensive AB Risk Assessment

- Take control of a zero tolerance approach regarding gifts, hospitality, donations, and any other benefits. This means to conduct a physical walk through every office and collect, record, and remove all the gifts and any brands from business associates from all the offices.
- Conduct due diligence pertaining to every company found to provide gifts to any person of your company
- Develop and implement a robust whistleblowers policy
- Implement a hotline for anyone to report anonymously, addressing all modes of reporting
- Appoint AB champions in the organization to identify and recognize anything which could raise concerns
- Make the implementation of an ABMS a requirement to all the top 10-20 vendors or at-risk vendors identified during the AB Risk Assessment
- Enforce compliance and be consistent

6. CONCLUSION

Bribery, whether direct or indirect, is a global phenomenon. Any organization that wants to conduct business globally, must make a deliberate, intentional, and conscious decision to continuously improve their global standing.

Through the implementation of a robust ABMS, companies can compete and grow without fear of reputational risk. The benefits outweigh the decision of not implementing an ABMS. Not implementing an ABMS is also a deliberate, intentional, and conscious decision.

Nico Snyman
Founder and CEO of Crest Advisory Africa (Pty) Ltd

in

Nico Snyman is the Founder and Chief Executive Officer (CEO) of Crest Advisory Africa (Pty) Ltd (hereinafter CAA), based in Johannesburg, South Africa. Nico has an MBA, specializing in Total Quality Management (TQM), and is an internationally Certified Management System Auditor with PECB. Nico is also a PECB-certified Senior Lead Auditor for 14 ISO standards.

With over 35 years of experience in various disciplines, Nico has a vast subject matter expertise (SME) base across various industries, from government, corporate, regulators, banks, mines, medical schemes, etc.

He served as a Brigadier in the South African Police Service (SAPS), an Executive on the biggest global project between 2007 and 2011, the Gautrain Project, and as an Executive, was instrumental to the establishment of the Bombela Operating Company (BOC) between 2009 and 2013.

PECB Lead Cloud Security Manager training course

Do you want to support your organization in ensuring security and compliance and minimizing risks within the cloud computing environment?

Complete the training course, take the exam, and GET CERTIFIED!

⟶ CONTACT US

Anti-Bribery Management Systems based on ISO 37001 — Why and How?

✎ BY SERGE BARBEAU

The two most frequently asked questions by clients are "Why should I implement an ABMS?" and "How do I implement an ABMS and get it certified?" This article will answer those very questions!

Why Should I Implement an ABMS in Accordance with the Requirements of ISO 37001?

When approaching us, besides the abovementioned questions, our clients also ask: "What added value does the implementation of the standard bring to my organization?" or "We have a code of ethics and our finances are audited annually by external auditors! We have not been involved in any corruption scandals! So, why implement an ABMS in our organization?"

Having a code of ethics and having the financial results audited are not enough to prevent and detect acts of corruption. Experience shows precisely the opposite!

Several organizations that were involved in corruption scandals had codes of ethics and had their finances regularly audited. However, no corruption risk assessment had been carried out and the controls to ensure compliance with the code of ethics were at best ineffective or at worst nonexistent.

A code of ethics is certainly a key element of sound management in an organization. However, it still needs to be supported by policies, procedures, and ethical and disciplinary processes to prevent corruption and take corrective actions.

As for financial audits, they are mainly used as an aid to take business decisions and to ensure the accuracy of accounting information.

Since the adoption of the ISO 37001 standard by all ISO member countries, several organizations have implemented an ABMS in response to allegations (real or suspected) of corruption by their leaders or representatives.

However, we are noticing a trend on the part of heads of government bodies and businesses that favor the implementation of an ABMS to prevent and detect in a timely fashion behavior that could be interpreted as wrongdoing, corruption, or collusion.

Corruption scandals reported in the media often cause irreparable damage to the organizations associated with them. In addition, social acceptability for business strategies based on cheating, corruption, or collusion is rapidly declining. What once was considered "the way of doing business" is now openly criticized and subject to investigation resulting in significant financial and personal penalties.

How Do I Implement an ABMS and Get It Certified?

The effective and efficient implementation of a management system in an organization is a major challenge, regardless of the nature or the objectives of the management system.

Depending on the context, policymakers will seize an opportunity brought by a crisis or opt for change dictated by the business environment or new regulatory standards. In any case, unlike other types of management systems, an ABMS addresses directly the organizational culture and the behavior of the leaders and representatives of the organization.

The implementation of an ABMS can also be the result of negotiations between the leaders of an organization and the judicial authorities of a country to right the wrongs caused by illegal business practices such as corruption. Regardless of the reasons underlying the implementation of an ABMS, the leaders of the organizations must be willing and ready to answer the questions raised by the project in order to engage all employees, partners, and customers in its success.

Here is the proposed roadmap for the planning, implementation, deployment, and control phases of an ABMS in an organization. The content of this roadmap is based on best practices in project management, interpretation of the requirements of ISO 37001:2016, and experiences of implementing new processes in organizations.

Each organization has its own ways of doing things and unique business processes. It is therefore important to remember that the person in charge of the ABMS implementation project must first take the time to fully understand the structure and functioning of the organization, its managerial culture as well as the context in which this project takes place.

For a successful implementation project, we suggest four (4) phases:

1. **The planning phase** during which the project manager must understand and document the managerial processes of the organization, its partner and customer relationships as well as its business objectives.

2. **The development phase** during which an organizational diagnosis must be carried out in order to assess the gaps between the policies, procedures, and means of control in place in the organization and the requirements of the ISO 37001 standard. A risk assessment must also be carried out in order to identify and assess corruption risk.

3. **The deployment phase** during which the ABMS is operationalized in the organization. This phase can take place over several months during which training and awareness activities will be conducted and monitored.

4. **The control phase** during which the internal audit and the reviews by the anti-bribery compliance function, management, and governance will be carried out. These reviews will result in the adoption of a continuous improvement plan.

Depending on the objectives of the organization's management, **a fifth phase may be added, the certification phase**. During this phase, the top management in collaboration with the anti-bribery compliance function will choose a certification body that has accreditation for ABMS.

Each of the phases briefly described above must be the subject of detailed planning according to best project management practices. All activities must be:

> Listed and grouped into lots (if applicable)

> Linked to each other according to a path that takes into account their hierarchy in the critical path of the project (concomitant activities vs. preliminary activities)

> Recorded in an implementation schedule (Gantt chart or similar tool)

> Monitored and evaluated to ensure compliance with deadlines and expected results

1. Planning Phase

Understanding of the organization

> Describe the organization (mission, objectives, values, business strategies, regulatory history, number of employees, number of sites, material resources, summary of the organization's performance, and previous situations which had negative consequences on its reputation)

> Describe the external environment (strengths, weaknesses, opportunities and threats, direct and indirect competitors, presence of controversies in the industry or business area, etc.)

> Describe the main governance processes (strategic, tactical, and operational)

> Identify the interested parties (donors, shareholders, unions, pressure groups, watchdogs, media, etc.) and their expectations, if applicable

> Describe the legal, regulatory, and contractual obligations (which are related to the prevention of corruption)

Analysis of existing systems

> Describe the management and control systems in place

> Describe the human resources processes (hiring, due diligence, staffing, performance evaluation, promotion)

> Describe the disciplinary processes (analysis of complaints, investigations, decisions)

> Describe the process for reporting concerns and, where applicable, whistleblower protection programs

> Conduct a gap analysis between the management and control processes in place and the requirements of the ISO 37001 standard

Determination of the (initial) scope of application of ABMS

> Describe an initial scope for the implementation of the ABMS

> Validate the description of the proposed scope with management and governance

> Obtain governance commitment (documented decision, allocation of necessary resources)

2. Development Phase

Organization of the project team

> Appoint the person in charge of the implementation project

> Assign the required human, financial, and material resources (offices, ICT)

> Train members of the project team on the requirements of the standard and best anti-bribery practices

> Review the implementation plan, its objectives, and its timeline with the members of the project team

> Assign tasks and deliverables to members of the project team

> Establish a detailed schedule of the stages of the project

> Monitor project activities, timelines, and budgets

> Report on the progress of the project to management and, if applicable, to governance

Risk assessment

> Choose a recognized risk assessment method that corresponds to the particularities of the organization

> Prepare the documents necessary for the risk assessment process (information to participants, assessment grids, meaning of assessment criteria)

> Obtain approval of the results of the risk assessment from management and, where applicable, governance (documented decision)

> Obtain acceptance by management or, if applicable, governance for the list of residual risks (documented decision)

Develop the anti-bribery policy

> Write a policy according to the requirements of the standard (clause 5.2)

> Present the policy to management and, if applicable, to governance

> Obtain approval from management and, if applicable, governance (documented decision)

> Develop an internal and external communication plan to publish the policy (documented plan)

> Evaluate the performance of the publishing strategy according to the objectives set out in the communication plan

Determine the control processes and operational procedures necessary to mitigate medium and high corruption risks

> Facilitate meetings with managers or targeted departments to identify effective control processes and procedures for each of the medium and high risks identified

> Identify performance indicators

> Write the procedures and directives necessary for the implementation of control measures

> Obtain approval for procedures and guidelines from management or, where applicable, governance (documented decision)

> Prepare guides and content of training sessions (if necessary) for managers and users of forms

Establish relevant mechanisms for reporting concerns and protecting whistleblowers

> Determine what means of reporting concerns will be put in place

> Establish analysis and investigation procedures relating to reports

> Prepare a communication and awareness plan regarding the means of communicating concerns to all staff of the organization

> Evaluate the performance of the communication plan

Structure the ABMS

> Establish the roles and responsibilities of management and employees in the operation of the ABMS

> Revise the organizational chart to reflect anti-bribery responsibilities

> Review job descriptions and responsibilities for all relevant hierarchical levels

> Review the performance appraisal process to include responsibilities and tasks related to the ABMS

> Develop supporting documents for changes to the performance appraisal process

3. Deployment Phase

Deploy the ABMS in the organization

> Determine the date of deployment (D-Day)

> Establish the roles and responsibilities of project team members during the deployment phase

> Monitor deployment activities

> Document the activities of the deployment phase (reports, monitoring forms)

> Report the performance of the deployment phase to management and, if applicable, to governance (document decisions, if applicable)

Monitor operational procedures

> Monitor the performance of all the control measures put in place according to the performance indicators of the ABMS

- Financial controls
- Non-financial controls
- Human resource control
- Reasonable due diligence
- Anti-bribery commitments
- Documented information
- Gifts, hospitality, donations, and similar benefits
- Training and awareness
- Management of inadequacies
- Reporting concerns
- Analysis of reports and investigations

> Obtain the reports scheduled for ABMS (daily, weekly, monthly)

> Analyze reports according to procedures and guidelines

> Propose fixes and modifications if necessary

> Write periodic performance reports of the ABMS

> Communicate performance reports to managers according to agreed procedures (dashboards)

> Document the follow-ups and the transmission of reports

4. Control Phase

Internal audit

> Establish the internal audit program

> Create audit tools

> Identify auditors

> Train auditors (if necessary)

> Plan audit activities

> Allocate resources for audit activities

> Audit all ABMS criteria

> Write the audit report

> Write nonconformity reports (if applicable)

> Analyze and correct nonconformities (if applicable)

> Monitor the nonconformities (if applicable)

> Document the audit process

Review by the Anti-bribery Compliance Function

> Document the monitoring procedures, as well as the difficulties encountered

> Record the conclusions of periodic checks and internal audit

> List the reports of concerns and the measures taken (analysis, investigation, decision)

> Describe the observations made and the areas for improvement identified

> Prepare a report for management and, if applicable, governance

> Prepare a continuous improvement plan containing objectives and deadlines

Management review

> Plan with management the presentation of the review report of the Anti-bribery Compliance Function

> Present and comment on the review report

> Obtain approval for the report (documented decision)

> Present the continuous improvement plan

> Obtain approval for the continuous improvement plan (documented decision)

> Implement the continuous improvement plan (if applicable)

Governance review

> Plan with management the presentation of the review report of the Anti-bribery Compliance Function
> Present and comment on the review report
> Obtain approval for the report (documented decision)
> Present the continuous improvement plan
> Obtain approval for the continuous improvement plan (documented decision)
> Implement the continuous improvement plan (if applicable)

All the activities described above require adaptation to the specific internal and external environments of an organization. Depending on the nature of the organization and its operations, it is necessary to review each of the activities indicated and, if necessary, add or subtract from them.

The implementation of the anti-bribery management system based on the requirements of ISO 37001 allows the organizations and its leaders to promote stakeholders, suppliers, and customers confidence and demonstrate to regulatory bodies their commitment to transparent and ethical business processes.
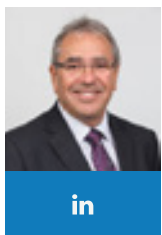
Serge Barbeau
Senior Advisor and Project Director
at Gestion Jean Bourdeau Inc.

in

Serge Barbeau holds a master's degree in public administration from the National School of Public Administration (1992). He also completed studies in communications, labor relations, crisis management, project management, and organizational development. He is a Certified Protection Professional (CPP) from the American Society for Industrial Security (ASIS), a Certified Professional in Critical Infrastructure Protection (PCIP) from the Critical Infrastructure Institute of Canada, and a Certified Port Facility Security Officer (PFSO). Mr. Barbeau was also trained in predictive profiling and is fluently bilingual (French – English).

Mr. Barbeau is a PECB Certified Trainer, a Management System Auditor, an ISO 37001 (Anti-Bribery Management Systems) Lead Implementer and Lead Auditor. Furthermore, Mr. Barbeau is a PECB Certified ISO 18788 (Security Operations Management Systems) Lead Implementer and Lead Auditor.

Enjoyed Reading this Article?

Mr. Barbeau is one of the panelists in our upcoming Anti-Bribery Conference scheduled for May 17-20, 2021. Register for FREE and attend the conference for more insights on related topics.

PECB
Winner of the Best Cybersecurity Education Provider Gold Award

For the third year in a row we have been awarded the Best Cybersecurity Education Provider Gold Award (North America, between 100 – 499 employees) by the Cybersecurity Excellence Award. This award is given to companies who have demonstrated excellence, innovation, and leadership in information security.

We thank all of our partners, trainers, and wide network for the collaborative efforts and support which allows us to continuously provide valuable knowledge, educative content, and best practices through our training courses.

⟶ FIND OUT MORE

A Future-Fit Approach for Selecting Non-Financial Risk Management Technology

BY WILLEM PUNT

The rise of technology in risk management, in particular non-financial risk management, has been accelerating over the last decade. Significant advances in data science, machine learning, and artificial intelligence, as well as increased interest by regulators in how these technologies may be used to drive corporate accountability and good outcomes for customers and markets, have been fueling growth in Regtech innovation.

Generally, these technologies develop faster than the pace of change within business and risk management. As a result, much vaunted technology solutions often do not perform as the marketing brochure promised or are subject to such delays that they are no longer fit for purpose by the time of eventual implementation.

If these technologies are sports cars, the business and risk management systems that they need to serve or integrate with, are often not more than gravel paths. One can think of disparate platforms creating fragmented data environments, very high volumes of poor-quality unstructured data, no data in place, or impractical and competing risk policies and programs. Most often, all these factors act in concert to impede the timely and proper application of technology applications to support risk management.

The risk technology solutions that are relatively simple to implement are, unsurprisingly, less platform or risk program dependent or have been purposely designed to compensate for their expected deficiencies.

Two good examples are:

> Electronic discovery tools that apply increasingly sophisticated machine learning to find relevant documentation among very high volumes of unstructured data, much quicker and more reliably than can be done manually. Apart from now well-established application in legal proceedings, the use of such technology to assist organizations in responding quickly and consistently to growing volumes of day-to-day regulatory requests to produce information can be fruitfully explored.

> Voice analytics applications that leverage existing but otherwise underutilized voice recordings to identify noncompliant market conduct is a growing area. Interestingly, these technologies are also being applied to assess the psychological vulnerability of customers at the point of sale. In an age where concepts such vulnerability and information asymmetry have entered regulatory parlance, having a risk strategy for voice assets is no longer a luxury.

These examples solve important but narrow problems. For risk technology solutions to be more versatile in their application and broader in their benefits, these technologies need improved information architecture environments, especially on largely digitized platforms, and more future-fit non-financial risk management programs.

It is useful to focus on the trends that are shaping non-financial risk management program needs to enable us to determine a must-have set of non-financial risk management technology solutions. By understanding the key trends that are shaping non-financial risk management design – and bribery and corruption specifically – one could evaluate solutions for their ability to assist organizations in non-financial risk management and responding to these trends.

Given the challenges described above, non-financial risk management practice would need to be responsive to a number of key trends.

The evolution of legal design and regulatory obligations

Anti–Bribery and Corruption (ABC) legislation has been leading the way in introducing so called "failure-to-prevent" clauses to legal frameworks. These clauses require regulated entities be able to demonstrate, upon demand, adequate cultural attributes, and control procedures to combat bribery and corruption.

These procedures act as a type of insurance policy that, when well designed and implemented, protects the regulated organization from liability for systemic failures to prevent misconduct. While this concept has its origin as far back as the introduction of the US Federal Sentencing Guidelines for Organizations in 1990, the adoption of this legal feature in the UK Bribery Act (2010) has added momentum to what is essentially a shift of the burden of proof from the regulator to the regulated entity.

When combined with the adoption of deferred prosecution arrangements, the practical effect is a lowering of the burden of proof, and as a result, significant expansion of regulator power to pursue ABC matters. Following the UK example, French bribery and corruption law reform culminated in Sapin II (2017), and contains broadly similar provisions, while proposed foreign bribery reforms in Australia will introduce both a failure-to-prevent provision as well as DPA scheme to the Asia Pacific region.

This trend – of combining failure-to-prevent provisions with DPA arrangements – is set to continue within the global ABC landscape, while it can be reasonably expected that regulators having these instruments at their disposal, will be increasingly inclined to use them. It is also prudent to expect the use of such instruments to expand to legal risk themes other than ABC but sharing similar high legal burdens of proof and major financial, but also significant social consequences, when such risks are not prevented. Bribery and corruption are certainly financial crimes, but often go hand in glove with human and environmental rights abuses.

The evolution of corporate crime and corruption

Academics such as professor Adam Graycar of the Stretton Institute at Adelaide University in Australia, point out that globally organized crime is becoming more sophisticated, and is shifting activities from violent crime to corruption. Corruption pays more than violence.

At the same time, corrupt activities are becoming less individualized, more coordinated among multiple groups, and as a result, increasingly complex in organizations. An example of this phenomenon is state capture. In South Africa, a dedicated commission of inquiry, the Zondo Commission, has been set up to investigate incidences where institutions of state and corrupt private sector businesses have colluded to gain access to the purchase power of those organizations for their illicit gain. The consequence is corruption on a massive scale, abusing institutions with legitimate and other very necessary social mandates while these captured institutions are steadily robbed of their ability to function and deliver on key social mandates such as healthcare, energy production, and potable water provision.

As a result, the distinction between legitimate and illegitimate institutions is becoming more difficult to establish at face value. Jurisdictional risk indicators, often used by risk managers to set in-country risk appetites will need to increase political and institutional intelligence gathering, while organizations will need to make enhancements to their third-party, supply chain, and customer risk analysis programs.

The evolution of community expectations and social obligations

The reputation and business risk impact of corporate misconduct is rising. Broadly termed as community expectations, these expectations encapsulate environmental, social, and governance issues. Importantly, these community expectations are coalescing into social obligations that have the potential to deeply impact organizations while they are developing faster than formal regulatory obligations. This momentum appears to be sustained by a global trust crisis impacting almost all major institutions.

At the heart of the global trust crisis, appears to be a crisis of hopelessness – a deeply held concern among many ordinary citizens that a future characterized by rapid technology changes such as robotics and artificial intelligence, will leave them, and their children vulnerable and financially insecure. As a result, they distrust the institutions they perceive to be at the heart of the changes they fear.

This dynamic is deeply embedded in our modern social fabric and as a result, the distrust feeding the velocity and impact of social obligations is not likely to dissipate anytime soon.

Prudent organizations are responsive to these social obligations. A good example is major financial institutions who are increasingly using their considerable influence in lending and investment to require investees, and to encourage clients, to pursue business

practices that prioritize environmental sustainability and good governance practices that go beyond minimum legal obligations. The same dynamic is causing large global companies to be more willing to openly advocate for specific social justice positions that until recently would have been considered outside of the realm of business to publicly opine on. This generates risks, but also opportunities.

In practice, we are experiencing a convergence between legal and social obligations that makes the business and the risk management landscape increasingly complex and challenging to navigate. As a result, a non-financial risk management strategy that only focuses on legal obligations, and does not deeply consider social obligations

in the context of these statutory duties, will no longer be sufficient to manage serious reputation and business risk.

The rise in the importance of business integrity and an ethical culture

The practical effect of this convergence of legal and social obligations is that it places more demand on organizations to consciously understand their own organizational culture, in particular, how it adopts values and make decisions – its ethics.

Organizations need to take care to understand what these values are, for they may not be the ones in the code of conduct or on the banners in the lobby. Following on this

concept, it is important to understand whether these values are the most appropriate ones, and in turn, how able senior managers are in applying these values to business decisions across many jurisdictions. A key objective of future orientated non-financial risk management would need to be programs of work to enhance the quality of responsible business decision making.

Ethics has often been on sidelines of risk management. It is now moving to the core of non-financial risk management strategy as it becomes a key skill to enable faster, but also more responsible decision-making. Business ethics long understood to be a soft topic, would need to be managed in a hard way – in a deliberate, and a considerate manner.

Another aspect to consider is measurement. There are many valid dimensions to organizational culture and culture assessment. Employee engagement is a common lens, while attitudes to risk management – so called risk culture – is another. These remain useful approaches but would need to

be supplemented with a conscious and deliberate focus on how organizations adopt values when balancing increasingly complex legal and social obligations both competently and consistently, and in a commercially sustainable manner. This is a tough ask and not easily captured in single surveys. However, the data points for such insights often already exists, within existing survey data, but also other data sources. These existing data points need to be interpreted differently, with the factors influencing the quality of decision-making in mind. If one could understand these factors, one may develop culture data that is strongly correlated to latent risk and thus more predictive in nature.

So where does this leave us?

It is clear that non-financial risk management landscape is changing. It is changing because the society is changing. The combination of enhanced legal obligations, increased sophistication of organized crime, and prevalent distrust fueling the velocity, and impact of social obligations, are

placing new demands on our ability to formulate and manage controls, as well as understand and shape organizational culture to propagate ethical business decision-making.

These trends require changes in the skillset of non-financial managers. Persons with a legal background have often dominated this profession, especially in compliance. Yet, in the context of the trends discussed, the non-financial risk professional would increasingly need to show proficiency not only in law and regulation, but also the ability to traverse social, cultural, and technological domains.

Building on the technology point – senior non-financial risk managers would need to consider technology solutions to:

> Enable and demonstrate cultural attributes and adequate control procedures on demand
>   • On the control front, technology needs to support books and records as well as continuous monitoring,
>   • On the culture front, technology may be applied to produce culture data, from existing survey material and other data points to identify, where and by whom decisions are actually made, and the conditions that could impede or enable the likelihood of these decisions being made in a sound and ethically defensible manner.
> Generate meta data and insights to identify increasingly complex and camouflaged organized crime risks
> Identify weak signals of social obligations early on and analyze possible policy impacts before they become greater risks

There are many other areas of application for technology solutions, and I am not suggesting these others do not hold value. Yet, it seems that at the core of your technology suite would need to be solutions that aid responsiveness to the trends discussed above in order for non-financial risk management to remain future-fit.

Let me conclude with a word of caution. Often the greatest challenge with technology is not the technology itself, but knowing what you need to tell it to do. Technology cannot compensate for inadequate policy formulation as much as it cannot compensate for poor governance or a lack of leadership commitment to build and sustain an ethical culture. The greatest risk benefits are derived from business programs aimed at establishing appropriate information architecture across product and service life cycles. This means that often, risk technology solutions offer the best value when they are understood not as separate risk solutions but as enablers to culture programs aimed at fostering good executive decision-making, and business programs that have risk objectives and controls embedded into those business processes. This is initially harder to do, but once established the costs to compliance, the ratio is highly beneficial.

Good compliance is an outcome, not a goal.

Willem Punt
Anti-bribery and Corruption Leader at ANZ Bank

in

Willem is an experienced conduct, culture, and compliance professional. He has 20 years of experience in managing non-financial risk in banking and other industries. He prefers to work at the junction of regulation, business integrity, and technology to design and operate risk solutions that are robust and effective. His focus areas are anti-bribery and corruption, third-party risk management, compliance transformation, and culture risk. He lives in Australia, is married, has three children, and enjoys cycling and writing.

PECB *Store*

FOR YOUR CHOICE AND CONVENIENCE!

Purchase these standards and start building a culture of compliance and anti-bribery in your organization!

ISO 37301:2021

ISO 37301: 2021

Compliance management systems — Requirements with guidance for use

ISO 37001:2016

ISO 37001: 2016

ISO 37001:2016 Anti-bribery management systems — Requirements with guidance for use

🛒 ISO 37301: 2021

🛒 ISO 37001: 2016

DON'T MISS OUR UPCOMING WEBINAR!

Data Privacy, Information Security, and Cybersecurity: What Your Business Needs to Know

May 26 | 3:00 pm CEST

Presenters:

Seyed Hejazi
Director in RSM Canada's Security and Privacy Risk Practice

Hardeep Mehrotara
Manager of IT Security DevSecOps at Coast Capital Federal Credit Union

→ SAVE MY SEAT

PECB WEBiNARS

The Evolving Nature of Financial and Cyber Crime Behavior Detection

✎ BY RICK HAMILTON

The views expressed in this article reflect those of the author and not those of his employer or colleagues.

Money laundering remains a significant global problem as criminals of all stripes have strong financial incentives to innovate and adapt to the changing detection methods employed by financial institutions, law enforcement, and government actors. According to Deloitte's Anti-Money Laundering Preparedness Survey Report 2020, it is estimated that the amount of money laundered in one year is between 2% and 5% of global GDP ($800B – $2.0T). In their December 2018 joint agency statement, the US federal banking agencies issued a statement encouraging innovative industry approaches to addressing Anti-Money Laundering (AML) and Combating the Financing of Terrorism (CFT).

Banks have responded by exploring applications of new technologies to enhance onboarding, due diligence, and transaction monitoring requirements. Some of these innovations have made their way into production and are making a difference in how we, as a collective force, combat the use of the financial system by criminals.

This article, the first of three planned pieces addressing behavior detection (BD) in AML/CFT, fraud, and cybercrime, will focus on how banks align their organizations and processes to better leverage advances in data and behavior classification techniques in their transaction

monitoring programs. In particular, it will explore several ways that the current alignment of these functions could be optimized to improve the responsiveness and effectiveness of BD programs.

At this point, it is important to acknowledge my good fortune to work with many very bright and talented individuals in the AML modeling, investigations, technology, and validation space. The innovations discussed herein are a distillation of the ideas to which I have been exposed and are being offered as a means to foster broader consideration of these topics. Unlike many aspects of the financial services industry, AML is a team sport. We all share a common goal of reducing the exploitation of the financial services industry by criminals. Sharing ideas in this manner is one way to advance our common objective.

Traditional AML Behavior Detection

Broadly speaking, BD has two primary origination points: human and automated. Human detection involves an employee reporting behavior that seems unusual for the customer or circumstances and is critical as the front-line staff of financial institutions are in a unique position to directly observe behaviors that warrant a closer look. Conversely, automated BD reflects the application of screening and classification algorithms that can leverage transaction data, and increasingly non-transaction data, to identify customers and accounts that are exhibiting potentially interesting[1] behavior. Traditionally, BD has been organized around particular types of behaviors, customer types, and products. For example, the simplest forms of BD can consist of grouping customers and products into more homogeneous sets and applying filters that screen for particular behavior types.

For example, a scenario focused on detecting structuring will likely focus on cash deposits over a short period that, in aggregate, exceed currency transaction reporting limits but are comprised of multiple cash deposits under the filing limit. A scenario looking for changes in behavior patterns may compare the total amount of transactions over different periods and classify those with large changes as potentially interesting.

In the main, these types of scenarios can detect activity worthy of investigation. However, due to their simplicity, they are often very inefficient. For example, a low-activity account that was opened by a criminal six months ago for the purpose of laundering proceeds today, will probably be

---

[1] In the context of behavior detection, interesting refers to behavior that is out of the ordinary and cannot be readily explained upon initial review.

flagged by a simple change in behavior scenario when it is used. However, a non-criminal that transfers funds from an account at a brokerage firm to their bank checking account in order to make a college tuition payment may also flag as interesting. This is an example of a "false positive alert" in which a scenario classifies normal behavior as interesting and is an all too common occurrence in some BD scenarios. Even if the scenario is effective at finding a high percentage of all interesting activity, which is not guaranteed, it may do so very inefficiently.

Another option that improves efficiency and effectiveness is the use of decision tree logic to classify behavior. Decision trees expand upon traditional filters by requiring that behaviors meet multiple conditions before being classified as interesting. For example, the aforementioned change in behavior scenario could be improved by requiring both a large change in total transaction amount and transaction counts. In this example, let's say the criminal's account has a relatively small number of total transactions (say 10) but the college parent's account has a typical amount for a family (say 50). Then, for a given dollar increase in total transaction amount, the scenario could be designed to alert only if the transaction count is less than 15. It goes without saying, that many combinations of different behaviors can be tested for their effectiveness at properly classifying activity.

In the model development world, the behaviors noted above are converted into mathematical or logical expressions and are referred to as variables or features. A large number of features increases the chances of finding combinations that are effective at flagging bad actors for investigation while ignoring the average customer. This stems from the fact that diverse features increase the likelihood that one, or a combination of several, will be effective at finding hidden patterns. Feature variety is particularly important when considering the application of machine learning which is particularly well suited to evaluating very large data sets. The importance of this discipline will be examined further later in this article.

The development of decision trees is often a painstaking process in which a model developer uses statistical data and their own experience to find combinations that achieve their effectiveness and efficiency objectives. While this process can be very effective for relatively focused applications, the obvious constraint is the time and effort required for a person to test combinations of features. In contrast, machine learning algorithms enable a model developer to test the effectiveness of huge numbers of different feature combinations in relatively short periods of time. They do this by using optimization

algorithms to test millions of combinations of hundreds of features and in doing so allow a developer to efficiently compare the relative effectiveness of different algorithms. This capability allows for the detection of hidden relationships between features that are effective at isolating the good actors from the bad actors.

A discussion of the best machine learning algorithms for AML/CFT is well beyond the scope of this article but gradient boosted trees and random forests have been shown to be effective.

So two points should be becoming clear at this point. First, features are very critical to BD. They are the "oil" of behavior detection, to re-use a tired analogy. Second, machine learning is very helpful at finding helpful combinations of features. These two facts point to opportunities to re-tool the behavior detection model manufacturing process. In particular, they suggest that we could rearrange the development process and consider moving from episodic scenario development to a more continuous development and updating process.

From Baking the Cake to Food Engineering

In my grandparents' youth, baking involved the use of ingredients that were available at the local store (or could be made at home) and an oven to transform them into a cake.

Today, food engineering involves the careful construction of ingredients tailored to please our palate that are combined using a variety of technologies (ovens, microwaves, etc.) to create an appealing product at a low cost. Furthermore, the process for creating ingredients has evolved to be separate from their specific use. Some food engineers design new ingredients while others find the best combination of those ingredients to make desirable products.

The construction of behavior detection models lends itself to this approach. Rather than the traditional process where a model developer selects from readily available features and perhaps creates a few more for the job at hand, we could transform the feature creation into a continuous process that steadily adds features to a "feature store". BD would likely be strengthened by transforming feature development into a distinct discipline within the AML/CFT behavior detection world.

Specifically, a team comprised of experts in criminal behavior and data science could be established to focus exclusively on the creation and deployment of features. The experts in criminal behavior could be borrowed from the firm's surveillance operations group and tasked with identifying emergent behaviors. They may derive their inspiration from reading the bank's investigative summaries, reading government agency bulletins, or networking with others in the field. Regardless of the

source, this team will be on the lookout for patterns that identify bad or good actors.

The data engineers on the team would work closely with the typology experts to understand the behaviors and convert them into mathematical representations that can be used by model developers. For example, an investigator may determine that accounts flagged as interesting are often one-hop removed from accounts that were previously identified as interesting. The data scientist may then recommend that a graph query be used to tag all accounts that are one hop away on a network graph from all accounts previously flagged as interesting.

In doing so, the team will have converted an experience-based observation into data that can be used in the model development process. Through a continual focus on creating new features, the feature store will be refreshed with new and relevant features that can be used by model developers.

Meanwhile, the model developers would be hard at work creating algorithms that are effective at detecting classifying the good from the not-so-good actors in the portfolio. For example, if the bank decides it needs to implement a scenario to better target a particular form of human trafficking, the model developers would take the lead on developing samples, working with the operations team to identify clear examples of the typology, selected potential features from the feature store, and selecting the best algorithms, conducting hold-out testing, gaining approval from the business, and managing the model validation process.

One Model to Rule Them All?

The advent of machine learning has opened up the possibility of shifting from heavy reliance upon multiple behavior-focused scenarios towards a framework centered around a primary detection engine (PDE). Specifically, since machine learning algorithms are effective at finding subtle relationships between features, there is evidence to support the idea that we can create a PDE that estimates a customer's AML risk, or at least one that a rank-orders the relative AML risk of all customers. Peripheral scenarios would likely be needed for edge cases where a bank lacks sufficient data to train its model to detect a particular activity. However, with appropriate sampling strategies and the thoughtful creation of features, the development of a PDE is a possibility worth exploring.

Two benefits of a PDE include are worth calling out. First, it is easier to update a single machine learning model with new data and features than 10 or 20 scenarios. As will be

discussed later, the process for building a PDE needs to be carefully considered to reap the full benefits of this approach. Second, it enables more efficient use of sampling resources in that the number of samples needed to develop and monitor a single model may be lower than that required to support a collection of scenarios covering the same risks.

The March Towards Continuous Improvement

The process of building new behavior detection models is, by definition, episodic. The business determines that a new layer of detection is required and then directs its experts to tackle the problem. The process of updating existing scenarios follows a similar path in that scenarios are typically revised in response to performance concerns or due to changes in products, customer composition, and geographic exposure. These discrete event-driven changes typically require the development team to adjust each affected model individually. The time required to review samples, fit models, obtain appropriate approvals, and deploy the final application can run to several months or more. There are ways to potentially expedite this, however.

Ongoing Sampling

The first approach is by instituting an ongoing monitoring sampling process. Samples are critical for the development of scenarios as they provide labeled examples of interesting and normal activities that can be used to train a model. They are typically episodic, large, and time-consuming to disposition. In contrast, ongoing monitoring sampling involves using a statistically appropriate method for selecting samples from the population of customers each time the scenarios execute. These samples are then dispositioned by the surveillance operations team along with the regular production alerts generated by the scenarios. The benefits of this process are many.

First, if the operations team dispositions both true alerts and monitoring samples, bias is eliminated because the reviewer does not know that the samples have a lower probability of being uninteresting. Second, as samples are accumulated run by run, a store of samples is available for the developers to leverage. For example, samples can be used to measure the type 2 error of the model while simultaneously providing information to the feature development team, and support model redevelopment.

Finally, as with the feature store, the sample store can be used to rapidly redevelop models. Rather than relying upon large discrete samples to collect data, developers can rely solely upon monitoring samples or, if they need a closer look at certain regions, they can gather smaller development samples. Either way, the development process is accelerated.

Regular Updates and Releases to Models

The move to machine learning can also expedite the updating of models. For example, updating a data set and incorporating features from the firm's feature store to a machine learning model can be done in weeks. With the use of automated machine learning tools, the process can even be expanded to test alternative algorithms to determine which fit the updated data set best. An update frequency of quarterly or semi-annually for certain scenarios, and more importantly for a PDE, can help to keep models up to date with changes in customer behaviors. Of course, all of this requires a well-choreographed set of procedures and clear decision criteria for making a go/no go decision. Heavy reliance upon validation and hold-out testing to evidence model performance, combined with rigorous ongoing testing, is critical to enabling frequent model updates.

Streamlined Documentation

Documentation remains the bane of the developer's existence. However, it is no less vital than the model itself for without it the model does not exist in the eyes of management or regulators.

Given the enormous effort involved in completing documentation for complex models, this process needs to be carefully considered at the same time the development process is re-engineered. Each model change has a documentation cost and therefore must be considered in light of the creative latitude afforded developers. For example, standardized reporting on data quality, model results, approvals, and other evidence will streamline the documentation process.

However, such standardization may also limit the ability of developers to explore alternative approaches. This means finding ways to minimize exceptions to the development process would often be at odds with innovation. However, the movement towards standardization would likely result in a net increase in the velocity with which the overall BD infrastructure can be improved. It also means finding agreement with the model risk management group on the best approach to validating frequently updated models is vital.

Re-defining Validation

Model risk management is a vital part of ensuring that only properly constructed models which align with a firm's risk tolerances are deployed into production. However, model risk management can be a time-consuming process as reviewers need weeks or months, depending upon the model, to review and challenge the submitted documentation. If a bank wishes to continuously update its models, rules need to be established governing the evidence required to demonstrate the soundness of a model. The model developers would need to create standardized development procedures that can be approved ex-ante by the model risk management team.

Model validation teams would need to become comfortable with approving the deployment of models developed using these procedures and relying upon periodic testing to evidence compliance with the procedures. The use of periodic compliance testing with an agreed-upon development process, as opposed to deep dives into each model release, could accelerate the responsiveness of BD programs to changes in coverage needs.

Conclusion

The stakeholders in the fight against money laundering and terrorist financing are exploring ways how best to leverage improvements in data and technology to stay abreast of the ever-changing criminal landscape. Machine learning and changes in model development processes offer the tantalizing promise that institutions will be able to both improve the effectiveness of their BD programs while improving the speed with which they can deploy enhancements.

I am hopeful that this article will stimulate further discussion between the various stakeholders in this fight so that we may collectively find ways to help law enforcement in identifying suspicious activity.

Rick Hamilton
AML Risk Management at PNC

in

Rick is the executive responsible for the models used within AML Risk Management at PNC. In this capacity, he drives the strategic direction of the AML modeling infrastructure and oversees the development and deployment of models, scenarios and analytics spanning transaction monitoring, sanctions screening, customer verification, and data visualization. Rick earned Master of Science in Management Science and MBA degrees from Case Western Reserve University as well as a Bachelors in Economics from the University of Michigan. His professional certifications include the Certified Anti-Money Laundering Specialist (CAMS) and Certified AML and Fraud Practitioner (CAFP). He also completed a certification course in Fintech Innovation: Future Commerce, Information Technology from MIT.

Fernando Cevallos

A Latin American Global Leader in the Fight against Fraud, Bribery, and Corruption

The global pandemic that we are experiencing gives us a clear reminder: The abuse of power for personal benefits can cost citizens their freedom, health, life, and future.

It is a fact that all crises teach us that the progress against fraud, bribery, and corruption can be achieved even in the most adverse conditions. My job is, precisely, to investigate fraud, bribery, and corruption, but also and equally important, to mitigate the effects of those illnesses through anti-fraud frameworks and compliance and anti-bribery programs.

I studied Economics in Ecuador, did my MBA in Brazil, and obtained several certifications in the USA and Canada. Since 2005, I have been living and working in four continents, conducting global cross-border and complex forensic investigations and compliance projects. For the last eight years, I have resided in Mexico City where I founded, and am the CEO of a global consulting firm, F&C Consulting Group. In addition, I co-founded and coordinate international academic programs in ethics, compliance, and anti-corruption. I also teach anti-bribery and anti-fraud subjects at postgraduate levels, professional certifications, and master's levels at universities in Mexico and Brazil.

I have 22 years of international experience and I am a citizen of the world. I was born and raised in Ecuador and for the last 17 years I have lived, worked, and led cross-border projects in and from six countries, including Ecuador itself, the United States, Switzerland, Brazil, Argentina, and Mexico. All my projects have been carried out mainly in Latin America, the United States, Canada, Europe, Asia, and the Middle East.

Here is another fact: My passion for integrity and ethics coupled with my enthusiasm for forensic investigations led me to create, in 2016, a consulting firm, a strong team that put together pieces of a puzzle and identified and managed risks to build robust compliance programs and IT governance.

The investigations consist of reconstructing a story (as we have seen in police series) supported by facts obtained through documentation (accounting records, physical and electronic), e-Discovery, background search, data analytics, among others.

"We detect purposed or negligent errors or corrupt acts that disadvantaged or exposed companies to potential fines and penalties or to the violations of the code of conduct and the internal policies or procedures. There we find all the facts that could be considered a theft, fraud, financial or white-collar crime. It is fascinating because it takes time, methodical review, and analysis of documents, background

search, interviews with various people, confrontations, and then… the puzzle is assembled or could lead to other issues, but most importantly, it will help to improve the compliance program and/or the internal control framework. The same investigation methodology or approach will apply for allegations related to discrimination, sexual or labor harassment, as well."

First Steps: Opportunity Is Born From Crisis

My story begins 22 years ago, in 1999, after graduating from Economics and when Ecuador was going through its financial crash.

I had finished my university studies and finding a job was not easy. My plans were to travel to the United States to seek for opportunities. Suddenly, in April 1999, the opportunity itself came from a renowned international consulting firm in Ecuador, and there I had my first contact with forensic investigations, which marked my career and therefore I began my path into the forensic investigations and compliance worlds.

Due to the economic crisis in my country, there were several events related to fraud and breaches of trust, and one of them took place in the consultancy of which I was part of.

My very first case, in 1999, was a fraud investigation matter in Ecuador, which was related to a misappropriation of assets and a non-disclosed conflict of interest. This event revealed that the company (a United States subsidiary) lacked controls and oversight. The investigation objective was to find evidence to file criminal charges and apply the appropriate internal sanctions. For me, it was an emblematic investigation and in that precise moment, I fell in love with this profession and started my passion to get specialized and trained in forensic investigations of potential wrong-doings or noncompliance or criminal acts that arose, where companies needed to implement a remediation plan or improve their internal controls.

In addition, during that time, the firm required personnel to clarify the case and as I was the only one speaking fluent English, I had the opportunity to assume a key role in this case.

After this challenging first project, I decided to look for an even more defiant and greater added value job, which would allow me to broaden my panorama on the methodologies used in organizations. This is when I joined the largest glass manufacturer in the world (with global headquarters at Perrysburg, Ohio), in the area of Treasury and Financial Planning. During this experience, I learned a lot about manufacturing procedures and client collection, accounts payable, cash management, and other financial instruments. This was a great professional experience that helped me to better understand the clients' language and allowed me to be closer to fully understand their needs on a global level.

Finally, in this company, I implemented a securitization program in Europe, dealing with multiple financial institutions and increasing the effectiveness of the collection process by building a robust business relationship with clients.

Unraveling a Great Challenge

I soon became one of the pioneers in the development of the Brazilian Anti-Corruption Law together with a great community and friends from Brazil – very sharp professionals and leaders in this field. I was invited by leaders of the Sao Paulo Bar Association to comment on the Brazilian anti-corruption project during its development. It was an awesome journey and experience.

Various investigations of corporate crimes have passed through me, and one that represented a great challenge was the Car Wash ("Lava Jato") case in its early stages, prior to moving to Mexico; the scandal that uncovered corruption in Brazil in 2014, considered by the Police and Justice of that country as one of the largest corruption investigations in Latin America.

On other matters, I had managed and led teams and projects as a forensic advisor for various international law firms, including US regulators, cases of fraud and corruption investigations, mergers and acquisitions transactions, follow-up reviews, and monitoring of compliance programs.

After all these experiences, I believe that I found the keys to the passion of my professional journey: my perseverance, my nature as an inquisitive person in all professional tasks, and of course, my ability to connect very well with the people I work with around the world.

Creating Knowledge

In 2011 in Brazil, I co-founded of the FIA Master's Degree in Compliance and Fraud Risk Management, the business school of the University of Sao Paulo.

Since 2016, I have been the Academic Coordinator and Founder of the graduate program in Ethics and International Compliance at Tecnológico de Monterrey University.

Additionally, in this same year, I co-founded the Mexican Association of Ethics and Compliance Professionals (AMPEC, for its Spanish acronym), of which I am currently the President of.

I am also the Lead Editor of "Compliance Urbano", a Spanish blog specialized in Forensic Investigations and Compliance for Latin America telling stories in a simple and realistic way.

I am also an opinion leader and an international speaker and teacher in various Ethics and Compliance programs in Latin America and educational institutes in the Middle East.

ISO 37001 and the Governance Standards

Between 2014 and 2016, I was appointed by the global leadership to be the Global Coordinator of the Communications Committee at the International ISO 37001 Group, aligning a consistent message about the advantages and the benefits of this standard; a situation that led me (since October 2016) to start advising on this standard. The outcome of this standard was a great team effort of 80+ professionals around the world, countries, and government institutions.

During the last years, I have become one of the global opinion leaders on ISO 37001, writing and giving interviews in different digital and print media such as ISOFocus magazine, The Wall Street Journal, CNA Broadcast Asia, CNN Spanish, LEC Brazil, América Economía, FCPA Blog, Líderes, PECB events, and in sessions on the regulation with senior officials of the Singaporean government, among others.

I have been working extensively in the development of other standards, such as ISO 37301 (Compliance) which will replace ISO 19600. We have been following closely the development of ISO 37000 (Governance) and do have extensive experience in ISO 31000. This is part of our portfolio with PECB.

F&C Consulting Group

More than being part of a team, I always wanted to form one. This is where one of my great successes and passions arises: F&C Consulting Group, a global consulting firm that was born in the heart of Latin America, specialized in emerging markets creating and strengthening the culture of integrity and security. A team with an international presence, committed and passionate about caring for and cultivating the reputation of our clients, with the objective of leaving a legacy that transcends in society and its organizations.

With headquarters in Mexico and operations in the United States, Colombia, Ecuador, Brazil, Spain, and Hong Kong, we achieved to be one of the international leaders and experts in forensic investigations, compliance, risk management, and control systems – ISO 37001 (Anti-bribery), ISO 37301 (Compliance), and ISO/IEC 27001 (Information Security).

Partnership with PECB

I am proud of my relationship and partnership with PECB, which began in 2017. However, our professional experience in ISO 37001 started in 2014, as a member of the Mexican Committee, leading the global Communication Committee.

I really trust that the partnership with PECB is a successful strategic directive and it will help us to develop more and more certification trainings, allowing us the advisory or support to organizations in the development of the prevention and implementation mechanisms to fight against bribery and corruption.

As part of our partnership, we can deliver trainings throughout Latin America, Spain, Portugal, and recently in the United States and the Asia Pacific. Exciting times!

Gracias. Thank you.

My entire gratitude goes to all the people around the world who have supported me along my professional path, people who taught me and inspired me to keep walking in this journey. The team, my partners, and consultants that believe in this vision that turned into their passion – this dream that became a reality.

My commitment and promise is that I will continue working with passion and dedication, and will inspire the next generations, my team, our clients, and my wife and daughters, my engines. I am on-board with this amazing challenge, but let's commit and unite efforts to keep fighting against fraud, bribery, and corruption.

THE PECB ANTI-BRIBERY 2021 VIRTUAL CONFERENCE IS APPROACHING!

MAY 17-20, 2021

Don't miss out on the opportunity to hear from more than 30 industry professionals about different topics on anti-bribery and COVID-19, blockchain, artificial intelligence, whistleblowing, and more.

The sessions will be delivered in three languages, English, French, and Spanish. The first three ones will start on May 17 at 3:00 PM CEST.

For further information, please check the conference program or contact us at events@pecb.com

PECB ANTI-BRIBERY 2021 CONFERENCE

⟶ **REGISTER NOW FOR FREE**

Cryptocurrency and Anti-Money Laundering Compliance

✎ **BY BRENT BARKER**

This article presents an overview of anti–money laundering as applied to cryptocurrency. Cryptocurrency is young and efforts to adapt and apply the rules banks and financial institutions follow are still in the early stages.

Criminals are early adaptors of new technology. They excel at finding ways to use the latest technology to commit new crimes and to improve old crimes. This has been true for cryptocurrency, including cryptocurrency money laundering.

What is Money Laundering and Anti-Money Laundering?

Money laundering, in one form or another, has been around for centuries. Many attribute the term "money laundering" to Al Capone, who used laundromats as a way to hide the cash from drug smuggling, prostitution, and tax evasion.

The [Money Laundering Control Act](#) of 1986 first made money laundering a federal crime in the United States. This act defines money laundering as any attempt to conduct a financial transaction which involves the proceeds of unlawful activity while knowing that the transaction is designed to conceal or disguise the origin of the proceeds.

Money laundering provides fuel for criminals, terrorists, and corrupt governments to operate and expand their illegal activities. Money laundering is used for "cleaning" the proceeds of drug activity, human trafficking, ransomware payments, and many more crimes. However, money laundering is used for more than crime. Money laundering is a threat to national and international security. Laundered funds are used for terrorist attacks, to fund nuclear proliferation, and to avoid international sanctions.

According to a 2009 report by the [United Nations Office on Drugs and Crime](#), criminals launder around $1.6 trillion a year, or 2.7% of global GDP. The report suggests that the level of global seizure of money laundered funds is low. It estimates that less than 1% of laundered proceeds of crime are seized.

Anti-Money Laundering (AML) is the process of detecting and disrupting money laundering and terrorism funding activities. Two laws are the foundation of the US efforts to combat money laundering. The first is the Bank Secrecy Act of 1970 (BSA). The BSA required banks and financial institutions to cooperate in detecting and reporting money laundering. The second is the Patriot Act of 2001. The Patriot Act added countering the funding of terrorism (CFT) to US anti-money laundering laws and regulations.

On the international level, the Financial Action Task Force (FATF) was established in 1989 by the Group of Seven (G-7) countries to develop measures to combat money laundering. The FATF expanded its mandate to include combating terrorist financing in 2001 and added countering the financing of weapons of mass destruction in 2012.

The objectives of the FATF are to set standards and promote measures for combating money laundering, terrorist financing, and other threats to the international financial system. Thirty-seven countries and two regional organizations are members. Today, the FATF is a cornerstone in the international fight against money laundering and terrorist financing.

Cryptocurrency and Cryptocurrency Anti-Money Laundering Laws

Cryptocurrency started 11 years ago with Bitcoin. On October 31, 2008, a paper entitled "Bitcoin – A Peer to Peer Electronic Cash System" was posted online. On January 9, 2009, the first Bitcoins were released. Today, there are over 4,600 different cryptocurrencies. Only 96 are worth more than $1 billion and only 17 individually are worth $10 billion or more.

Bitcoin remains the largest of the cryptocurrencies, making up to 58% of the value of all cryptocurrencies. On April 13, 2021, one Bitcoin reached a new high of $ 64,829. The total market value of all cryptocurrencies has reached over $2 trillion with Bitcoin making up over $1 trillion of that.

The public perception linking cryptocurrency and crime began with Silk Road in 2011. Silk Road was the world's largest online black-market website. You could buy illegal drugs, fake documents, and even hire a hitman or computer hacker. Silk Road was also used to launder hundreds of millions of dollars in criminal proceeds. Bitcoins were the only currency accepted. In 2013, the FBI shut down the website and arrested the site's founder.

As the legitimate use and price of cryptocurrencies have grown, so has cryptocurrency crime. The company CipherTrace produces an annual Cryptocurrency Crime and Anti-Money Laundering Report. The 2020 report shows that cryptocurrency thefts, hacks, and frauds reached $1.9 billion — the second-highest annual crimes total recorded. The only year higher was 2019, because of a massive Ponzi scheme involving the cryptocurrency exchange PlusToken, which stole $2.9 billion in a scam.

In 2014, the Financial Crimes Enforcement Network (FinCEN) designated cryptocurrency exchanges as a money service business (MSB). In 2019, FinCEN, the Commodity Futures Trading Commission (CFTC) and the Securities and Exchange Commission (SEC) issued a joint statement that made cryptocurrency subject to the Bank Secrecy Act. This made cryptocurrency exchanges subject to all federal anti-money laundering regulations enforced by FinCEN.

The FATF issued its first report on anti-money laundering and countering terrorism financing risks of virtual currencies (cryptocurrencies) in 2014. Now the FATF issues global, binding standards to prevent money laundering with virtual currencies. In 2020, the FATF issued a review of revised standards on virtual currencies and virtual asset service providers (VASP) or cryptocurrency exchanges.

Private Company Cryptocurrency Investigations

One unusual aspect of cryptocurrency anti-money laundering efforts is the role played by private companies in assisting law enforcement investigations and regulatory compliance. Some of the leading companies are Chainalysis, Elliptic, and CipherTrace which play a key role in tracking and tracing cryptocurrency transactions in money laundering investigations. The companies also assist financial institutions with anti-money laundering laws and regulations compliance.

The Future of Cryptocurrency Anti-Money Laundering Compliance

Recent efforts to strengthen cryptocurrency compliance with anti-money laundering include:

Anti-Money Laundering Act of 2020

On January 1, 2021, the US National Defense Authorization Act for Fiscal Year 2021 (NDAA) became law. Within the NDAA is the Anti-Money Laundering Act of 2020 (AMLA), which introduces substantial reforms to US anti-money laundering and counter-terrorism financing laws. The AMLA is the most significant anti-money laundering law since the 2001 PATRIOT Act.

FinCEN has long held that cryptocurrency exchanges are subject to FinCEN's regulations. The AMLA codifies FinCEN's legal authority and expands its regulatory power. The definition of BSA for financial institution now includes entities engaged in the exchange or transmission of "value that substitutes for currency".

Department of Justice Cryptocurrency Enforcement Framework

In October 2020, the Department of Justice Cyber Digital Task Force released the Cryptocurrency Enforcement Framework. The report identifies the types of illegal uses of cryptocurrencies, the existing tools federal law enforcement has to address cryptocurrency crimes, and how the department, and other federal and state agencies can do more to fight cryptocurrency crime. The report states that criminals are increasingly using cryptocurrency to launder criminal proceeds.

Many of the laws being used to prosecute cryptocurrency crime are laws that currently exist such as mail fraud, securities fraud, and computer intrusion. Two areas of concern raised by the Justice Department Framework were the increasing use of untraceable cryptocurrencies and efforts to obscure transactions such as mixing and tumbling.

The report indicates that the Justice Department will take aggressive action in the future. The report recognizes the "breathtaking possibilities" of cryptocurrencies and recommends the Justice Department focus on efforts to prevent their illegal use rather than focus on prohibiting cryptocurrencies.

The Travel Rule

In 1996, FinCEN issued new rules requiring all US financial institutions to pass on certain identification information to the next financial institution as part of certain funds transactions. This became known as the "Travel Rule". In 2011, FinCEN stated that cryptocurrency exchanges must comply with the "Travel Rule".

In June 2019, FATF published a guidance requiring virtual asset service providers (VASPs) to provide identification information during virtual currency transactions. It is called the FATF Travel Rule because it mimics the US FinCEN Travel Rule.

In June 2020, the FATF conducted a 12-month review of the implementation of the new guidance. FATF decided to extend the preparation period to June 2021 and gave VASPs more time to comply with the Travel Rule. By this time, it expects all member nations to have implemented the new requirement. A review in 2021 will examine whether further updates to the FATF Standards are necessary.

FinCEN Proposed Rulemaking

In December 2020, the outgoing Trump administration announced a last-minute Notice of Proposed Rulemaking (NPRM) which would create new requirements for financial services firms to record the identities of individual cryptocurrency holders conducting transactions. Normally, such rules undergo a lengthy public process involving months of feedback and revisions. However, when FinCEN published the rule on December 18, 2020, it allowed only 15 days for comments.

The move generated over 65,000 negative comments including companies like Fidelity and Square. The US Chamber of Commerce and the Electronic Frontier Foundation both came out against the rule.

On January 14, 2021, the Treasury Department extended the comment period to the end of March, leaving the matter to the Biden administration. On January 26, 2021, FinCEN announced a new 60-day period for comments.

Final Thoughts

Cryptocurrencies have many benefits. They can make payments easier, faster, and cheaper. Cryptocurrencies can provide alternative methods for those without access to regular financial institutions.

The mainstream adoption of cryptocurrency is growing. The Office of the Comptroller of the Currency has issued guidelines to banks on how they can provide cryptocurrency services. Visa announced it would develop a cryptocurrency business and allow the settlement of cryptocurrencies on its network. PayPal users in the US can buy, sell, and hold selected cryptocurrencies directly in their accounts. Several countries are exploring a national Central Bank Digital Currency. China is already experimenting with digital Yuan.

The nature of cryptocurrency crime has changed since it was first used on Silk Road. Today, cryptocurrency crime includes the use of cryptocurrency in other crimes, the theft of cryptocurrency, and their use to launder criminal proceeds.

Money launderers have historically outpaced efforts by regulators and law-enforcement to apply anti-money laundering regulations. Many of the future challenges to cryptocurrency money laundering involve the ways in which cryptocurrency transactions can be hidden or disguised. In the early days of Silk Road many believed that Bitcoin was anonymous. It is not. But now there are cryptocurrencies designed to be untraceable called privacy coins. There are an estimated 79 privacy coins cryptocurrencies.

There are also mixing or tumbling services that can hide the trail of your cryptocurrencies. They break the currency into different parts and mix them with other client's cryptocurrencies. Some have a reserve of "clean coins" that they use to mix in with client coins. No log of the mixing is kept.

How can the US and the international community strengthen cryptocurrency anti-money laundering and countering financing of terrorism compliance? They must strengthen regulatory oversight of cryptocurrencies, exchanges, and transactions. This includes an increased focus on criminal investigation of cryptocurrency money laundering both by itself and as a part of other crimes.

The US, the international community, and FATF must continue to create strong laws and regulations, conduct more regulatory enforcement and criminal prosecutions, and prepare to counter increasingly creative methods of cryptocurrency money laundering. Increased international cooperation is essential. Cryptocurrency money laundering is most often international; it rarely takes place in a single country. Nations must work together both to prevent and prosecute these crimes.

It is essential that governments and the FATF continue to modernize regulations to meet new challenges. They must also expand international collaboration and devote more resources to regulatory and criminal enforcement. Trust of cryptocurrencies will increase as strong regulation and enforcement delineate largescale legitimate use from illegal use.

Some believe that this increased oversight undercuts the original intent of cryptocurrencies to be free of banks and government control. However, for cryptocurrency to expand and flourish legitimately, such oversight is essential.

Brent Barker
Cryptocurrency and Blockchain Security Expert at Barker Global Security

in

Brent Barker is a blockchain security advocate with over 30 years of security experience with the US Army, US Department of State, University of Washington, and as a private consultant. As a Diplomatic Security Service Special Agent, he served at US Embassies and Consulates around the world and as the State Department Liaison to the US Marshals Service. He established the University of Washington's international travel security program.

He worked with the World Economic Forum Travel Initiative Working Group to shape the future of security in travel using of blockchain. He is a member of the ASIS ad-hoc group reviewing the International Organization of Standards (ISO) draft standard for Travel Risk Management (ISO 31030). His focus is on blockchain security. His goal is to educate the security industry about the importance of blockchain and work for international standards, regulations, and laws for blockchain.

LEARNING LIKE ON VACATION WITH CARMAO AND PECB TRAINING COURSES

⦿ Limburg an der Lahn

Certification and continuous training is not only an option in many industries and business sectors but also a requirement by standards and regulations for certain industries. Together with PECB, CARMAO GmbH offers qualifications and further training for specialists and managers. These can be booked – depending on demand and current situation – as online training courses as well as on-site events. When traveling and on-site activities are allowed again, a visit to CARMAO in Limburg an der Lahn with its numerous sights and idyllic surroundings is a good idea.

Walderdorffer Hof Palace

The COVID-19 pandemic has put many companies in a difficult or uncertain position. It is high time for companies to prepare systematically for current and future negative influences and to position themselves resiliently. To maintain the future viability of the company, it is advisable to strengthen its "immune system" in the long term through organizational resilience measures. This also includes employee development.

Ulrich Heun, Managing Director of CARMAO GmbH (specialist for corporate resilience), explains:

"For companies and employees, the priority is to be able to react flexibly to constant change and to contribute to change themselves. On the company side, it is advantageous to anticipate certain events and plan for contingencies. Likewise, employees should be proactive. Lifelong learning paves the way to being up to date, reacting to new challenges, and achieving mental flexibility. To ensure this, CARMAO offers a wide range of training courses in this sector."

In the area of certifiable trainings, CARMAO cooperates with the PECB. As an authorized Gold Partner of PECB, CARMAO's goal is to provide its customers with a high, globally uniform standard of education. For this purpose, CARMAO has special trainings, qualifications, and corresponding seminars in its portfolio.

As is well known, learning is even better in beautiful surroundings. Participants in the training courses offered by CARMAO and PECB can therefore travel to CARMAO in the idyllic Limburg an der Lahn, hopefully once the pandemic is over. In doing so, they can ideally combine learning and leisure time on-site in Limburg. CARMAO GmbH is based in the historic Walderdorffer Hof Palace, a medieval building from the turn of the late Renaissance and early Baroque periods. The historic building, which is more than 356 years old, became the property of a foundation in 1989 and was thoroughly renovated and modernized. The Stadtpalais (City or Town Palace) is located in the middle of Limburg's picturesque old town and skillfully spans the arc from past to modern.

Middle Ages Meet Modern Times in Limburg an der Lahn

Limburg an der Lahn is not only suitable as a place of exchange, it is also a source of recreation. The detailed renovated half-timbered houses and picturesque alleys convey medieval charm. Many sights around the historic city center, as well as a picturesque landscape along the Lahn invite visitors to walks, explorations, and hikes.

The Limburg Cathedral and the Limburg Castle perch on the Domberg (Cathedral Hill). Visitors can enjoy a view of the entire city from here. The castle has a history of more than 1000 years and once served to secure the roads and monitor comings and goings on the river Lahn. Limburg Cathedral is a three-nave basilica that combines late Romanesque and early Gothic elements. The magnificent cathedral has seven towers, which are associated with a variety of symbolism and are unique in all of Germany.

The number 7 plays a significant role in another sight. The listed "House of the Seven Vices" in the old town of Limburg dates from the 16th century and is adorned with numerous ornate carvings, which are interpreted as the seven biblical vices. The Werner-Senger-Haus is also one of the oldest preserved buildings in the old town of Limburg. The Gothic half-timbered house from the 13th century served for centuries as the seat of wealthy Limburg merchants. In 1802, the notorious local thief called Schinderhannes was arrested here. Even though the vaulted chamber, including the prison, is well preserved, today the house offers guests and visitors primarily epicurean delights.

Another architectural jewel in Limburg's old town is also an excellent place to dine. The newly renovated "Weinhaus Schulte" has been in existence since 1836 and is also open to guests from near and far for overnight stays. The "Tafelspitz" is another popular address for lovers of good food and focuses on traditional German and down-to-earth Alpine cuisine. It is a popular overnight destination for business travelers and cyclists too. In the middle of Limburg's old town is the original Italian Ristorante di famiglia "Don Camillo", which offers Mediterranean specialties with fresh herbs in a cozy atmosphere.

The historic Old Lahn Bridge represents a particularly popular destination for day visitors and tourists. In the Middle Ages, the "Via Publica" used the impressive arched bridge to cross the Lahn. First from Cologne to Frankfurt, later from Siegen to Wiesbaden. Today, the Old Lahn Bridge is no longer used for any long-distance road.

Limburg is ideally located for seminar participants due to its ICE (High-speed train) stop, the connection to the A3 motorway, as well as the proximity to Frankfurt airport and Cologne airport.

Where to Stay

Limburg is also worth an overnight stay. We are presenting here four main places where you can stay.

The Limburg Cathedral

Old Lahn Bridge

The historic **Hotel Nassauer Hof** is located at the river Lahn. The hotel is centrally located in the historic old town and has stylishly furnished rooms with all amenities for a relaxing stay.

A perfect location for city travelers is also the **Vienna House**. It is just a few minutes' walk to the idyllic banks of the Lahn, the train station, and the cathedral. The hotel has clean and nicely decorated rooms, fresh and delicious breakfast, and super friendly staff.

The 4-star **Dom Hotel** is located in a historic building from the 19th century. Located in the old center of Limburg, this hotel has stylish, comfortable, and well-maintained rooms. The breakfast, service, and helpful staff will make your stay even better. If you are interested in booking any tours, their staff will be happy to assist. Thanks to its excellent location, the important sights can be easily reached on foot from the Dom Hotel Limburg.

Hotel Amts-Apotheke has a very convenient location at the heart of old town; around a 5-minute walk from the Central Station of Limburg. Stylish and elegant rooms, delicious breakfast, and its friendly staff will make your stay a fantastic experience.

Continuously Implementing Further Training

In the stunning environment of Limburg an der Lahn or via online training courses, trainees can acquire knowledge in a pleasant way. The PECB training courses offered by CARMAO focus on sustainability. With digitalization and globalization, the half-life of learned knowledge and processes is becoming shorter and shorter in many industries. At the same time, security requirements, for example, are constantly increasing and changing, and the need for expert knowledge is growing as a result.

In order to implement meaningful corporate resilience with individual components, continuous training is an important lever for companies. Employees should therefore be sensitized, qualified, and continuously trained for their tasks in areas such as information security, compliance, business continuity, risk management, and service management.

CARMAO offers training and consulting services in the area of information security, business continuity management, and organizational resilience. The extensive portfolio includes, for example, special training courses on individual management systems.

One important topic in the training portfolio is information security. Corresponding strategies no longer stop at national borders but are often controlled centrally in internationally oriented companies. In order to meet the requirement of a globally uniform educational standard, CARMAO has continuously expanded its cooperation with PECB for its training services.

The PECB training courses are tailored to individual needs and include the latest standards, innovative technologies, and practical methods. As a partner, CARMAO offers those training courses for specialists and managers – both as on-site training courses and online. During the COVID-19 phase, CARMAO adapted the certification modules methodically and didactically to the changed requirements and permanently expanded the training options through flexible, digitally supported learning forms. In this way, the PECB training courses offered by CARMAO equip individuals with knowledge and skills that they can use to help companies in implementing sustainable risk management systems and the continuous development of organizational resilience, even in the pandemic era. This is particularly important in times of crisis. And after the Corona measures have been relaxed, learning and leisure can be meaningfully combined on-site in the beautiful Limburg an der Lahn. Continuing education is worth the trip.
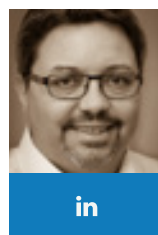
Ulrich Heun
Founder and Managing Partner at CARMAO GmbH

in

Ulrich Heun is the founder and managing partner of CARMAO GmbH, founded in 2003, and a proven specialist in the field of organizational resilience. In addition to consulting on topics in the area of information security management systems (ISMS), their extension to data protection (ISO/IEC 27701), risk management, business continuity management (BCM) as well as data protection management and BSI IT-Grundschutz, he focuses on the conceptual development of CARMAO's CHARISMA Resilience Management Framework. In addition, he is active as honorary chairman of the CISO Alliance e.V.. Ulrich Heun is a PECB Certified ISO/IEC 27001 Lead Implementer, PECB Certified ISO/IEC 27005 Lead Risk Manager, PECB Certified ISO 22316 Foundation, PECB Certified Cloud Security Manager, and a PECB Certified Trainer.

Happy World Book Day
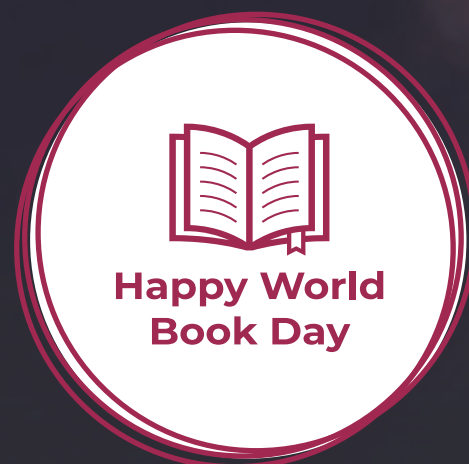
Best Anti-Bribery and Compliance Books to Read in 2021

Different factors such as legal and regulatory requirements and reputational risks have driven organizations to put in place systems to prevent, detect, and respond to corruption risks. The adoption of anti-bribery compliance programs helps organizations prevent any type of corruption and stay alert if someone from the company will be involved in illegal practices. It is important to highlight that the quality of governance is critical to tackling corruption.

For corruption and compliance professionals, C-Executives, or anyone who wants to gain a better understanding of the industry as well as advance their practice, here are some great reads about anti-bribery and compliance.

Anti Bribery Management System A Complete Guide (2020 Edition)
by Gerardus Blokdyk

This is a great guide to Anti-Bribery Management Systems from Gerardus Blokdyk, which makes sure that all fundamentals are covered from each angle. The guide also contains practical tools for self-assessment and outlines the benefits that organizations can gain from the implementation of an ABMS based on ISO 37001. When you purchase this book you will also receive additional valuable content such as the Self-Assessment Excel Dashboard (an example of a filled dashboard to give you an idea of how it works), as well as checklists, templates, and more. In addition, you will gain answers to a lot of questions related to the consequences of bribery, how to make sure that Anti-Bribery Management System outcome will be in place, how to successfully organize ABMS tasks so that outcomes are achieved, etc.

Bribery and Corruption in Weak Institutional Environments: Connecting the Dots from a Comparative Perspective
by Shaomin Li

A representation of twenty years of research and observations, using a comparative method, the author explains why in states with weak institutions corruption flourishes. The analysis by the author covers the impact of bribery and corruption in different environments such as political, social, and business. Moreover, it explains why despite efforts, corruption is still widespread. This book is a must-read for those who want to gain insight into corruption and bribery characteristics and understand the corruption and its impact on economic activities.

Crisis of Conscience: Whistleblowing in an Age of Fraud
by Tom Mueller
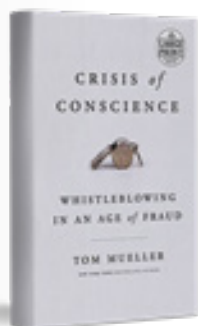
Whistleblowing remains a crucial part of maintaining order and carrying out values. This book is a great read about whistleblowing, and the author does a great job in explaining why whistleblowing is vital for protection against unlawful activity and the risks associated with it. Through human stories and interviews with more than two hundred people and many lawyers and experts, the author explains whistleblowing cases in different areas.

These cases involve money laundering, fraud, theft, tax evasion, and other violations. In addition, it explains what inspires some to speak out and risk relationships, reputation, and more, while others remain silent. A very relevant and informative read!

Compliance Management: A How-to Guide for Executives, Lawyers, and Other Compliance Professionals
by Nitish Singh and Thomas Bussen

One of the ways to improve productivity and lower business risks is by creating an effective compliance program. This book shows the crucial factors required to build such a program.

In the first part of the book, the authors present general guidelines for creating or improving internal compliance and ethics programs. Whereas, in the second part of the book the authors present an outline of relevant laws as well as best practices of these regulations. This book will help you create a new compliance program or improve the existing one.

If you want to get familiarized with business principles and basics of compliance, this book will be a very useful source. It should be read not only by professionals in the compliance industry but as well by business professionals from different backgrounds.

PECB CMMC FOUNDATIONS TRAINING COURSE

Stay ahead of the game! Gain the PECB CMMC Foundations Credential!

If you are interested in becoming familiar with the fundamental concepts and principles of the CMMC model, this training course is the one for you.

The PECB CMMC Foundations training course is a starting point for you to understand the structure of the CMMC model including levels, domains, capabilities, processes, and practices. You can help your organization prepare to implement and manage the requirements of the CMMC model, as well as foster a culture of cyber resiliency by understanding the fundamentals of this standard.

- ✔ Quizzes, examples, and best practices
- ✔ No professional experience required
- ✔ Two days + certification exam

It is time to start preparing!
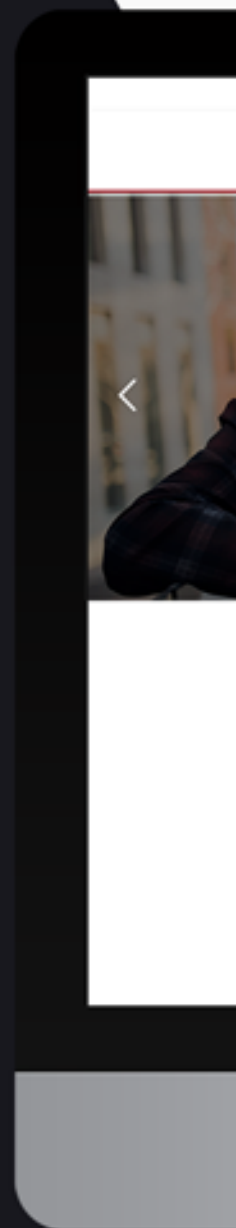
→ GET DETAILS
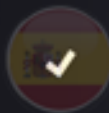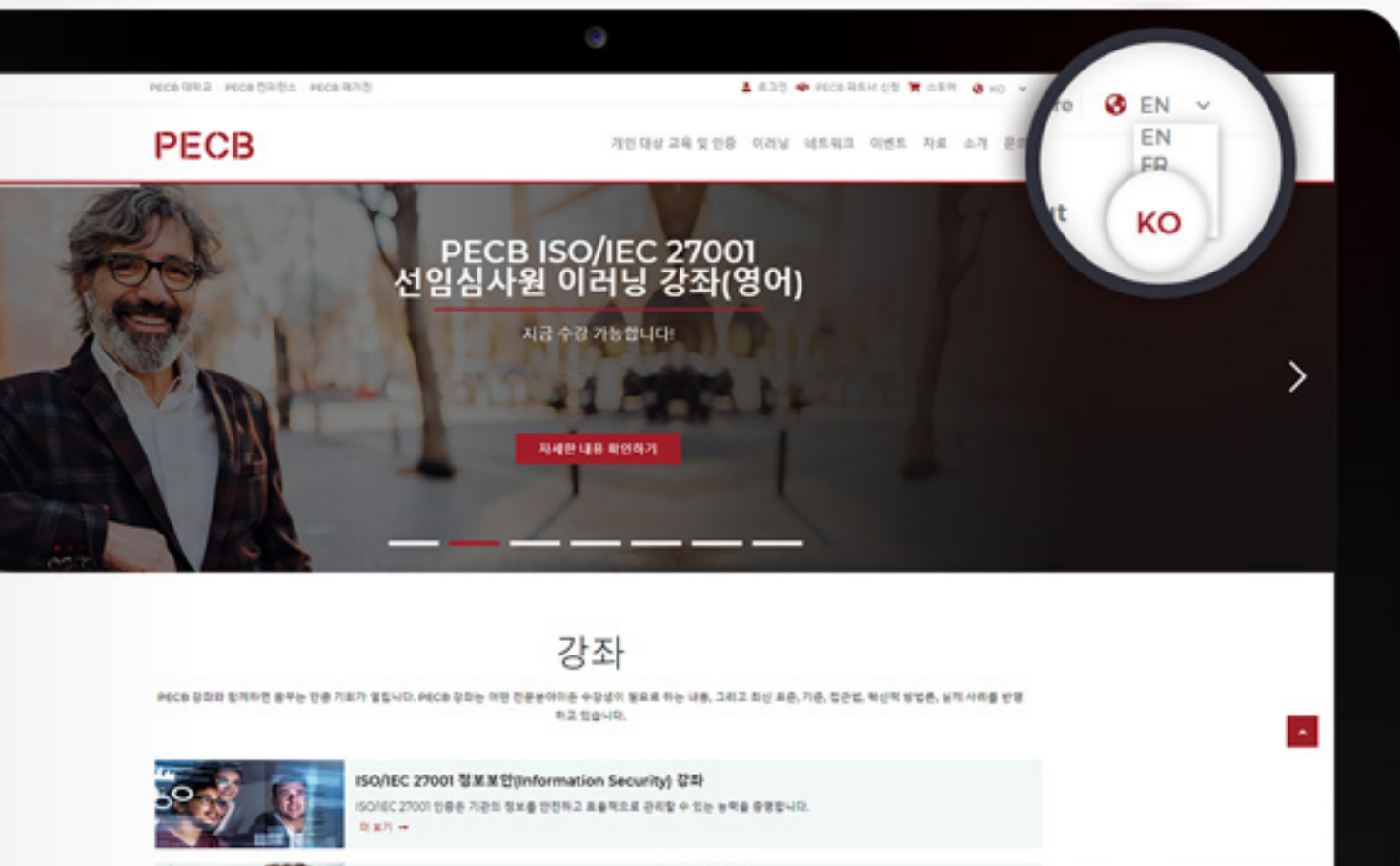
EN   GER   SPA   FR   KO

INTRODUCING THE PECB WEBSITE IN KOREAN

On March 1, 2021, Korean language was added to our website.

From now on, our Korean-speaking visitors will be able to find all the information about PECB products and services, resources, and network in their native language.

▶ ENJOY THE TOUR

Digitalized Compliance in 2021

TECHNOLOGICAL ADVANCEMENTS, BENEFITS, AND THE STRUGGLES OF IMPLEMENTING THEM

BY LUNDRIM SADIKU, PECB

Compliance directors in many organizations have started using new technological trends to facilitate their jobs. In light of some changes in our everyday lives, what does it mean to use artificial intelligence, machine learning, and robotic process automation for compliance operations? What challenges would compliance personnel face when incorporating new trends in their work? And more importantly, what's the ROI of compliance digitalization?

Introduction

Saying that businesses were affected by the pandemic is an understatement at this point. Similarly, it would be an understatement to say that different facets of organizations are undergoing digitalization rapidly. As a matter of fact, the year 2020 has served as a catalyzer to accelerate the pace of technological advancements and digitalization.

But what's in all this for compliance? After all, isn't compliance one of the few areas that has resisted the IT revolution, compared to other areas? Well, it turns out compliance can benefit greatly from incorporating digitalization in its activities.

Changes in the World and Challenges for Compliance

Let's take a look at what is happening in the world and what new challenges compliance is facing.

During- and post-COVID workplace(s)

Restrictions and regulations to contain the pandemic have pushed companies into changing their business models. Furthermore, more people than ever are working from home (WFR). The penchant for people's new workplaces and the WFR-attitude in general, will probably linger on for a while. For compliance, this means that risks need to be reevaluated. The topics that need to be addressed in a new compliance risk assessment plan are varied, from management and safety of essential staff working in company premises, to ensuring proper documentation by staff working remotely, and so on.

Brexit

Ah, good old Brexit! We thought it was done once and for all and it wouldn't appear in the news every day. But, for compliance professionals the reverberations of the Brexit deal are stronger now! In fact, after the 1000+ page deal was published, compliance directors and legal staff working in organizations that operate partly or fully within

the UK were among the first who needed to understand what the deal meant for their organizations. And of course, there are many issues that remain unclear.

Fraud, ransomware, and other threats

Malicious activities online, and especially fraud have seen an increase during the lockdown(s). See, for example, the report by LIMRA on fraud in financial services.

For compliance, this means that they have to stay one step ahead of the fraudsters, hackers, and so on, by maintaining existing security controls of various management systems and implementing new controls (i.e., updating those management systems). Furthermore, the remote workforce is more vulnerable to threats from outside compared to the workforce working on company premises. The compliance team, therefore, needs to reassess risks and offer support in light of the new work circumstances.

Laws and regulations on data collection and processing

Newer, stricter laws that regulate the collection, compiling, and processing of data and personally identifiable information (PII) are constantly being enforced in a lot of places (e.g., the GDPR in EU, CCPA in California).

Again, as was the case with the Brexit deal, compliance directors need to look out for the ways in which their organizations use data, how technological upgrades affect data collection and processing, and what protective measures are in place for individuals whose data is being collected and processed.

Money laundering and bribery

Compliance directors working in the EU need to understand the Money Laundering Directives (MLD) updates continuously. In fact, this document keeps being updated by EU authorities quite often. The latest update (MLD6) extends the criminal liability to legal persons and it expands the scope of criminality (with "aiding and abetting" being grounds for prosecution as well).

What Digitalization of Compliance Processes Entails

Well-configured software undoubtedly helps automatize many activities that some people would consider time-consuming and painstaking. Digitalization of compliance activities means that certain processes are now managed by technology, while the compliance personnel can shift their focus onto data analyses, interpretation, and other logical activities that technology cannot replace.

Artificial intelligence (AI)

A very valuable use of AI is finding relevant information across the entire internet. Google Alerts, for instance, is one example. The compliance personnel can rely on such tools to be notified every time something that pertains to their work comes up, without having to do random internet searches periodically.

More specialized uses of AI include risk and threat identification and rating based on previously set configurations. AI can also approximate the likelihood of threats occurring.

Another use of AI that cannot be overlooked is the conducting of gap analyses. AI can compare and contrast an existing system with a desired one, thus identifying the gaps which would later be analyzed by the compliance personnel.

Machine learning (ML)

As you can probably infer from the name, machine learning "teaches" computers to acquire data, analyze and make predictions, and it does this through big data. An example of machine learning in use are analyses and predictions for the number of and risk presented by malicious emails based on data from previous attacks.

Robotic process automation (RPA) in monitoring and measurement

RPA is optimized for collecting data from multiple sources (non-financial or numerical data included, as well as risk reporting) thus enabling companies to refocus their employees' potential in highly complex tasks that are judgment-based. Interestingly, RPA can also be optimized for risk-analyses, root-cause analyses, and so on.

Key Takeaways

✔ **Digitalization nowadays is unavoidable, and the pandemic has only accelerated it.**

✔ **The world going through major changes and that means more work for compliance; those changes can be political (as is Brexit), legal (GDPR, CCPA), or social (work-from-home attitudes, social inclusivity, etc.).**

✔ **Digitalization of compliance activities allows the personnel not to do time-consuming tasks, which can be done by AI and other software, but instead to focus on meaningful analyses and be involved in decision-making.**

Where to Go From Here

First and foremost, implementing new systems or tools is not always easy. In the case of digitalization of compliance, it is a process that requires the involvement of multiple stakeholders. The top management must express their support in concrete ways; the compliance team must cooperate with the IT and/or software development team since their expertise is needed; compliance staff themselves need to have some IT background, apart from their business and/or financial education, and so on.

PECB Resources to Improve Your Compliance Processes

PECB's eLearning platform brings you several training courses on international standards in information security and risk management, with training courses on data protection, anti-bribery, and privacy protection to come this year.

The anti-bribery virtual conference scheduled to be held in May is also a great opportunity to bring people from all around the world closer and learn more about the latest updates, trends, and practices in anti-bribery measures. Sign up for free and learn from various sessions in French, English, or Spanish.

APRIL 28

HAPPY WORLD DAY FOR SAFETY AND HEALTH AT WORK

Anticipate, prepare, and respond to crises – Invest Now in Resilient Occupational Safety and Health Systems

Almost every aspect of the world of work has been impacted since the COVID-19 pandemic emerged as a global crisis in 2020. The current crisis demonstrates the importance of strengthening OHS systems and investing and creating resilient Occupational Health and Safety systems, which will help mitigate the spread of the virus at the workplace.

PECB can help you! Celebrate this day by taking any of our ISO 45001 training courses!

→ FIND OUT MORE

Are you ready to fall in love with the Istrian Peninsula?
Our Istria itinerary highlights the most charming places to
visit in Istria, from medieval towns and breathtaking scenery
to ancient ruins and the beautiful coast of the Adriatic Sea.
If you are wondering what to see and which places to visit on
the Istrian Peninsula, continue reading and start planning
your ultimate Istrian Peninsula road trip.

ARTICLE BY CHASING LENSCAPES

Istrian Peninsula

CROATIA

PECB advises you to avoid traveling nowadays due to the ongoing COVID-19 outbreak. However, make sure you add this incredible destination on your travel bucket list.

The heart-shaped Istrian peninsula is one of the most charming places in Croatia, and the fact that it has successfully stayed under the radar of mass tourism for such a long time is an added bonus. However, things are changing quickly and in recent years, more and more tourists have been visiting Istria. So our advice is to start planning your Istria itinerary ASAP if you want a chance to explore the highlights of the Istrian peninsula before it loses its charm.

Where Is the Istrian Peninsula Located?

The Istrian peninsula is the largest peninsula in Croatia. It is located in the westernmost part of Croatia at the head of the Adriatic between the Gulf of Trieste and Kvarner Bay.

Motovun, Central Istria

The peninsula is shared by Croatia, Italy, and Slovenia, though the most substantial part belongs to Croatia. Blue Istria (along the coast) and Green Istria (inland) are two places that are worth mentioning when talking about the Istrian peninsula.

Green and Blue Istria Highlights

So why should you visit the Istrian peninsula when there are so many other charming places all over Croatia? The answer is simple enough; the Istrian peninsula is different from any other county in Croatia. We fell in love with the beautiful scenery, stunning medieval towns and fishing villages, food scene, and the unique atmosphere.

When talking about Istria, there are actually two different parts you can explore. Along the coast, you will find Blue Istria with its charming coastal towns and marinas, colorful Venetian houses, seafood restaurants, stunning beaches, and luxurious hotels. The inner areas of the Istrian peninsula are referred to as Green Istria. When traveling around these parts of the peninsula, you will see vineyards and olive groves, photogenic medieval towns perched on cliffs, an agricultural landscape, and a general rustic and homey vibe which means less posh accommodation choices.

There are a couple of cities in Istria and a few small towns, but you will mostly find villages there, the majority of which are located in Green Istria. According to the Croatian census, there are over 500 villages in Istria. An average Istrian village has a community of about 100 people. Some might have over 300 inhabitants, but there are also villages which are populated by only a dozen of people and some are completely deserted. So what are some the highlights of the Istrian peninsula in our opinion?

> Some of the most stunning towns in Croatia are located on the Istrian peninsula: Rovinj, Poreč, and Motovun, to name a few.

> Breathtaking scenery of rolling hills, olive groves, vineyards, and the hues of blue, green, and turquoise of the Adriatic Sea

> A foodie scene with an emphasis on truffles, wine, olive oil, and seafood

> Old traditional charm combined with a unique mixture of Italian-Croatian atmosphere

> Beautiful rocky and pebble beaches where you can enjoy the Adriatic Sea without crowds

> A unique focus on hiking and cycling trails so you can plan an active vacation combined with wine tasting

DAY 1

ROVINJ, THE MOST CHARMING TOWN ON THE ISTRIAN PENINSULA

Rovinj

Rovinj is our favorite town in Istria. Once you visit it, you will understand why we recommend staying here for your first few nights. From the moment we started exploring Rovinj's old town, we couldn't have enough of the colorful houses and Mediterranean atmosphere. Rovinj's old town used to be an island, so while you are strolling through the narrow cobbled streets, try and find these bottom porches that will reward you with beautiful views of the Adriatic Sea. There are hidden gems behind every corner, cool cafés, unique boutiques, colorful houses with photogenic laundry lines, and many more such treasures waiting to be found.

We stayed at Residence Rovinj, a cute hotel with its own parking lot that was within walking distance to the old town. If you have a car, make sure your hotel has a parking lot. We loved the intimate and friendly atmosphere, the large rooms and good breakfast. It is a good choice for mid-range accommodation.

If you'd like to stay at the heart of the old town, Hotel Adriatic is an excellent choice. This luxurious boutique hotel provides beautiful views and is situated at the heart of Rovinj's old town. You will also find one of the best restaurants in town inside the hotel.

For a more budget-friendly choice, try the cozy but stylish The Melegran that also has a very central location and excellent reviews. For all hotels and apartments in Rovinj, check prices here.

Things to See in Rovinj

> Getting lost in Rovinj's old town (if you want to learn more about the history of Rovinj, check out this walking guided tour.)

> Visiting St. Euphemia Church and its Bell Tower

> Looking for Balbi's Arch and Rovinj Town Clock

> Wandering around Rovinj Harbor

> Looking for the famous Rovinj viewpoints

> Watching the sunset from one of the sea-front coffee shops and bars

> Exploring Rovinj Archipelago

> Going on a cycling trip along the coast. You can check this guided cycling tour that has great reviews.

DAY 2

PULA AND CAPE KAMENJAK

Aerial view of the Roman Amphitheatre in Pula

Pula

On day two of your itinerary, it is time to discover the southern part of the Istrian peninsula. Within a relatively short car ride from Rovinj, you'll find Pula, the largest city on the Istrian peninsula where you will also find an international airport.

Pula has some of the best ancient Roman ruins in the area and some charming alleys of its own.

What to See in Pula

> Visit Pula Arena – one of the most well-preserved Roman amphitheaters in the world

> Check out the Roman Forum

> Walk under the Arch of Sergii

> Enjoy the view from Fort Kaštel

> Stop by the House of Istrian Olive Oil

> Take a paddle-board tour or go kayaking and snorkeling around the sea caves along Pula coast with any of these recommended tours

Cape Kamenjak

The Kamenjak Peninsula or Peninsula of Premantura is located at the southernmost point of Istria. It is a protected reserve with a beautiful rugged coastline, stunning beaches and coves, and hiking and cycling trails.

Other than gorgeous beaches, the Premantura Peninsula is home to more than 500 plant species, including 20 orchid species. It is located only a short drive away from Pula. You can also go cliff jumping or kayaking in the area.

Kamenjak

# LIM FJORD, POREČ, AND NOVIGRAD

Lim Fjord

The third day on your itinerary is dedicated to a road trip along the northern part of the Adriatic coast along the Istrian peninsula. This area of Istria is dotted with beautiful fishing towns, stunning beaches, and some breathtaking views, such as the stunning Lim Bay.

Things to Do in Lim Fjord

> Take a boat ride to explore the bay

> Eat fresh oysters and mussels

> Rest at the tiny beach

> Admire the views and beautiful scenery

Lim Fjord
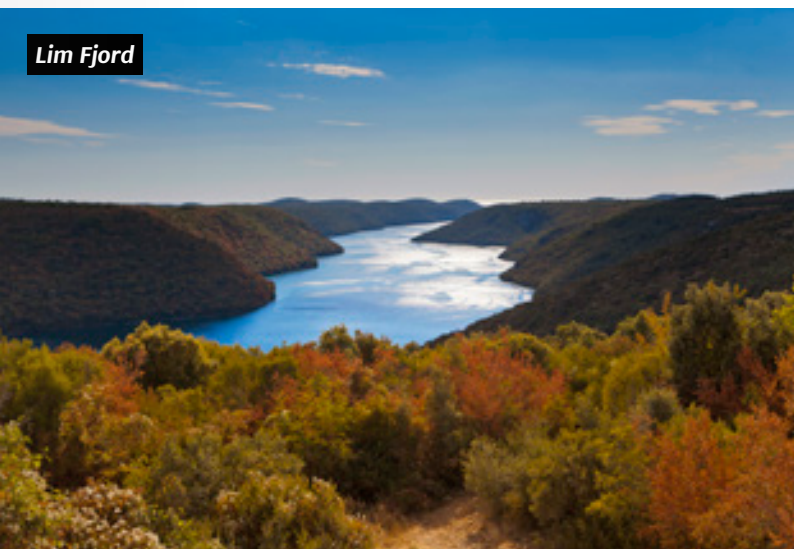
Euphrasian Basilica in Porec

Poreč

If for some reason you'd rather stay at a different town than Rovinj, Poreč is probably one of the best places to stay along the coast of the Istrian peninsula. It offers just the right mixture of historical monuments, charming cobbled streets, lovely beaches, and foodie and night scenes.

If you are looking for a central location, Valamar Riviera Hotel & Residence is a great choice. With its modern design, rich breakfast, and private beach on the nearby Sveti Nikola island (free shuttle boat), it offers some great deals on rooms throughout the year. You can check other accommodation choices here.

Things to See and Do in Poreč

> Visit the Euphrasian Basilica – a UNESCO World Heritage Site

> Wander around the Historic Center of Poreč

> Walk along the two main streets, Decumanus and Cardo Maximus

> Stop by the main square – Marafor

> Check out the Round Tower where you will find Torre Rotonda Caffé Bar

> Visit the Poreč Heritage Museum

Novigrad

Novigrad is located just north of Poreč, and it has been gaining a reputation for itself as a foodie town. Other than excellent restaurants, you will find here lovely beaches and a charming historic center.

Check out the smart Boutique Hotel Rivalmare which is beautifully designed and is situated just near the old town and the beach. You can check other options for hotels and apartments in Novigrad here.

Things to See and Do in Novigrad

> Visit the charming old town

> Look for the local churches and bell towers

> Visit the Maritime Museum

> Explore the beaches and visit the water sports center

> Visit some of the best restaurants on the Istrian peninsula

DAY 4-5

GREEN ISTRIA ROAD TRIP (OPRTALJ, MOTOVUN, GROŽNJAN, AND BUJE)

Motovun

After spending a couple of nights in Rovinj, it was time for us to start our journey to discover the charms of the inner parts of the Istrian peninsula. We spent the next couple of nights in Oprtalj, a small town with breathtaking views that is located very close to Motovun.

Oprtalj

Oprtalj (or Portole in Italian) is one of the most picturesque towns in green Istria. To be honest, there is not much to do in this tiny town, but we chose it as our place of accommodation thanks to the stunning views of the Mirna Valley and proximity to Motovun. We didn't know what to expect, but strolling along the tiny old town of Opetalj, we felt we had discovered a hidden gem. It is a place where time stood still. Photogenic crumbling walls decorating narrow cobbled alleys that lead to ancient houses and beautiful archways, an old bell tower, and the occasional flowers and green vines dotting this historic town.

We stayed at the charming B&B Palazzo Angelica (for adults only). We didn't stay at the main house, but we had a lovely apartment inside the old town. The only downfall was that we had to carry our suitcases on the uneven cobbled alley (uphill) and then climb a few flights of stairs.

However, the friendly staff will gladly help you. We loved our stay here but be warned, Oprtalj is very low key and you only have two restaurants to choose from. If you are looking for a bit of a more lively atmosphere, Motovun or Grožnjan are going to suit you more.

Things to See in Oprtalj

> Admire the unbelievable view from Venetian Loggia
> Check out the old main gates of the old town
> Wander along the cobbled alleys of the old town
> Have a snack or a glass of wine with the most amazing view

Motovun

You can't visit Green Istria without stopping at Motovun. Motovun is perched on a 270-meter hill and is surrounded by vineyards and olive groves. The sight of Motovun and the surrounding area in the early hours of the morning covered gently in a veil of fog, is magical. If you stay in the area (and you should), try and catch a glimpse of it with your camera. Nevertheless, if you can't bother to catch the sunrise or you choose to visit Motovun on a day trip from the coast, don't worry, it's stunning every hour of the day.

If you want to stay in a hotel at the heart of Motovun, check out Hotel Kastel. Other than that, there are several apartments and B&B you can check here. If it's luxury you are looking for, then Wine & Heritage hotel ROXANICH is a boutique hotel located very close to Motovun which also has its own gourmet restaurant and a wellness center.

Things to See in Motovun

> Take a picture from the road of the landscape with the beautiful Motovun perched on the hill

> Wander around Motovun's cobbled alleys

> See the historical monuments of the ancient city of Kastelijer with its defensive walls, fortifications, and gates

> Admire the mixture of Gothic, Romanesque, and Renaissance architecture

> Visit the Parish Church of St. Stephen with its bell tower

> Buy some local souvenirs

> Admire the view with a glass of wine

Grožnjan

Grožnjan is located very close to Motovun and Oprtalj. It is another beautiful Istrian village which is known as the village of artists. One of the highlights of strolling around this charming village was to see all of these unique and beautiful medieval houses adorned by artistic displays.

In Grožnjan you'll find only small apartments. You can check the prices here.

What to See in Grožnjan

> Stroll around the picturesque streets

> Look for unique souvenirs

> Visit the Fonticus Gallery

> Look for the Church of St Vitus, Modest, and Crescentiu

> Have the best cappuccino with a platter of cheese accompanied by a stunning view

Grožnjan

Buje

We only had one day to explore the central and northern part of the Istrian peninsula, which means we didn't get to see everything we wanted (and we stopped for some wine tasting as well). Buje has plenty to offer, so if you do have the time, try and include it in your Istria itinerary.

We were planning on staying at San Servolo Resort & Beer Spa, which has beautiful views, modern and funky design, and a beer spa. Check the prices for other accommodation choices in Buje here.

What to See in Buje

> Visit St. Servulus church and its bell tower for some magnificent view of the area

> See the Tower of St. Martin which was part of the Venetian walls that surrounded Buje

> See the collections at the Ethnographic museum, which showcases local handicrafts and highlights the culture of the area

> Roam the alleys of the historic center and look for local delicacies

> If you're looking for an extraordinary experience, visit the beer spa at San Servolo Resort & Beer Spa

---

DAY 6

DUGA UVULA, RABAC, AND LABIN

Duga Uvula or Rabac

There are plenty of beaches all around Istria and even from the center of Istria it should take no more than 45 minutes to get to one of the beaches. We wanted to have a relaxed day and mainly do some photography, and we've heard Duga Uvula is a beautiful place. Duga Uvula is a beautiful cove with stunning crystal-clear water and a friendly vibe. When you follow the path, there are many options to take one of the stairs that lead straight to the sea. The beach is not very kid-friendly, at least the parts we visited. There was a very simple bar with some drinks and snacks (Punta Beach Bar) where we visited. For us, it was the perfect spot because we were looking for a private location. However, if you are looking for a lively atmosphere and more options in terms of attractions and restaurants, check out the small resort town of Rabac. It is much more touristy and suited for families, there are more restaurants and a few beaches to choose from. There is also a lovely promenade. Note that it is a trendy place to visit in the summer so it can get crowded.

Rabac

Labin

Labin

We've heard about Labin only on our last day in Istria and so it was too late to visit it. Since it is located very close to Duga Uvula and Rabac, you should stop there if you have a chance. Labin is another medieval hilltop town which used to be the largest mining center in Croatia. Nowadays, you can find here a few galleries, charming alleys, historical sites, and gorgeous views of the Adriatic Sea. You'll find many resorts and apartments around Rabac for different budgets. Check their prices here. In Labin, you'll find only two hotels. Hotel Peteani offers stylish rooms, great breakfast, and free bikes and has great prices for solo travelers. The second hotel, La Loggia Diffused Hotel, is another great choice for visitors who are looking for modern and stylish design and a budget friendly price tag. For more accommodation choices in Labin, check your options here.

What to See in Labin

> See the Little Theatre or Il Teatrino at Labin old town

> Check out Porta Sanfior, the old town gate

> Visit the Church of the Blessed Virgin Mary's Birth

> Admire some of the Baroque palaces and buildings such as the Battiala-Lazzarini Palace

> Stop by the art galleries or Labin's city museum

> Admire the view from Fortica Viewpoint

Final Tips to Help You Plan the Perfect Istria Road Trip Itinerary

1. Try to arrive early to the main tourist attractions since you can't get into the old city with your car, and you'll have to find a parking lot (some of which can get crowded later in the day).

2. Don't forget to ask for a GPS in your car or use a GPS app on your phone. We recommend downloading an Istria Map from Google Maps before your trip since at some places, you will have a bad signal. At least you'll have a map of the area on your mobile.

3. You can use the Croatian Automobile Club's app, Hak Traffic, to check for any traffic, closed roads, etc.

4. The roads in Istria are pretty narrow, can be curvy, and some of them are basically dirt roads. Therefore, check the ETA on your app and consider your gasoline consumption. Many times we arrived at our destination later than anticipated.

5. Relax and enjoy your time – part of the reason we didn't get to check off all the attractions on our bucket list was simply since we wanted to enjoy the moment. So instead of rushing from place to place, choose the top sites you'd like to visit in advance and leave room for improvisation.

10 WAYS TO PROTECT
EARTH
EVERY DAY

Here are some tips to protect earth everyday and take action and continuously spread awareness about protecting the environment and making it part of our everyday habits.

Source: The Old Farmer's Almanac

Support Our Pollinators

Bring native bees and other pollinating creatures to your garden by selecting the right plants.

Clean up Plastic in Your Neighborhood or Local Park

Swap out Your Kitchen and Household Products

Plant a Tree

Use Wildflowers and Native Plants

Wildflowers and indigenous species are not only beautiful but also attract native and beneficial insects that improve both pest control and pollination.

Reduce, Reuse, Recycle in the Garden

Stop Pesticides and Chemicals in the Garden

Conserve Water

Think About Your Diet

About one-third of the food that we produce every year goes to waste annually!

Get Kids Involved

Pass down a love of nature and plants to kids. There are lots of opportunities for hands-on learning experiences outside.

Anti-Bribery and Corruption: The Continuous Challenge

BY VIOLETA HAXHILLAZI, PECB UNIVERSITY

The development of the economy worldwide followed by a greater scale of globalization has been followed by bigger challenges with regard to anti-bribery and corruption (ABC) compliance. The globalized companies started expanding their activities in less developed countries with less regulated legal frameworks on the one hand, or the very well-regulated but ineffective agencies to provide with full enforcement of the legal and compliance framework. Under these circumstances, companies were left to the decision and efforts to self-develop new strategies of compliance that are not only global but also take into consideration the differences in the national regulations.

Anti-Bribery and Corruption Laws and Standards

Some of the laws and acts effectively in force to manage bribery and corruption are mentioned below:

> OECD's Code on Anti-Bribery and Corruption
> ISO 37001 standard
> The Prevention and Combating of Corrupt Activities Act (PCCA)
> The UK Bribery Act
> The US Foreign Corrupt Practices Act (FCPA)
> Many others in force on a national level

What Is an Anti-Bribery and Corruption Policy?

An anti-bribery and corruption policy sets out the company's stance on all forms of corruption. As policies are generally adopted by a governance body within the company, the ABC policy is about to send a powerful message from the top management to the employees, the third parties operating with the company, and possible regulatory authorities as well. The best practices show that the expected questions to be answered via the ABC policy in the company could be the following:

> What is bribery? What are the most common features of bribery and corruption?
> How is that demonstrated internally and externally? What measures have the companies taken to manage third-party operations?
> What is the regulatory framework to nationally comply? Are there any new best practices foreseen to mitigate the reputation risks associated with it?
> What are the company's plans to raise the awareness by strengthening the control environment: training programs, surveys, etc.?

Challenges in Managing ABC

As stated in the list of laws and standards, the first initiatives were from the members' organization of OECD (the Organization for Economic Co-operation and Development) who signed a convention aiming the establishment of the legally binding standards to criminalize the bribery of public officials. Since then, a growing number of states have embraced the practice and passed ABC laws. However, despite all the extended efforts to combat bribery, the illicit payments to the counterparties continue to burden economies. Referring to the surveys conducted by several international consulting companies, the findings have the same denominator:

1. There is a high responded number of the participants from the companies' part of the surveys that confirm that "they are challenged by the issue of ABC compared with the survey results of years ago."

2. As companies continue to globalize, management of third parties poses the greatest challenge in executing ABC programs.

3. Despite the high attention towards the matter, the right to-audit clauses over the third parties have not exercised the right. Plus, due to the frequent and complex transactions, the difficulty of monitoring the business dealing with the third parties remains a high-risk area.

4. Recently, data analytics is supporting the assessment of ABC controls in a more efficient and effective way. Yet, despite of having a cost-effective tool in place, more remains to be used in data analysis.

5. Lack of resources and continuous training programs to manage ABC risks, are not set high in the top management.
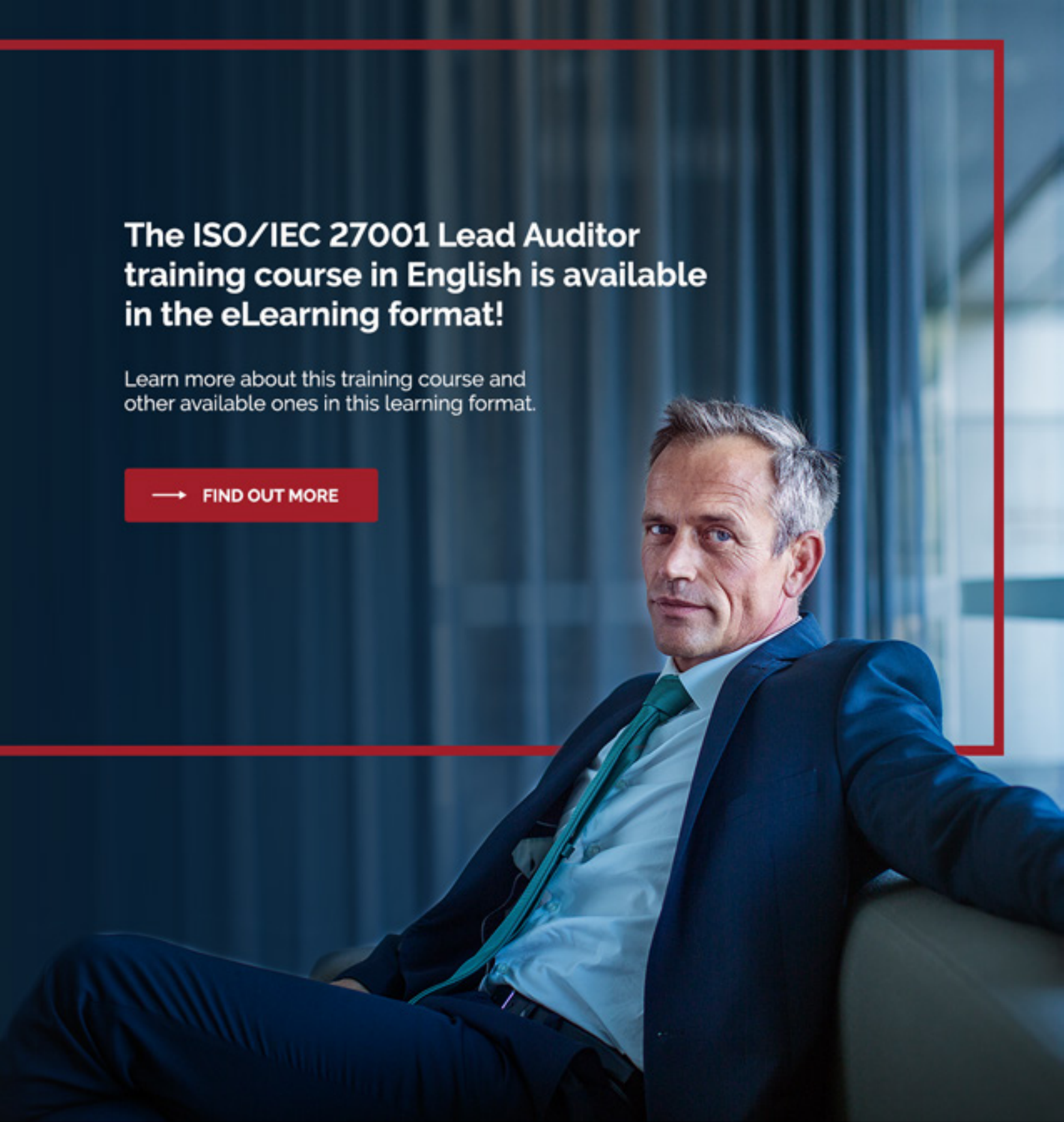
Compliance is about to strengthen by conducting risk-based anti-corruption due diligence procedures on the potential business acquisitions and/or operations to avoid not only any successor liabilities but also any future bribe payments. Companies should take at least the steps to inform themselves as much as possible from publicly available sources about the targeted company, its reputation and the management ethics, its likely customers, and government relationship.

Ultimately, it remains critical that the top management not only issues policies with regard to ABC, but it foremost ensures that they carefully approach how they deal with the implementation in practical manners of them turning themselves into the role models for the employees and the third-party representatives.

AN EXCELLENT FOUNDATION FOR FUTURE SUCCESS

Experience the difference through PECB training courses!
Check our new and most recently updated training courses
and take the one that suits you best.

Training Course	Language	Status	
ISO 14001 Foundation	English	Updated	→
Lead SCADA Security Manager	English	Updated	→
GDPR – Certified Data Protection Officer (CDPO)	Spanish	Updated	→
ISO 22301 Lead Implementer	English	Updated	→
Lead Cloud Security Manager	English	New!	→
ISO/IEC 27001 Lead Implementer	Korean	New!	→

SPECIAL T[

TITANIUM

Global Knowledge

Your fastest way to learn. Why wait?
FIREBRAND

GRUPO CONCEPTA

O
f o

PLATINUM

EduGroupe
Accompagner pour réussir

ib

i t²
التقنية الأمنية

★ iCERTWORKS
TRAINING & CERTIFICATION

SecurityKaizen
The Training Division Of Bluekaizen.org

PHILLIPS CONSULTING

CYNTHUS

NEOS

GOLD PA

E-WORK

Deloitte.
LATAM

mii
Formation

RESTREPO RAMAS

Tenol Alpha
LIMITED

BIT

Tecnofor

QMC
Quality Management Center

alc

FCT

tfkeir

BSJ

TSTC
ICT en Security Trainingen

Afenoid

KRUCEK

aac aswar akka consultancy

CIP
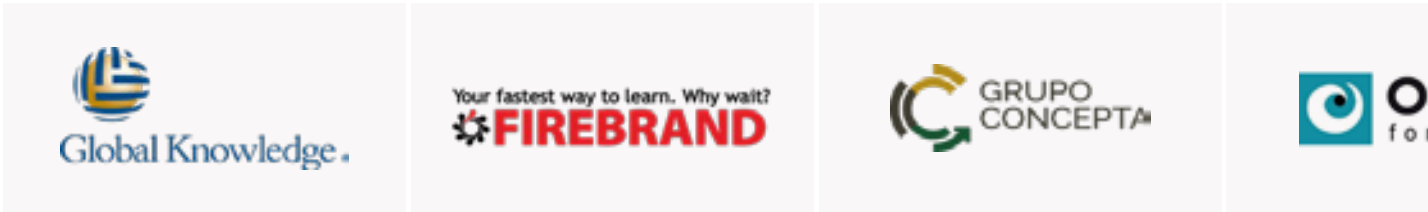
Note that PECB Partners are listed as per the credits a

HANKS TO

PARTNERS

PARTNERS

ARTNERS

acquired from January 1, 2020 to December 31, 2020.
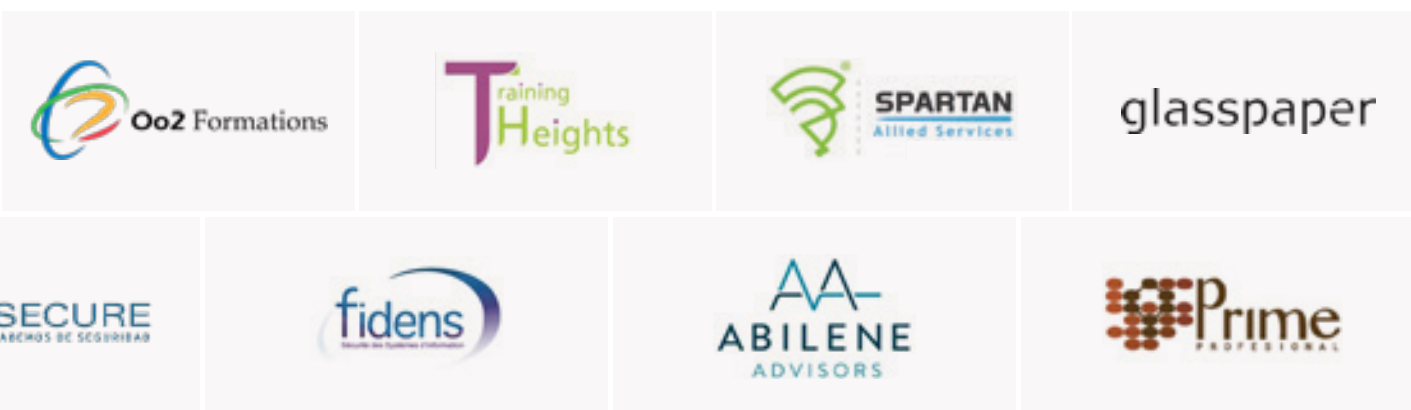
SHIELD YOUR ORGANIZATION!

Take our anti-bribery and compliance training courses and be better equipped to support anti-bribery and corruption compliance organization-wide.

Attend the Anti-Bribery Conference 2021 scheduled for May 17–20 for stimulating discussions on the challenges of combating bribery and many related topics.

→ REGISTER FOR FREE