encompass
the full picture, fast

EBOOK

the **digital KYC** model

why **regtech** is vital for **Australian regulated firms**

encompasscorporation.com

contents

The Hayne Royal Commission is engendering increased regulatory activity, while Australian financial institutions' management of their regulatory responsibilities continues to generate media coverage.

Industry insiders observe that a resetting of institutions' commitment to Know Your Customer (KYC) as a means of guarding the national economy against the corrosive effects of financial crime will lead to much-needed modernisation of business operating models.

Australian institutions can accelerate their own transformations and achieve world-class KYC operations by learning from the experiences of their peers in Europe, particularly the UK. While every component of the KYC operating model demands attention, putting people at the centre of this modernisation will reap the greatest benefits.

> a modern KYC operating model augments the KYC experts already in place, with a business process that starts with a clear definition of policy and spans business, compliance and audit professionals organised as three lines of defence.

When faced with increasingly stringent anti-money laundering (AML) regulations, many UK institutions initially attempted to bolster out-dated business processes by hiring ever-larger teams of KYC professionals. A shortage of KYC skills in the local market closes this avenue to Australian institutions. While the largest Australian banks are hiring and relocating experts from London, global competition for these resources drives the cost of importing expertise and experience beyond many tier 2 financial institutions.

A modern KYC operating model augments the KYC experts already in place, with a business process that starts with a clear definition of policy and spans business, compliance and audit professionals organised as three lines of defence.

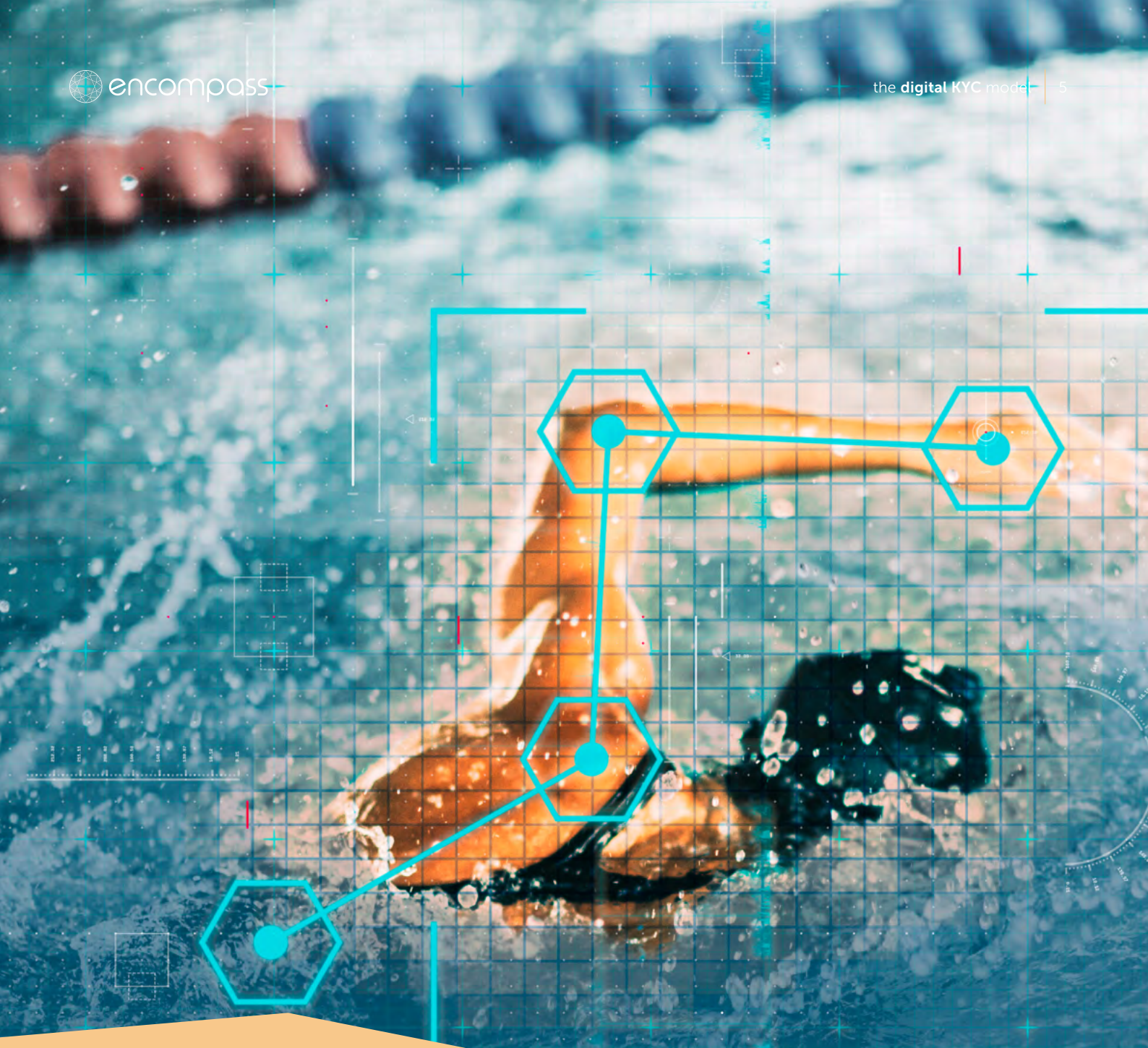
The work of these professionals is underpinned by a digital system capable of collecting and analysing data from multiple global sources to create a digital profile of each customer that persists through the lifetime of the business relationship to support informed decision-making by compliance professionals.

In *Transforming Risk Efficiency and Effectiveness*, McKinsey & Company report that a "well-executed, end-to-end risk-function transformation can decrease costs by up to 20 percent while improving transparency, accountability, and employee and customer experience".

Overseas institutions that have digitally transformed their KYC operating model improve governance, reduce their cost of operations by radically improving work efficiency, lift the morale and commitment of their compliance professionals, and deliver a better experience to customers by limiting requests for information and clarification.

With sound strategy and rigorous execution, Australian institutions can

- create modern KYC operating models that minimise the risk of regulatory intervention, on-site inspections and enforcement actions
- optimise investments in data and technology
- accelerate opportunities for growing revenues



KYC from an Australian regulatory perspective

The Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry has brought broad political, community and media attention to Australia's banking sector.

As licence holders under the Banking Act 1959, Australian banks are subject to stringent regulations including the Anti-Money Laundering and Counter-Terrorism Financing Act 2006. This legislation obliges Banks to assume a primary role in protecting the Australian economy from financial crime.

Under the *Banking Act 1959*, and also the *Insurance Act 1973* and the *Life Insurance Act 1995*, the Australian Prudential Regulation Authority (APRA) made Prudential Standard CPS 220 Risk Management. This states:

> This Prudential Standard requires an APRA-regulated institution and a Head of a group to have systems for identifying, measuring, evaluating, monitoring, reporting, and controlling or mitigating material risks that may affect its ability, or the ability of the group it heads, to meet its obligations to depositors and/or policyholders. These systems, together with the structures, policies, processes and people supporting them, comprise an institution's or group's risk management framework.

The work of KYC necessary to undertake due diligence compatible with an institution's AML obligations falls within this risk management framework.

On 8 January 2020, the Australian Financial Review reported that APRA "described the risk and compliance functions of the nation's largest financial institutions as in need of urgent overhaul". Chairman Wayne Byres warned that "institutions found wanting could expect significant penalties". In 2020 APRA will introduce reforms to CPS 220 "aimed at lifting governance, culture, risk and accountability standards to a world-leading standard". These reforms will apply to all institutions holding licences under the *Banking Act 1959*.

the **traditional approach** to **KYC operations**

Traditional KYC operations rely on a process that combines manual tasks with electronic communications.

A fundamental challenge with manual operations is ensuring adherence with an institution's policies. A KYC policy is a written statement of how an institution will operate its business to remain within limits of the risk appetite established by its Board. At the level of KYC operations a policy can be understood as a sequence of business rules. In pre-digital operations, interactions between KYC policies and compliance professionals can be categorised as interpretative, and it is not uncommon to find inconsistent and incomplete application of policy, particularly in institutions with different teams responsible for initial onboarding, ongoing customer due diligence and remediation driven by changing regulations. Any gap between a policy's intent and its implementation can present operational risk; breaches also damage the effectiveness of business operations.

any gap between a policy's intent and its implementation can present operational risk; breaches also damage the effectiveness of business operations.

The work of KYC stalls in situations when client-facing staff collect and pass-on an insufficient or incomplete document set to their colleagues in the compliance team. Client-facing staff must now reach out to recontact the prospective customer. Repetitive client outreach is frustrating to both the client and business professionals and delays onboarding. A common scenario is for client service professionals to attach copies of identification documents to an email sent to the Compliance team and for these documents to be used to drive due diligence following corporate policy. While this can be made to work, it lacks a control infrastructure to enforce individual responsibility and accountability and to ensure coordination across departments.

KYC professionals undertaking customer due diligence work with multiple independent sources of information that reside outside of their institutions. Analysts typically download documents as files in PDF or as screen grabs from websites and, once they have completed their due diligence, pass these along the chain of work either as attachments to emails or as links referencing documents stored on shared drives.

Sharing electronic files means KYC professionals must re-interpret work already completed by colleagues to understand the current state of customer due diligence - this is particularly true whenever work is handed off between individuals and across teams. This can be challenging for internal auditors responsible for providing independent assurance that the institution's risk management and internal control processes are operating effectively. These inefficiencies have the potential to create gaps in an institution's defence against money laundering.

The work of KYC operations is itself challenging. When companies employ deep structures which span national boundaries, KYC analysts must "pull on a thread" to follow a chain of ownership by accessing different sources of information. Even experienced analysts miss details and these human errors are sources of operational risk. It is common practice for the emerging structure to be captured in a graphics package or spreadsheet, both of which prove inefficient ways of working. This situation is exacerbated when analysts uncover that a beneficial owner is also a politically exposed person (PEP). The work of screening for news of PEPs using search engines generates enormous volumes of false positives creating days of futile work and introducing the risk of distraction from real news of material interest.

innovating with a **digital KYC operating model**

The experience from overseas is that in the face of increasingly stringent regulation such as that foreshadowed by APRA, institutions first instinct is to hire more professionals to operate existing manual KYC processes.

Taking this route has proven to be an expensive way to reach a dead-end. In 2017, McKinsey & Company reported "in the United States, anti–money laundering (AML) compliance staff have increased up to tenfold at major banks over the past five years or so". It is unlikely that Australian institutions will take this approach as a shortage of KYC professionals in the local market has already forced one of the major banks to hire senior staff from London.

The way forward is to embrace a digital KYC operating model and to integrate this innovation with a bank's wider digital transformation program. Taking this approach can unearth opportunities to use data collected in due diligence in other functions such as sales and customer service. The key to success is to put people at the centre and to consider how each component of a KYC operating model can best support and augment the work of these professionals.

> well-executed,end-to-end risk-function transformation can decrease costs by up to 20% while improving transparency, accountability, and employee and customer experience.
>
> McKinsey & Company
> Transforming Risk Efficiency and Effectiveness

people
in a **digital KYC operating model**

Authorities including the Institute of Internal Auditors Australia, the Office of the Comptroller of the Currency within the United States Department of the Treasury and the UK's Chartered Institute of Internal Audit recommend that institutions align the people within their risk management system as three lines of defence.

> organising as three lines of defence proves effective at galvanising professionals in different roles across multiple departments to focus their attention on managing risk

The first line of defence is formed typically of customer-facing staff such as client relationship managers in a financial institution. The second line of defence is commonly the compliance function, responsible for setting policies and KYC operations, while internal audit forms the third line of defence.

This alignment ensures that each person develops a clear understanding of their individual and collective responsibilities and accountabilities for assessing, controlling and mitigating AML risks and recognise when they should interact with professionals in other teams within the broader risk management framework. Organising as three lines of defence proves effective at galvanising professionals in different roles across multiple departments to focus their attention on managing risk and allows for clear communications to the executive team and the institution's board.

people and **policies**
in a **digital KYC operating model**

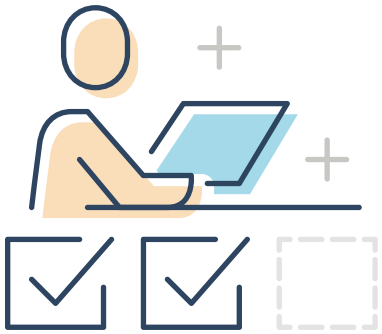
A KYC policy is a written statement of how an institution will operate its business to remain within limits of the risk appetite established by its Board. When applied to KYC operations, a policy can be understood as a sequence of business rules.

Unlike manual KYC where KYC policies are interpretative and potential sources of inconsistencies and operational risk, in a digital KYC operating model KYC policies are rendered in a machine-readable form. This makes policies declarative; the policy definition serves as a digital instruction set controlling software responsible for searching and analysing information necessary in customer due diligence.

KYC due diligence outcomes are now binary. Either KYC operations complete with absolute consistency or they stall before completion. When they stall, their incomplete status is brought to the attention of human experts to complete a task and then control is passed back to software to complete due diligence consistent with the policy's definition. This digital transformation greatly increases the effectiveness of KYC.

people and **process** in a **digital KYC operating model**

Modern KYC establishes a digital process with a formal workflow across all three lines of defence. Customer-facing staff in the first line of defence use their time with clients to collect documents necessary for identification and verification. Document images routed to KYC operations in the second line of defence drive a digital policy which automates the collection, analysis and integration of information from third party sources to generate a risk score. All activity including information collected and the person responsible for each task is securely logged to simplify the work of internal auditors in the third line of defence.



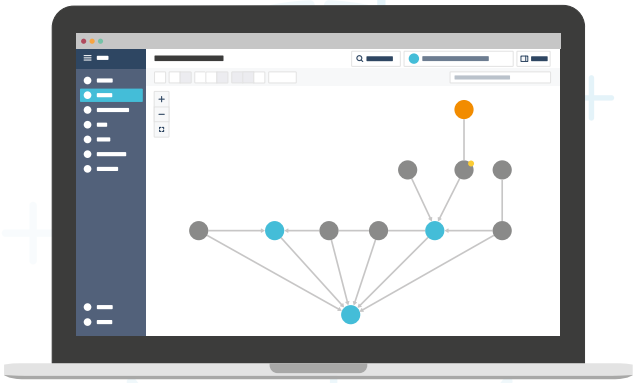
people and **information systems** in a **digital KYC operating model**

To complete their due diligence KYC professionals must work with multiple external sources of information such as company registers and business information aggregators. These sources are increasingly open to digital operations via application programming interfaces (APIs). This global information ecosystem is the "digital outside".

With digital KYC banks create a "digital inside" capable of connecting to third-party systems in real time, interrogating their contents and streaming data directly to digital workflows. KYC analysts undertaking due diligence create a digital profile for each client, and this rolling record persists through multiple cycles of refresh and remediation for the lifetime of the business relationship. This digital profile allows compliance professionals to focus on the real value they bring to banking: making consistent, high quality and informed decisions on the risks that each customer poses to their institution.

Encompass
your partner in
successful digital KYC

With an exclusive focus on regtech, **Encompass** is the natural choice for financial institutions looking to modernise and digitise KYC operations.



Banks expect fast return-on-investment for their digital transformation initiatives. Cloud-native and delivered as SaaS, Encompass allows for fast implementation with typical payback periods measured in months, not years.

Justifiably cautious that digital KYC with Encompass is better and faster KYC, institutions will typically compare the results of business-as-usual with a new digital approach. As this executive exclaimed "Encompass performed 5 times more searches, saved 6 times the number of documents, identified 5 times more connected parties, all within 16% of the time it took the bank's analysts". Digital KYC delivers other benefits; banks find they can remediate client profiles without outreach to customers, and this frictionless business improves client experience.

Many banks want to take advantage of new technology with minimum disruption to their own operations. These enterprises want to own their client-side applications which are used by employees to get work done and retain control over their workflows and their user interfaces. Encompass offer their customers a choice: either interact via a predefined user interface that we supply, or consume the services of our digital KYC platform via an API and integrate these into your workflows with your preferred user interface. An advantage of this flexibility is that banks generate immediate value by adopting new digital process designs while using the web interface, and then over time move to an API-based implementation with the interface of their choice.

By necessity, banking regulations must change to stay relevant as the wider business environment evolves. APRA recently flagged its intent to modify Prudential Standard CPS 220. Digital instruction sets created within Encompass to enforce each institution's KYC policies are simply modified, giving our customers the agility they need to remain compliant as regulations change.

McKinsey & Company's *Transforming Risk Efficiency and Effectiveness* report identifies 19 risk processes as candidates for automation and notes the opportunity to reduce costs by up to 20% while improving transparency, accountability, and employee and customer experience.

The report highlights Bank Secrecy Act and AML operations as having the highest automation feasibility as these operations yield both the highest effectiveness and the highest efficiency impacts. Returns from digitising AML operations are likely to be far higher than 20%, and KYC is a propitious starting point for digital transformation within a bank's risk function.

With an unrivalled reputation as a partner to banks undertaking digital transformation of their KYC operations, Encompass welcomes the opportunity to work with Australian banks.

> the way forward is to embrace a digital KYC operating model and to integrate this innovation with a bank's wider digital transformation program.

about **Encompass**

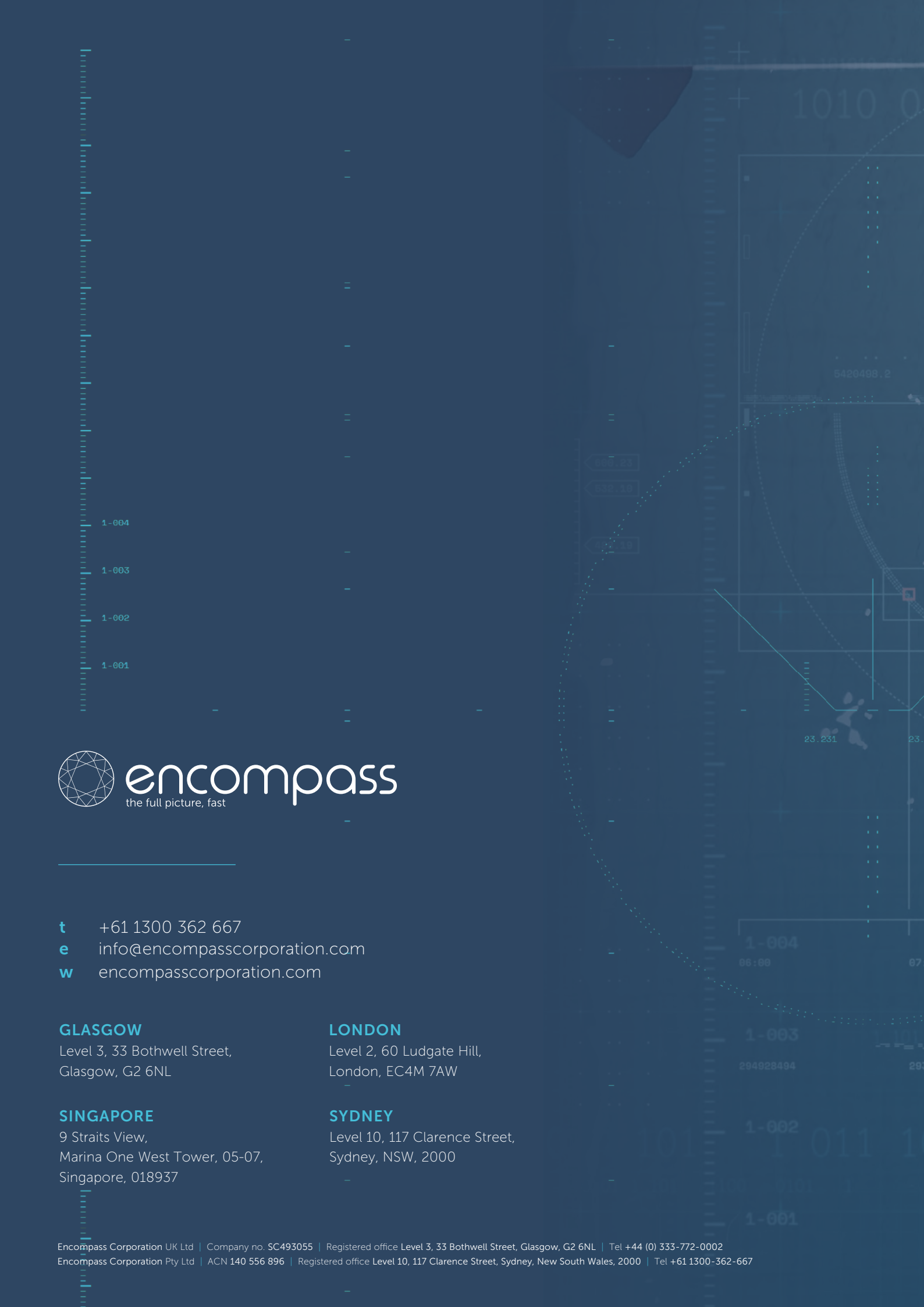
Encompass automates information and news discovery for KYC requirements for client onboarding, event-driven refresh and remediation.

encompass
the full picture, fast

Driven by your internal policies and choice of reliable, independent sources, Encompass constructs corporate ownership, discovers beneficial owners, and comprehensively screens entities and persons for risk.

Our advanced intelligent process automation dynamically builds a comprehensive KYC profile from multiple sources, including corporate registries, company and regulatory data, adverse media and identity verification - enabling fast, confident decisions. Incorporating leading biometric and eIDV sources for individual KYC verification, Encompass delivers a single platform to manage every type of customer.

Find out more at **encompass**corporation.com.



encompass
the full picture, fast

t +61 1300 362 667
e info@encompasscorporation.com
w encompasscorporation.com

GLASGOW
Level 3, 33 Bothwell Street,
Glasgow, G2 6NL

LONDON
Level 2, 60 Ludgate Hill,
London, EC4M 7AW

SINGAPORE
9 Straits View,
Marina One West Tower, 05-07,
Singapore, 018937

SYDNEY
Level 10, 117 Clarence Street,
Sydney, NSW, 2000

Encompass Corporation UK Ltd | Company no. SC493055 | Registered office Level 3, 33 Bothwell Street, Glasgow, G2 6NL | Tel +44 (0) 333-772-0002
Encompass Corporation Pty Ltd | ACN 140 556 896 | Registered office Level 10, 117 Clarence Street, Sydney, New South Wales, 2000 | Tel +61 1300-362-667