RiskNZ

WELCOME TO

RiskNZ Lunchtime Seminar: 22 November 2022

RiskNZ is proudly sponsored by:

Premier Sponsors

Camms.

PROTECHT
Redefining Risk

AON

LexisNexis®

Sponsors

SAI360
Risk | Learning | EHS | Sustainability

Insurance
BUSINESS NZ

F24

GRC solutions

Risk NZ – November 2022

Compliance Risk Management & Training

Julian Fenwick

Agenda

Compliance Risk Management & Training

This presentation will focus on the five elements of effective compliance management:

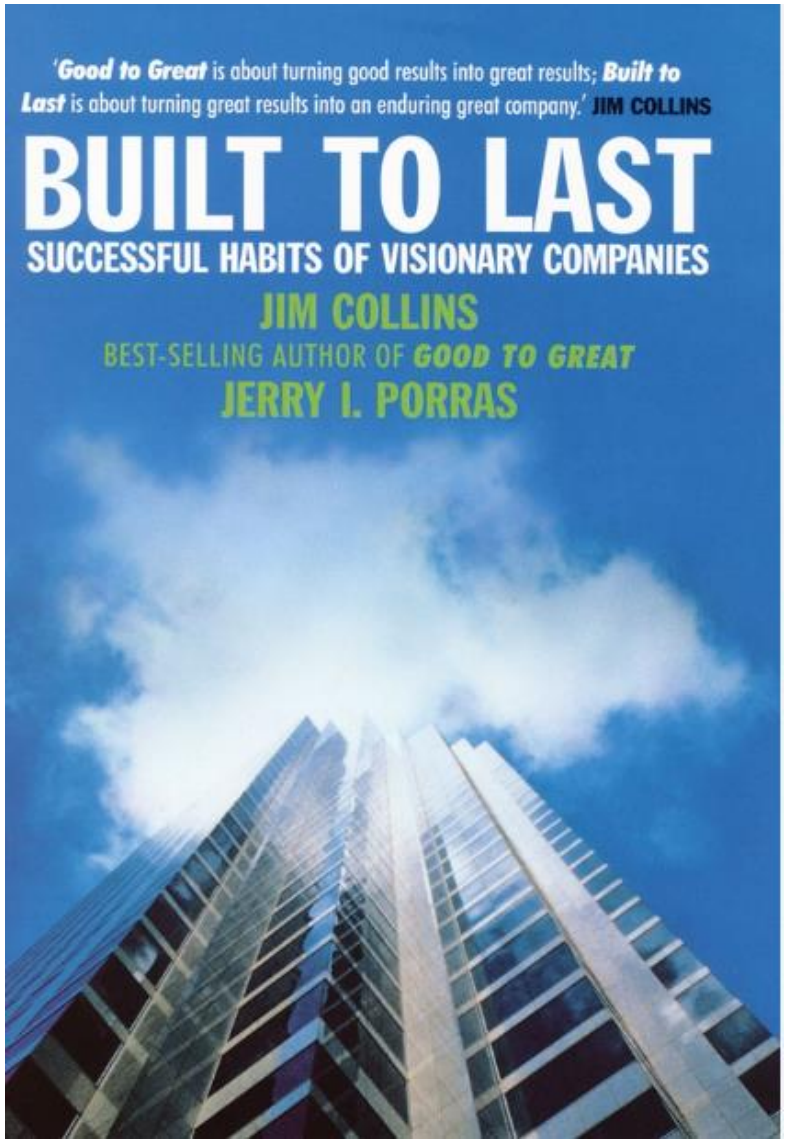
- Leadership.
- Risk Assessment.
- Standards and Controls.
- Training and Communications.
- Oversight.

Along with a review of ISO 37301 Compliance Risk Management Systems Standard and discussion on other frameworks such as the United States DOJ Guidance on the Evaluation of Corporate Compliance Programs.

Why Comply?

- Building organisational resilience.
- Surviving in challenging times and environments.
- Developing our organisations role in wider society
- Building trust and displaying integrity.
- Creating an inclusive and respectful culture.

All factors which go to building an enduring organisation.



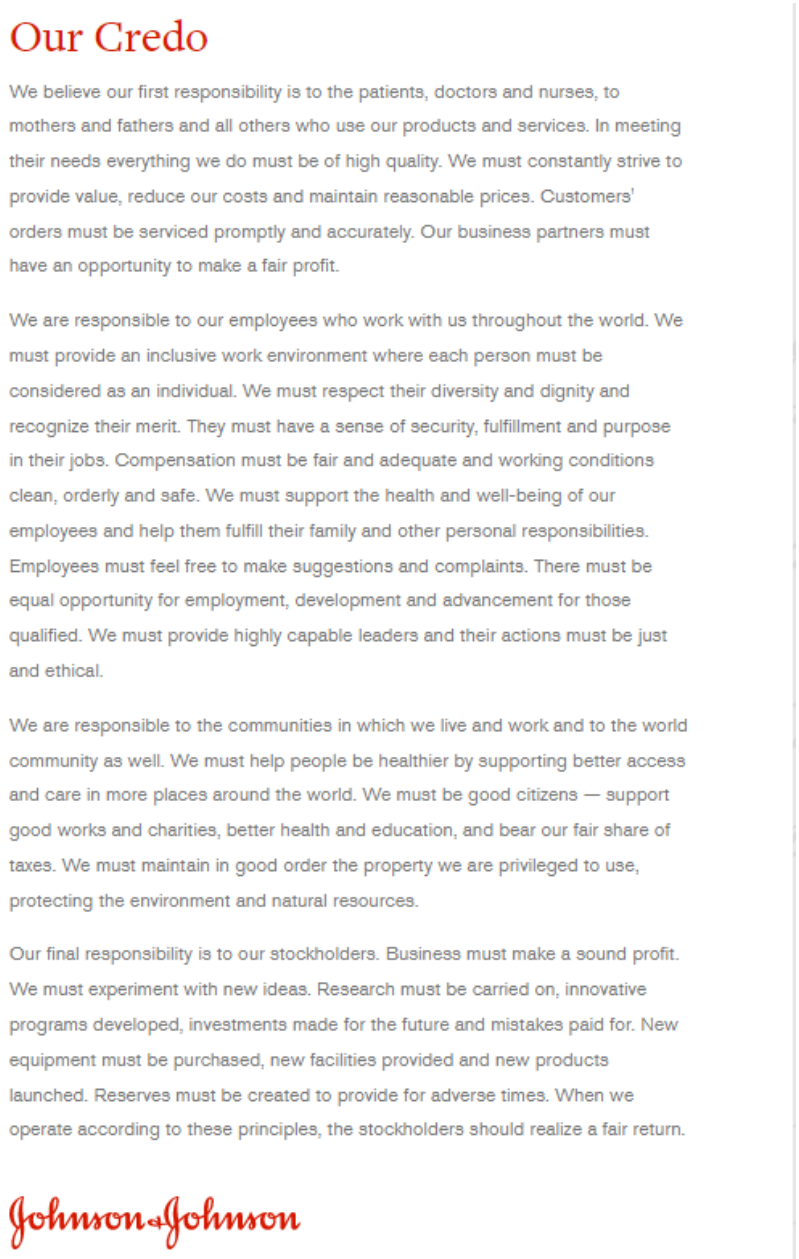
Stakeholders

Examples of external interested parties include:

- governments and government agencies;
- regulatory bodies;
- customers;
- contractors;
- suppliers;
- third-party intermediaries;
- owners, shareholders and investors;
- non-governmental organisations;
- society and community groups;
- business associates.

1943 Credo by R.W. Johnson Jnr

https://www.jnj.com/credo/



Our Credo

We believe our first responsibility is to the patients, doctors and nurses, to mothers and fathers and all others who use our products and services. In meeting their needs everything we do must be of high quality. We must constantly strive to provide value, reduce our costs and maintain reasonable prices. Customers' orders must be serviced promptly and accurately. Our business partners must have an opportunity to make a fair profit.

We are responsible to our employees who work with us throughout the world. We must provide an inclusive work environment where each person must be considered as an individual. We must respect their diversity and dignity and recognize their merit. They must have a sense of security, fulfillment and purpose in their jobs. Compensation must be fair and adequate and working conditions clean, orderly and safe. We must support the health and well-being of our employees and help them fulfill their family and other personal responsibilities. Employees must feel free to make suggestions and complaints. There must be equal opportunity for employment, development and advancement for those qualified. We must provide highly capable leaders and their actions must be just and ethical.

We are responsible to the communities in which we live and work and to the world community as well. We must help people be healthier by supporting better access and care in more places around the world. We must be good citizens — support good works and charities, better health and education, and bear our fair share of taxes. We must maintain in good order the property we are privileged to use, protecting the environment and natural resources.

Our final responsibility is to our stockholders. Business must make a sound profit. We must experiment with new ideas. Research must be carried on, innovative programs developed, investments made for the future and mistakes paid for. New equipment must be purchased, new facilities provided and new products launched. Reserves must be created to provide for adverse times. When we operate according to these principles, the stockholders should realize a fair return.

Johnson & Johnson

ISO 37301

- Compliance is an ongoing process and the outcome of an organisation meeting its obligations.

- Compliance is made sustainable by embedding it in the culture of the organisation and in the behaviour and attitude of people working for it.

- While maintaining its independence, it is preferable that compliance management is integrated with the organisation’s other management processes and its operational requirements and procedures

ISO 37301

One of the objectives of this standard is to assist organisations to develop and spread a positive culture of compliance, considering that an effective and sound management of compliance-related risks should be regarded as an opportunity to pursue and take, due to the several benefits that it provides to the organisation such as:

- improving business opportunities and sustainability;
- protecting and enhancing an organisation's reputation and credibility;
- taking into account expectations of interested parties;
- demonstrating an organisation's commitment to managing its compliance risks effectively and efficiently;
- increasing the confidence of third parties in the organisation's capacity to achieve sustained success;
- minimising the risk of a contravention occurring with the attendant costs and reputational damage

ISO 37301 vs ISO 19600

Elements of a Compliance Management System

The main and the most important difference between these two standards is that ISO 19600 provides only recommendations, as opposed to ISO 37301 which provides requirements for the implementation of a compliance management system.

Therefore, with the new standard, organisations can verify and certify their compliance program meets the standard which could offer valuable mitigation if a breach were to occur.

At this stage there are limited number of people approved to accredit this standard, but expect that to grow.

ISO 37301

A Certifiable Standard

Unlike its predecessor, ISO 37301 is a Type A standard. This means regulators and independent experts can certify the CMS of an organisation as ISO 37301 compliant. Organisations operating in high compliance risk industries may be required to maintain certification as a licence condition.

Bidders for future public projects may find calls for tenders require a certified CMS.

Other organisations may wish to obtain certification to demonstrate their competence to clients and improve their standing in the industry.

ISO 37301

Scale & Applicability – The Risk Based Approach

ISO 37301 is scalable to organisations of any size and in any industry. Organisations without a Compliance Management System (CMS) should consider the risk reduction benefits that come with ISO 37301 certification.

Organisations already aligned with ISO 19600 should update their CMS in accordance with ISO 37301 to achieve best practice.

Risk Assessments

The organisation shall identify, analyse and evaluate its compliance risks based upon a compliance risk assessment.

The organisation shall identify compliance risks by relating its compliance obligations to its activities, products, services and relevant aspects of its operations.

The organisation shall assess compliance risks related to outsourced and third-party processes.

The compliance risks shall be assessed periodically and whenever there are material changes in circumstances or organisational context.

The organisation shall retain documented information on the compliance risk assessment and on the actions to address its compliance risks.

https://arctic-intelligence.com/community/resources/aml-benchmarking-report-2022

Obligations Registers

The organisation shall systematically identify its compliance obligations resulting from its activities, products and services, and assess their impact on its operations.

The organisation shall have processes in place to:

a) identify new and changed compliance obligations to ensure ongoing compliance;
b) evaluate the impact of the identified changes and implement any necessary changes in the management of the compliance obligations.

The organisation shall maintain documented information of its compliance obligations

https://www.lexisnexis.co.nz/en/insights-and-analysis/blogs/whitepaper/complimentary-whitepaper-compliance-risk-and-iso-37301-reshaping-compliance-management

Whistleblowing

The new standard requires organisations to encourage whistleblowing.

Organisations must have formal systems that enable staff and other stakeholders to report their concerns easily, that protect reporters from retaliation, and that ensure the confidentiality of reports.

Checklist

1. **Commitment From Management**
2. **Ongoing Review and Evaluation**
3. **Policy Established in Consultation**
4. **Information and Training**
5. **Clearly Stepped out Processes**
6. **Multiple Reporting Times and Means**
7. **Anonymity and Confidentiality**
8. **Skills, Experience and Qualifications of External Party Receiving Report**
9. **Protection and Support Against Retaliation**
10. **Consequences of Misconduct Spelt Out**
11. **Key Roles & Responsibilities**
12. **Reportable Conduct Defined**

Whistleblowing & Culture

Elizabeth Holmes was facing up to 20 years in prison for misleading investors about the progress her once-heralded start-up, Theranos, was making with new blood-testing methods.

Former Theranos lab director Adam Rosendorff has spoken of the cult like culture and insistence on loyalty during his time there. His decision to blow the whistle was based on the risk posed to people's health by the fake blood testing.

However, the case was almost derailed when Rosendorff attempted to speak with Holmes prior to her sentencing. He felt guilty that his actions had left her children without a mother.
Holmes was sentenced to 11 years in jail.

Tailored Training

- What training have employees in relevant control functions received?
- Has the company provided tailored training for high-risk and control employees, including training that addresses risks in the area where the misconduct occurred?
- Have supervisory employees received different or supplementary training?
- **What analysis has the company undertaken to determine who should be trained and on what subjects?**

ISO 37301 Training

The Organisation shall provide relevant personnel with training on a regular basis, from the time of commencement of employment and at planned intervals determined by the Organisation.

Training shall be:

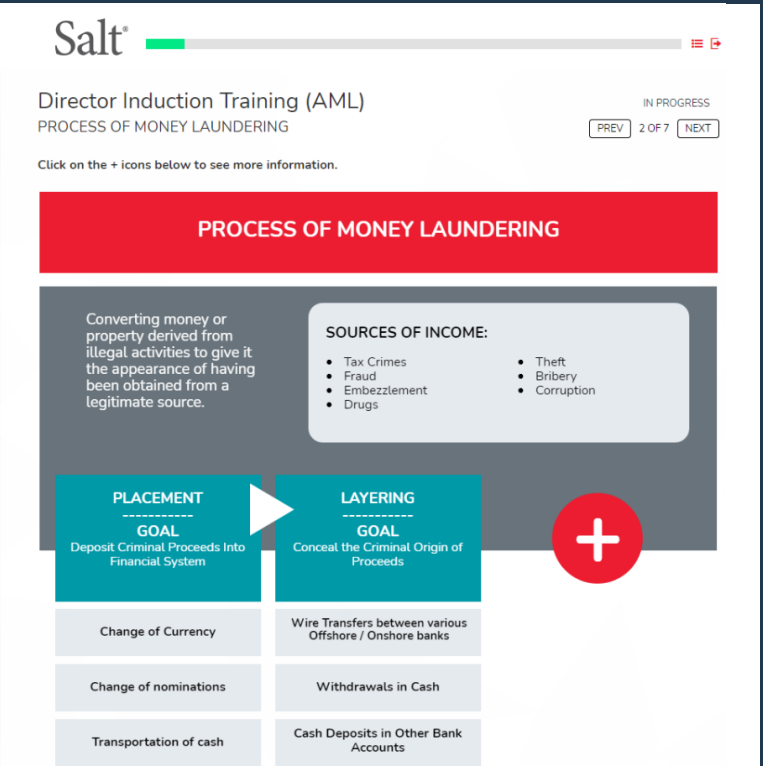
a) appropriate to the roles of personnel and the compliance risks to which personnel are exposed;
b) assessed for effectiveness;
c) reviewed regularly.

Taking into account the compliance risks identified, the Organisation shall ensure procedures are implemented to address compliance awareness and training for third parties who act on its behalf and who can pose a compliance risk to the Organisation.

Training records shall be retained as documented information

Customisation at Scale

Regulators Want Training to be Relevant, Risk Based & Up to Date*



Modular Training

Courses are developed as a group of modules

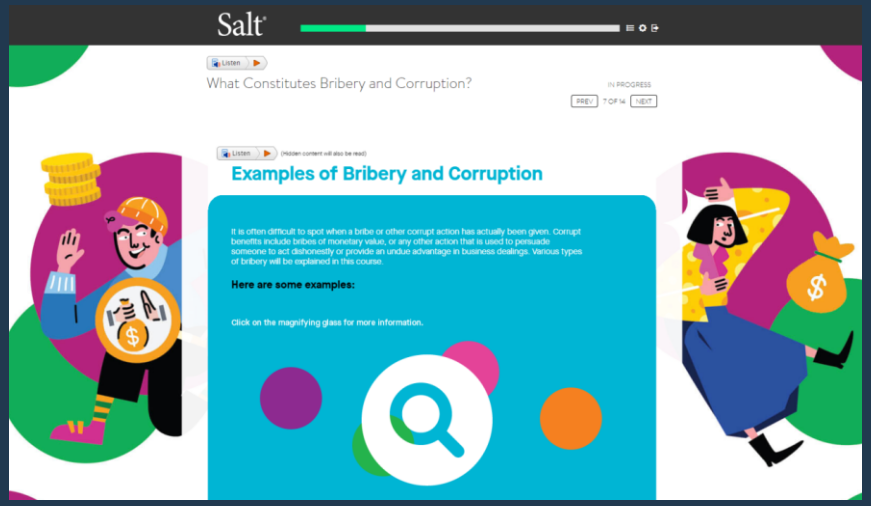
Allocated by line of business, job role, jurisdiction

Course Skinning

Courses can be branded without affecting the content

Course Cloning

Multiple versions of a course can be quickly and easily developed



Centralised maintenance

Ensures ease of updating

Audit Trail

Tracks all changes across all versions

*https://www.justice.gov/criminal-fraud/page/file/937501/download

ISO 37301 Communication

The Organisation shall determine the internal and external communications relevant to the compliance management system, including:

a) on what it will communicate;
b) when to communicate;
c) with whom to communicate;
d) how to communicate.

ISO 37301 Awareness

Persons doing work under the Organisation's control shall be aware of:

- the compliance policy;
- their contribution to the effectiveness of the compliance management system, including the benefits of improved compliance performance;
- the implications of not conforming with the compliance management system requirements;
- the means of and procedures for raising compliance concerns;
- the relation of the compliance policy and the compliance obligations relevant to their role;
- the importance of supporting compliance culture.

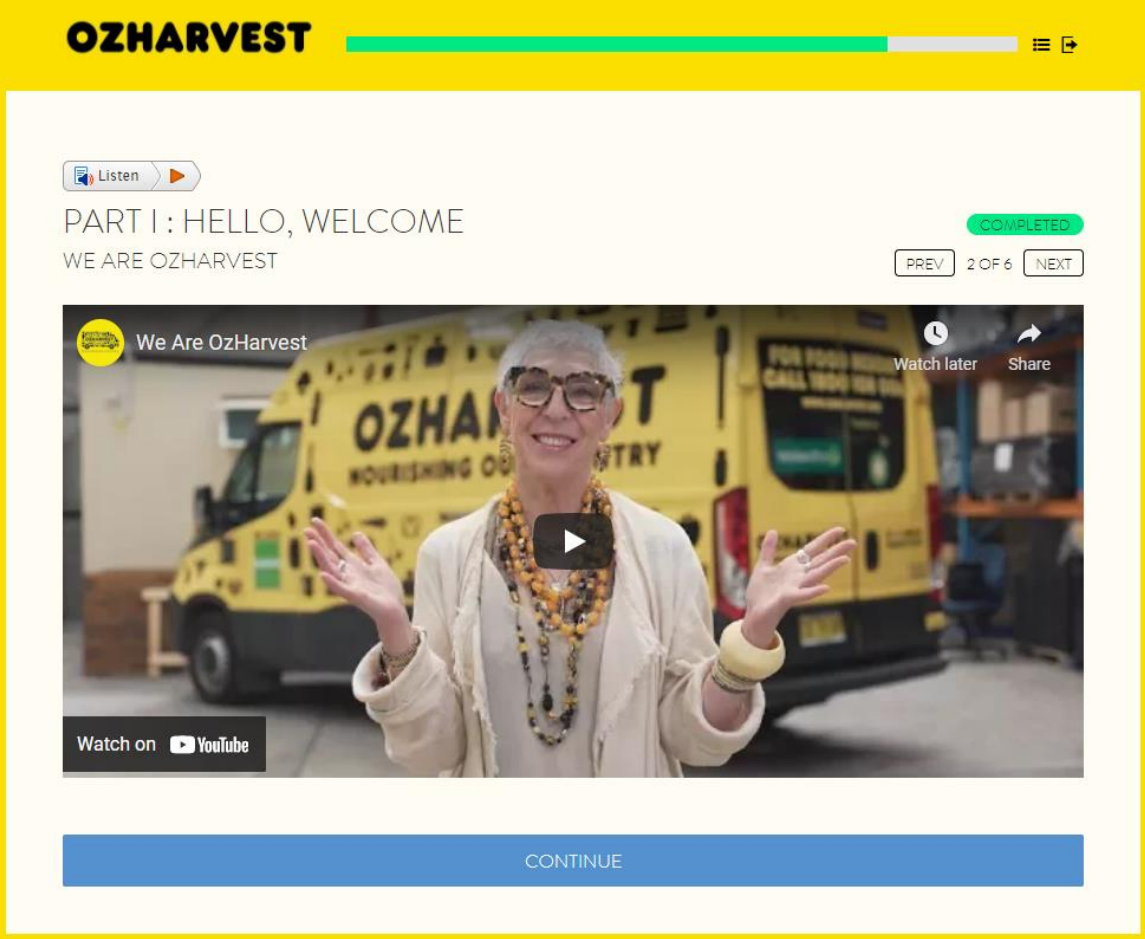
Evaluation of Corporate Compliance Programs – US DOJ

Communications about Misconduct

What has senior management done to let employees know the company's position concerning misconduct?

What communications have there been generally when an employee is terminated or otherwise disciplined for failure to comply with the company's policies, procedures, and controls?

Corporate Communications



Corporate communications are a vital part of setting organisational culture and ensuring people feel part of the team.

It’s important to get the message right and to ensure that staff have received and understood that message.

Reporting gives detailed analytics on who saw what when, for how long, and which questions they answered correctly & incorrectly.

Evaluation of Corporate Compliance Programs – US DOJ

GRC solutions

Availability of Guidance

What resources have been available to employees to provide guidance relating to compliance policies?

How has the company assessed whether its employees know when to seek advice and whether they would be willing to do so?

How has the organisation assessed comprehension of policies?

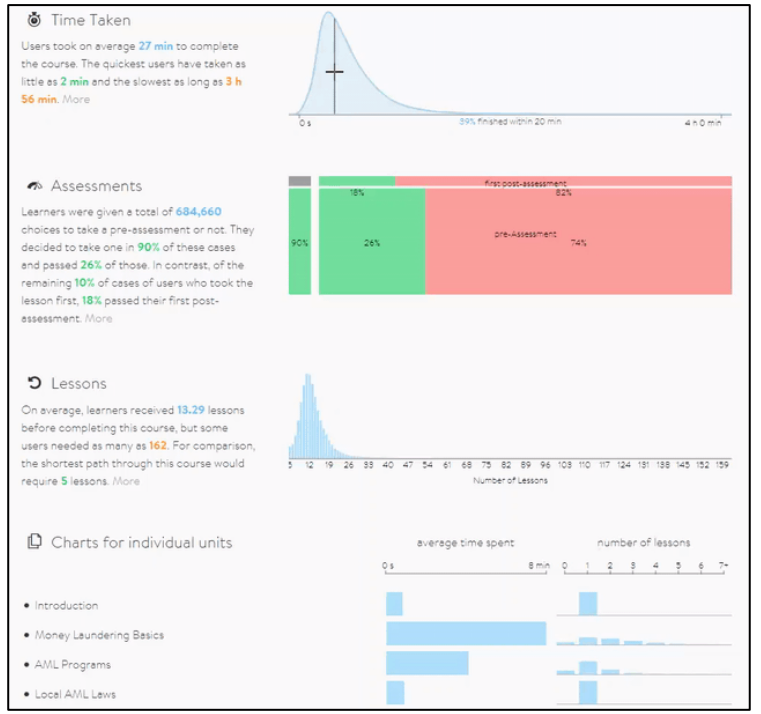
How is the organisation communicating changes in policy & regulation?

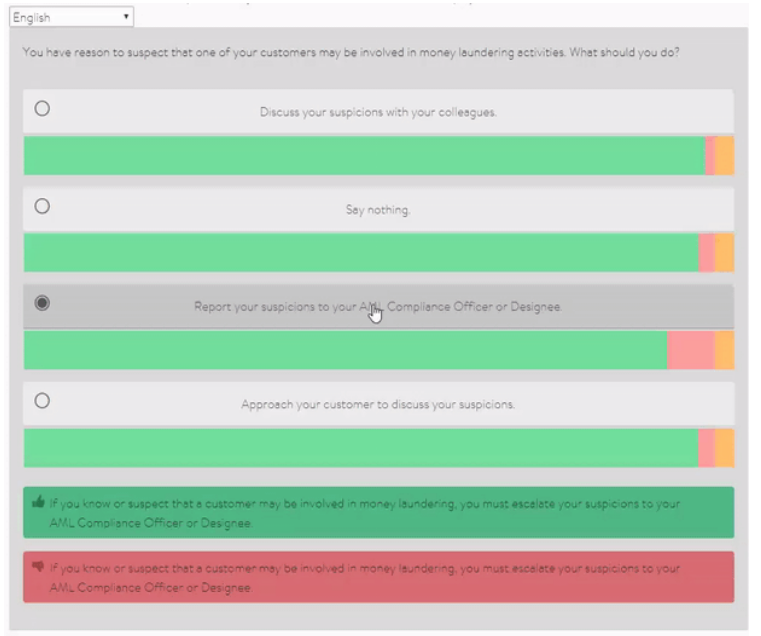
Effectiveness of Training

- Has the training been offered in the form and language appropriate for the audience?
- Is the training provided online or in person (or both), and what is the company's rationale for its choice?
- Has the training addressed lessons learned from prior compliance incidents?
- Whether online or in person, is there a process by which employees can ask questions arising out of the trainings?
- How has the company measured the effectiveness of the training?
- **Have employees been tested on what they have learned? How has the company address employees who fail all or a portion of the testing?**
- **Has the company evaluated the extent to which the training has impacted performance?**

Deep Data Analytics

- Use time taken data to evidence ROI & review outliers for remedial attention. Review lesson & assessment performance
- Deep dive into lessons to understand systemic issues & predict compliance risks
- Multi-lingual question analysis ensures homogeneous reporting across translations
- Use data to locate systemic issues & common errors or misunderstandings
- Promote deeper & more advanced learning





Organisational Culture & Leadership

Factors that will support the development of a compliance culture can include:

- A clear set of published values;
- Management actively and visibly implementing and abiding by the values;
- Consistency in the treatment of non-compliance, regardless of position;
- Mentoring, coaching and leading by example;
- An appropriate pre-employment assessment of potential personnel for critical functions including due diligence;
- An induction or orientation programme that emphasises compliance and the organisation's values;

Organisational Culture & Leadership

- Ongoing compliance training, including updates to the training to all personnel and relevant interested parties;
- Ongoing communication on compliance issues;
- Performance appraisal systems that consider the assessment of compliance behaviour and take into account performance pay to achieve compliance key performance measures and outcomes;
- A visible recognition of achievements in compliance management and outcomes;
- Prompt and proportionate disciplining in the case of wilful or negligent violations of compliance obligations;
- A clear link between the organisation's strategy and individual roles, emphasising compliance as essential to achieving organisational outcomes;
- **Open and appropriate communication about compliance, internally and externally**

ISO 37301

Compliance Governance

The new standard places increased emphasis on the role of managers at all levels in ensuring compliance. Organisations seeking certification must apply a management structure designed to promote compliance and define the roles and responsibilities of managers in a clear and transparent manner.

Management Accountability Regimes

The DOJ has increased its focus on accountability. In a recent speech, Deputy attorney general Lisa O. Monaco indicated that **“the Department’s number one priority is individual accountability…***

UK SMCR

UK financial services firms are regulated by the Financial Conduct Authority (FCA), and sometimes the Prudential Regulation Authority (PRA) too.

Individual accountability regimes focus on the people who manage these firms, ensuring they are fit and proper to do their jobs.

*https://fcpablog.com/2022/10/31/reframing-accountability-to-meet-the-new-doj-guidance/

Management Accountability Regimes

Australia – BEAR / FAR

The Banking Executive Accountability Regime (BEAR) applies to Authorised Deposit-taking Institutions (ADIs) in Australia. The Financial Accountability Regime (FAR) Bill 2022 was introduced into Parliament on 8 September 2022. ASIC will join APRA as a co-regulator under FAR, and FAR will replace the BEAR requirements and make a number of changes, including:

- Applying to all APRA-regulated entities, including insurers, RSE licensees, Non-Operating Holding Companies, and later extend to apply to entities that are solely regulated by ASIC under AFSLs and ACLs;
- Extending the obligations under FAR to apply to the accountable entities' subsidiaries and significant related;
- Introducing new responsibilities that will need to be allocated to senior executives as well as specific responsibilities to be allocated dependent on the type of entity; and
- There will be a corresponding focus on conduct such as through new accountability obligations like taking reasonable steps to prevent matters that would (or would be likely to) result in a material contravention of specified laws (including "financial services law" as defined in the Corporations Act).

Organisational Culture & Leadership

GRC solutions

The standard you walk past is the standard you accept!

Chief of the Army,
Lieutenant-General
David Morrison

https://www.youtube.com/watch?v=azbRhVCt8Rw

Questions?

Reach out to us for your compliance training requirements!

Sydney, Melbourne, Perth, Brisbane, Singapore and New York

contactus@grcsolutions.com.au | grcsolutions.com.au | saltlearning.com

RiskNZ

Thank you for joining us today