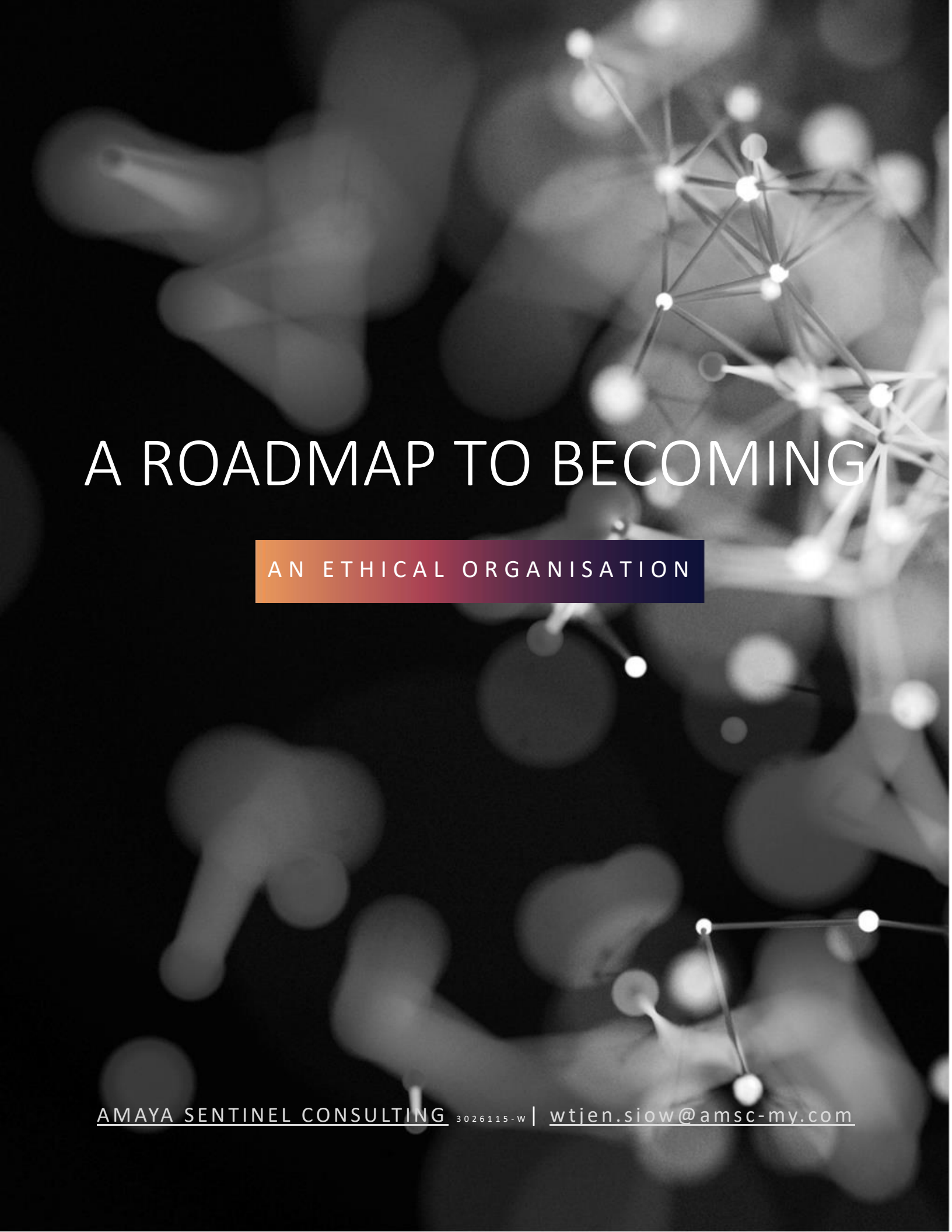
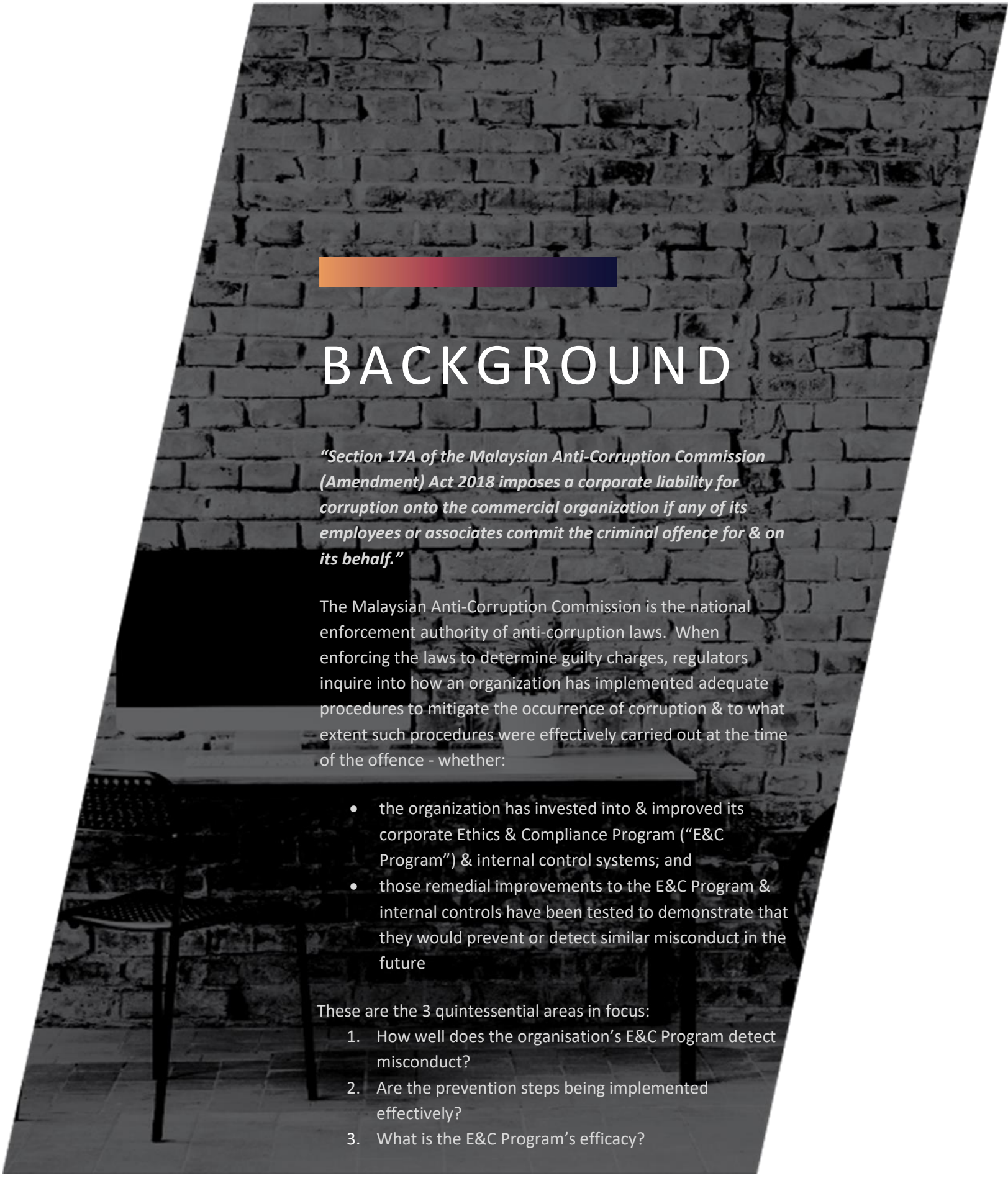


A ROADMAP TO BECOMING

AN ETHICAL ORGANISATION

AMAYA SENTINEL CONSULTING 3026115-W | wtjen.siow@amsc-my.com



BACKGROUND

"Section 17A of the Malaysian Anti-Corruption Commission (Amendment) Act 2018 imposes a corporate liability for corruption onto the commercial organization if any of its employees or associates commit the criminal offence for & on its behalf."

The Malaysian Anti-Corruption Commission is the national enforcement authority of anti-corruption laws. When enforcing the laws to determine guilty charges, regulators inquire into how an organization has implemented adequate procedures to mitigate the occurrence of corruption & to what extent such procedures were effectively carried out at the time of the offence - whether:

- the organization has invested into & improved its corporate Ethics & Compliance Program ("E&C Program") & internal control systems; and
- those remedial improvements to the E&C Program & internal controls have been tested to demonstrate that they would prevent or detect similar misconduct in the future

These are the 3 quintessential areas in focus:

1. How well does the organisation's E&C Program detect misconduct?
2. Are the prevention steps being implemented effectively?
3. What is the E&C Program's efficacy?

WHY HAVE AN ETHICS & COMPLIANCE PROGRAM?

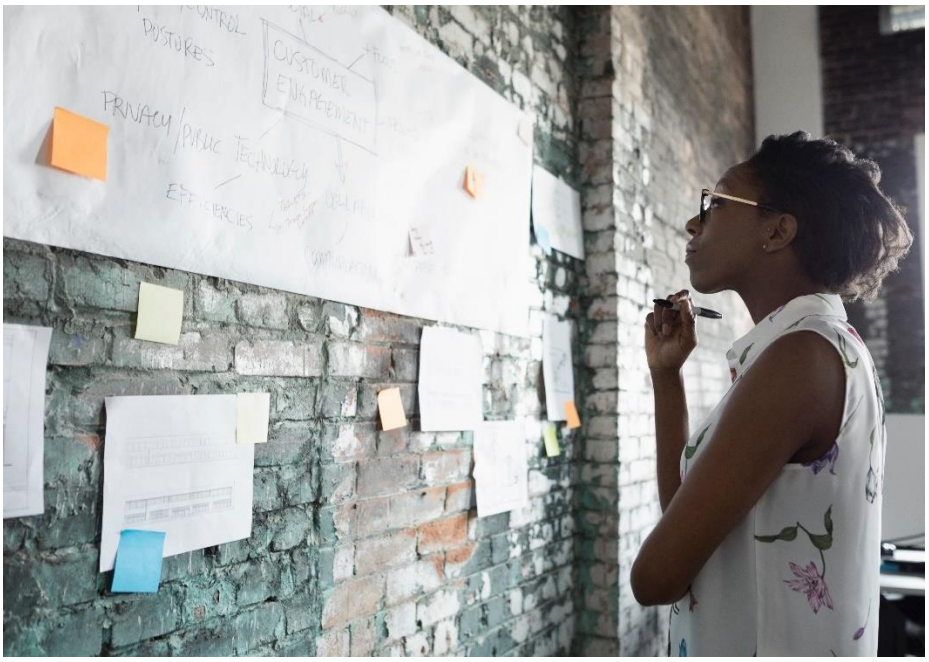
This is a guide to becoming an ethical organization, based on the Framework of an Ethics & Compliance Program
- to prevent, detect & remediate misconducts

"Non-compliance is far more expensive than a slight investment in an E&C Program.

While fines, penalties or jailtime might give sufficient motivation to address compliance risks, they may only represent a fraction of the overall costs associated with non-compliance.

Ongoing legal costs, falls in the company share price, losing the talent pool & lasting reputational damage can aggravate a company's bottom line into the red for some time.

Even an individual's professional career & honour will be hurt."



Enforcement is on the uptake. Board Members & senior executives can be vicariously liable for any illegal misconduct in the organisation. Like with all other strategic plans & decisions, they need to have oversight of ethics & compliance standards (even the lack thereof) in the organisation.

Compliance ensures that an organisation stays on the right side of the law. It is a form of mitigating risks on non-compliance of external laws & regulations, both legal & industrial. Compliance also mitigates risks on non-compliance of internal policies & procedures, as well as occurrence of fraud, corruption & other criminal offences that could cause reputational & financial losses.

Ethics upholds an organisation's reputation. It entails responsible behaviour like exhibiting professionalism while conducting business, making business decisions that align with the company's core values, respecting the rights of others & doing the right thing.

Companies that are having to operate in a highly complex & increasingly regulated ecosystem will source for long-term ethical business partners. In recognising this & maintaining a strong E&C Program, an organisation has a competitive advantage over its industry peers that do not.

Ethical organisations are creating plenty of goodwill with many stakeholders like their investors, employees, customers, partners, vendors, etc., who in turn extend their loyalty & pledge integrity to them. This can greatly impact a company's performance financially through better output from its reassured workforce, & more consumers of its products or services earns a premium on its prestige.

THE FRAMEWORK

CONDUCT AT THE TOP

- Leaders encourage compliance through their words & actions
- Models of proper behaviour for subordinates, the workforce & the business community

SHARED COMMITMENT

- Leaders demonstrate engagement to compliance initiatives & remediation efforts
- How they face competing interests & manage ethically challenging business decisions

OVERSIGHT

- Leadership does not skim on compliance expertise
- The Board holds meetings regularly with compliance audit committee
- Being discernable & diligent when going over misconduct reports

COMMITMENT BY LEADERSHIP

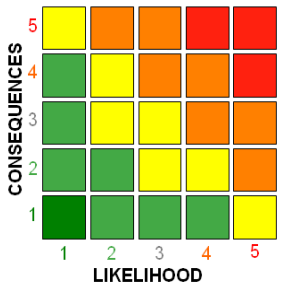
In creating & fostering a culture of good ethics & compliance with the law, the effectiveness of E&C Program starts with a high-level commitment by the organisation's leadership ("Board of Directors", "Senior Management") to set that `tone from the top'. Touted as the Owner & Driver of the organisation's E&C Program, the senior management articulates the organisation's ethical standards, conveys & disseminates them clearly & leads by example. This cadence is emulated by the mid-management, further reinforcing those standards & encouraging employees to abide by them.

The Compliance Function operates like a go-between for the Leadership, other functions, employees & external parties on compliance related matters. The competent compliance function:

- is an effective communicator,
- is independent,
- is a collaborator,
- advocates ethics well,
- knows the company & its organisation inside out, &
- has eyes on technical matters like regulatory updates, audits & the monitoring of performance of controls.

Assembling a team for compliance function depends on the company's business structure, risk profiles & resources. For example, smaller organisations with limited resources may appoint a part-time compliance champion as a present option. The compliance champion has a full-time job in the organisation performing finance reporting or human resources tasks but has the additional compliance responsibilities. The Leadership extends support to the compliance function of big or small organisations by giving ample *autonomy* to the latter to administer the E&C Program, being *accessible* to them, engaging external expertise & solution providers, providing *adequate budget* for compliance initiatives & interacting with other functions to mutually perform compliance responsibilities as are required of their role.

RISK ASSESSMENT



The effectiveness & the manner in which an organisation's E&C Program is tailored is based on its risk assessment & the risks related to the employee population. As the organisation changes/ adapts to business strategies, the risk criteria too should be periodically updated & revised, so that risk-tailored resources can be allocated appropriately.

Identifying & assessing risk profiles from a commercial perspective to detect particular types of misconduct most likely to occur in a particular line of business is rather intuitive, such as analysing & addressing varying risks presented by, inter alia:

- the business model, products or services,
- the location(s) of its operations, the regulatory landscape,
- the industry sector, the competitiveness of the market,
- the potential clients, supply chain & business partners,
- transactions with governments, payments to government officials,
- use of third-party intermediaries,
- offering discounts, rebates or free goods,
- providing gifts, travel & entertainment
- contributing to charities & political donations.

Define who or which function should lead the risk assessment. Clearly delineated roles & responsibilities should be communicated & understood. Whichever function is leading risk assessment is unlikely to have expertise in all risk areas. Therefore, other functions ie. the procurement, finance, HR, sales & marketing & logistics (list is not exhaustive) will be expected to provide details & information of risks & risk levels faced by their functions. The inventory of risks will be rated of the likelihood of occurrence & impact of the occurrence. Once the risk assessment is complete, the findings & recommendations are compiled in a comprehensive report to be presented to the board for review & approval. An action plan that prioritises the recommendations from the risk assessment should then be developed to ensure that the necessary enhancements are implemented

CONTROL MEASURES

A well-designed E&C Program consists of preventive measures stipulating processes & procedures for the risks identified & assessed. In this relation:

Corporate Code of Conduct & Compliance Policies is established to provide `form & function' to a E&C Program, reinforcing ethical & compliant behaviours to yield better business results. With the business units being consulted when forming procedural content in compliance policies, such inclusivity creates a sense of ownership in the policies, making acceptance easier for:

Operational Integration – adopting procedures from the policies into the organisation's internal control systems.

Comprehensiveness – monitoring of controls & reflecting upon the risk spectrums, including appreciating the legal & regulatory landscape.

A Reporting Mechanism provides employees the opportunity to confidentially report allegations of a breach of the corporate code of conduct, compliance policies or suspected or actual misconduct. People managers are part of this mechanism & are given the guidance to handle some of the procedures as diligently as possible.

Effectiveness of the Reporting Mechanism – Are employees aware of a reporting mechanism in the company? Does the organisation allow anonymous reporting? Has it been used? How has the organisation assessed the seriousness of the allegations it received? Does the compliance function have full access to reporting & investigative information?

Properly Scoped Investigations – How does the organisation determine which complaints merit investigation? How does the organisation ensure that the investigations are independent, objective, appropriately conducted & properly documented? How does the organisation determine who should conduct an investigation?

Investigation Response – Does the organisation apply timing metrics to ensure responsiveness? Does the organisation have a process for monitoring the outcome of investigations & ensuring accountability for the response to findings or recommendations?

Resources & Tracking of Results – How does the organisation collect, track, analyse & use information from its reporting mechanism? Does the organisation periodically analyse the reports or investigation findings for patterns of misconduct or other red flags for compliance weaknesses?

Third Party Management involves performing risk-based due diligence on its third-party relationships. It depends on the nature of the organisation, transactions & understanding of the qualifications & associations of third-party partners, including the agents, consultants & distributors that are commonly used to act as conduit for paying bribes to government officials.

Risk-Based & Integrated Processes – Some third parties are higher-risk than others. Third-party onboarding process should correspond to the nature of third parties & level of the transactions with them ("proportionate procedures"). The process is further integrated into the relevant procurement or vendor management systems in the organisation for continuous monitoring.

Appropriate Controls – The organisation has the responsibility to ensure that there is an appropriate business rationale for the use of every third party. This includes mechanisms to certify that the contract terms specifically describe the services to be performed, that the payment terms are appropriate, that the described contractual work is performed & that compensation commensurate with the services rendered.

Management of Relationships – Some third parties' compensation & incentive structures raise red flags; therefore, careful analysis of this risk area must not be missed. Approved third parties must be monitored for their contract performance. If the organisation carves in audit rights in the contracts to analyse their books & accounts, it should have to exercise those rights. Where applicable, conduct compulsory training for third parties about the organisation's E&C Program before any commercial relations start & certify their participation in compliance efforts.

Real Actions & Consequences – Does the organisation track red flags that are identified from due diligence of third parties & how are those red flags addressed? Does the organisation keep track of third parties that fail the organisation's due diligence or that are terminated & take steps to ensure that those third parties are not hired or re-hired at a later date? If a third party was involved in the misconduct at issue in an investigation, were red flags identified from the due diligence or after hiring the third party, & how were they resolved? Has a similar third party been suspended, terminated or audited as a result of compliance issues?

TESTING, REVIEWS & IMPROVEMENT

An organisation's business changes over time, as do the environments in which it operates, the nature of its customers, the laws that govern its actions & the applicable industry standards. Accordingly, the organisation has to engage in meaningful efforts to review its E&C Program to keep it up-to-date. Periodic audits are conducted to ensure that controls are functioning well & that the strength of controls is tested.

Internal Audit – Audits are requisite to detecting misconduct. Determine how frequently & what types of audits to conduct, ie. in the quarterly intervals, audit plans can be designated for selected high-risk areas while for the year-end audit plans, most risk areas will need to be audited. Material audit findings & remediation progress are reported to the senior management & the board on a regular basis. It is in their interest to have oversight in periodic audit reports.

Controls Testing – It is commonly regarded necessary to test & review the control measures of their preventative qualities for effectiveness. Meanwhile, collecting & analysing the findings ensure that non-compliance is met with appropriate action items for remediation & tracked for completion.

Evolving Updates – When priming whether policies/ procedures/ practices make sense for particular business segments/ subsidiaries, an ethically motivated organisation would update its risk assessments & accordingly review its compliance policies, procedures & practices. A gap analysis can be undertaken to determine if particular risk areas are sufficiently addressed in its policies, control measures or training.

TRAINING & COMMUNICATION

Policies & procedures are integrated into the organisation through periodic training & certification tailored for all directors, officers, relevant employees & where appropriate, external business partners. The effectiveness of the training curriculum is measured as follows:

Risk-Based – Are employees in relevant control functions trained to identify misconduct? The organisation may have to provide tailored training for employees transacting in high-risk areas, including how to address risks in the area where misconduct may occur. People managers also receive supplementary training, ie. encouraging subordinates to embrace compliance, guiding subordinates on applications of policies, being dependable when subordinates consider raising concerns with them, etc.

Form/ Content – For best results in gaining employees' attention, training needs to be offered in the form & language appropriate for the audience. Training should also move with times, ie. provided online if in-person is not viable. Training can include lessons learned from prior compliance incidents. Following training, the employees are tested on what they have understood & duly certified.

Communications about Misconduct – The senior management takes the lead in letting employees know the organisation's position concerning any misconduct. For example, communicating about termination of employment or disciplinary actions for failure to comply with the organisation's policies, procedures & controls, even if it is in abridgement to the code of conduct & relevant policies, is key to amplifying the cadence of a E&C Program.

Distribution of Guidance – The organisation can make resources available for employees to seek advice on compliance, ie. the Compliance Manager, employee handbook, Reporting Concerns posters, contact information on computer lock screen, mementoes with compliance reminders, etc.

WHAT'S NEXT

"An organisation's response to misconduct should be reflective on the extent & pervasiveness of criminal misconduct - the number & level of corporate employees involved; the seriousness, duration & frequency of the misconduct; any remedial actions taken by the organisation, including for example, disciplinary action against past violators uncovered by the E&C Program; & revisions to the E&C Program in light of lessons learned."

An organisation should perform a root cause analysis on the occurrence of misconduct & where appropriate, engineer remediation actions to address the root causes, including but not limited to:

Prior Weaknesses – Functions entrusted with ownership of their policies & procedures, are the gatekeepers of the designated controls within. Policies or procedures that should have prohibited the misconduct but have not been adhered to presents a compliance gap.

Flawed Payment Systems – How was the misconduct in question funded, ie. purchase orders, employee reimbursements, discounts, petty cash, donations? What processes could have prevented or detected the misappropriation of funds?

Vendor Management – If vendors were involved in the misconduct, what was the process for vendor selection & did the vendor undergo that process?

Prior Indications – Perhaps there had been prior opportunities in detecting a misconduct in question, such as audit reports identifying relevant control failures, allegations, complaints or investigations. But an organisation can go further analysing why such opportunities were missed.

Remediation – What specific changes has the organisation made to reduce the risk that the same or similar issues will not occur in the future? What specific remediation has addressed the issues identified in the root cause & missed opportunity analysis?

Accountability – The organisation must respond to any misconduct in a timely manner & take the necessary disciplinary actions, including self-reporting criminal misconduct to regulatory authorities. Hold managers accountable for misconduct that occurred under their supervision because managers too are expected to magnify the organisation's position on compliance. Any behaviour should be rewarded if modelled well after the E&C Program as much as be punished for non-compliance.

CONCLUSION

A robust E&C Program does not happen overnight. It evolves with time, implementation strategies, patience, the complexities of varied regulatory landscapes, access to technologies supporting business operations & a future that juggles even more influences on conducting ethical business. The thought process behind the fundamentals of preventing, detecting & responding to non-compliance is the starting point of an organisation's journey to being self-governing. Far-sighted leaders would liken it to an `insurance policy' that reasonably provides a strong legal defence against potential investigations into alleged non-compliance.

As much as a E&C Program protects an organisation's reputation, it empowers well-adjusted employees to be ambassadors of an organisation's values & elevate ethical practices within their own functions, ultimately protecting everyone in the organisation.

Such an organisation does not wait for the law to catch up with them.

For anything compliance, find out more with:

www.amayasentinelconsulting.com
wtjen.siow@amsc-my.com