KNOWING YOUR EMPLOYEES OR ‘PERSONNEL’ - THE POTENTIAL ML/TF (AND NOW, PF) RISKS AND THE OPERATION OF YOUR EMPLOYEE DUE DILIGENCE PROGRAM

One area of inquiry seen from both current and future reporting entities concerns how to address employee due diligence obligations and the potential ML/TF/PF risks presented by roles within reporting entities.

Specifically:

“How should I approach the potential ML/TF/PF risks that the roles I hire (and the persons in them) might present to my organisation? How should my employee due diligence program operate and what should I include in it?”

Often, entities may have taken a ‘blanketed’ approach to roles across their organisations (‘everyone gets treated the same’). This has the potential to generate inefficiencies and direct valuable resources away from the persons that should be the subject of greater inquiry.

As entities are renewing their risk assessments this year, we are seeing many contemplate whether they can better allocate their resources to focus on the medium to higher ML/TF/PF risk roles under their Employee Due Diligence Program (**EDD Program**).

Entities are also asking the right questions about whether there is any duplication in the work conducted:

- where using external hiring firms, and whether they can work together (subject to privacy requirements) to obtain this information from the potential hire (or transferor) efficiently; and/or
- where information about employees is obtained and held for the purposes of other regulatory requirements, and how this information might be applied for EDD Program purposes.

When collecting information from potential and actual employees, all reporting entities should obtain legal advice on their compliance obligations under Australia's privacy laws, and ensure that they obtain all relevant consents from applicants around the collection and sharing of personal information.

WHAT DOES AUSTRAC SAY?

AUSTRAC provides helpful guidance on what reporting entities must have in place in their Employee[1] Due Diligence Programs (see here).

AUSTRAC makes clear that reporting entities must have an EDD Program that sets out how the entity screens and rescreens its employees and contractors for ML/TF/PF Risks.

Screening means the business must check:

- the background of the proposed employee (**Applicant**) to determine whether he/she is suitable for the role;
- that the Applicant is who they say they are,
- the Applicant passes whatever probity requirements the business requires (for instance, gaming companies may require additional probity information for Applicants entering particular gaming roles); and
- the information provided by the Applicant is true and correct.

AUSTRAC also makes clear that the requirements of the AML/CTF Act and Rules is **risk-based**, and that "***you should tailor your EDD requirements to meet your specific circumstances including your senior management and/or board-approved risk appetite.***"

[1] Note that AUSTRAC, in its latest industry kits, refers to 'employees' as 'personnel' so these terms are used interchangeably here.

HOW DO YOU TAILOR IT TO YOUR CIRCUMSTANCES?
… CONDUCT A REVIEW OF THE ML/TF/PF RISKS EACH OF YOUR ROLES PRESENT, ASKING YOURSELF SENSIBLE QUESTIONS ABOUT WHERE THE RISK(S) MIGHT LIE

When conducting your annual enterprise-wide risk assessment, it is prudent to include the **ML/TF/PF risks presented by the roles you hire**, alongside your assessment of the ML/TF/PF Risks presented by your customers, your products/services, your channels and your jurisdictional risks

When considering the risks associated with your roles, you may consider documenting the following details across each role in your business:

- Role Title
- Job Description (and when that JD was last reviewed)
- Line Manager
- Business Unit (where applicable)
- Role Categorisation (e.g. front or back of house, management, services, Board)
- Tenure (permanent, contract for short/medium/long term)
- Number of Persons Employed In Role
- Compliance, Fraud or Predicate Crime History in respect of Role (has this role position caused you issues previously?)
- Role Risk Level (if available - is this role designated high risk for another reason by the business?)
- Casualisation / Turnover of Role
- Role as second form of employment
- Level of customer interaction
- Level of cash interaction (where applicable)
- Level of System / IT interaction

You should then consider looking at your ML/TF/PF Risk assessment on your customers, products and services, channels and jurisdiction and tailoring EDD questions relevant to the ML/TF/PF Risks (and the assessment criteria or scoring you used) you have identified. Think of this as 'focusing in' on those areas that might elevate the risk that the role could be in a position to be susceptible to bad actors.

For instance, some questions you might ask are:

- Is the role involved in customer due diligence procedures?
- Is the role able to download customer information from business systems?
- Is the role involved in making payments to customers for any designated services?
- Is the role involved back of house in releasing payments to customers for any designated services?

- Does this role engage with actual or potential high risk customers (for example, is the role involved in any VIP or other form of loyalty program)?
- Can the role determine to cease doing business with a customer?
- Can the role override AML/CTF controls in any business systems?
- Is the role involved in the chain of reporting of potentially unusual activity to the AMLCO?
- Does the role install or otherwise interact with products or services that you provide to customers?
- Is the role involved - directly or indirectly - in any key controls implemented by the business (for instance the Transaction Monitoring Program, IT, security, surveillance)?

This list is by no means exhaustive and as you think through the potential risks and typologies presented by your business, questions about the potential role and susceptibility of persons in it will become apparent.

WHAT WILL CONSTITUTE A LOW, MEDIUM AND HIGH RISK ROLE?

Having completed the assessment above, you will now be in a position to see whether a role presents a low, medium or high risk to your business.

It is recommended that you clearly set out in your risk assessment the definition of a low, medium or high ML/TF/PF risk in the context of the employee role review.

WHAT ABOUT YOUR 'GOVERNANCE' ROLES SPECIFICALLY?

Your AML/CTF governance roles - including your AML/CTF compliance officer, senior manager and governing body - require a higher level of scrutiny than your standard role risk assessment may capture.

These roles carry direct responsibility for the design, implementation and oversight of your AML/CTF Program, and any compromise in the integrity or competence of these persons presents a significant risk to your business.

For the AML/CTF compliance officer role in particular:

- The Starter Kits for tranche 2 entities flag that you should ensure a national criminal history check be carried out in addition to your standard screening processes[2].
- You must also notify AUSTRAC within 14 days of appointing a new AML/CTF compliance officer.

[2] Note these Starter Kits have been released for tranche 2 entities and not for Pubs and Clubs (which have their own guidance materials). The requirement is your AML/CTF Compliance Officer needs to be 'fit and proper' - a police check will help you demonstrate / evidence this.

Your EDD Program should reflect this enhanced level of due diligence for governance roles and clearly distinguish the screening and ongoing PDD requirements (see below) that apply to them from those that apply to other AML/CTF-related roles within your business.

YOUR EMPLOYEE DUE DILIGENCE PROGRAM - REVIEW AND UPDATE

Having identified the criteria to classify roles into low, medium or high ML/TF/PF risk to your business (likely because they are involved in the customer relationship or may otherwise be a 'target' for collusion or coercion by associates of criminal groups), pull out your existing EDD Program.

Using the results of the role risk assessment, ask yourself:

- **How does the current EDD Program assist our business in mitigating / managing the risks presented by the medium and high risk roles?**
- Do we need more rigorous screening for the medium and high risk roles? (see the AUSTRAC Guidance for what this might look like, as well as a review of any enforcement action by AUSTRAC that addresses EDD for key learnings)
- Should we be asking for police checks or bankruptcy searches for high and medium risk roles and if so, why, how and when?
- Are any of these roles outsourced and if so, are we comfortable with the checks being run? Are those checks the same as the ones we run on our employees?
- **Are there any resources allocated to due diligence on low risk roles that would be better allocated to the medium and high risk roles?**
- Are there any processes or controls we have applied historically 'across the business' that, having now conducted a detailed review of the risks involved, no longer need to apply to some roles but should apply to others?

There will be other questions - like ***"how do we address due diligence on employees that might enter our business in a lower risk role, but then move to a medium or higher risk role through a promotion?"***

ONGOING DUE DILIGENCE ON YOUR PERSONNEL/STAFF (ONGOING PDD)

Your EDD Program should not be a 'set and forget' exercise. Once you have conducted your initial screening and risk assessment of a role, you need a plan for how you will reassess suitability on an ongoing basis.

AUSTRAC makes clear that ongoing personnel due diligence (**ongoing PDD**) requires you to reassess the suitability of a person for a role as soon as practicable when you identify circumstances that may impact their suitability. This applies to all persons performing AML/CTF-related roles within your business.

Ongoing PDD broadly covers two areas:

- **Integrity** - this includes statutory declarations and any self-reported changes in circumstances that may affect a person's suitability for the role.

- **Competence** - this includes performance reviews, training outcomes and observed conduct relevant to AML/CTF responsibilities.

WHAT WILL LIKELY TRIGGER ONGOING PDD?

Your EDD Program should clearly set out the circumstances that will trigger a reassessment. These triggers will vary depending on the risk level you have assigned to each role, but may include:

- a change in the person's role or responsibilities (for example, a promotion from a low risk role to a medium or high risk role, or a lateral move into a role with greater customer interaction, cash handling or system access);
- adverse findings from internal or external sources, including adverse media checks, police checks or bankruptcy searches;
- a self-disclosure by the person of a change in circumstances that may impact their suitability (for example, criminal charges, bankruptcy or conflicts of interest);
- observed conduct or behaviour that raises concerns about the person's integrity or reliability in the context of ML/TF/PF risks;
- a material change in the ML/TF/PF risk profile of the role itself (for example, the introduction of new products, services or channels that elevate the risk associated with that role);
- findings from your enterprise-wide ML/TF/PF risk assessment that change the risk rating of the role;
- outcomes from performance reviews or training assessments that indicate a person may not be meeting their AML/CTF obligations or does not understand them; and
- a direction or finding from AUSTRAC, law enforcement or another regulatory body that is relevant to the person or the role.

How would I manage this?

All personnel in AML/CTF-related roles should be required to self-report any circumstances that may impact their suitability as soon as practicable. This obligation should be clearly communicated at the time of appointment and reinforced through your training program.

For medium and high risk roles, consider whether periodic rescreening (for example, annual police checks or statutory declarations) is appropriate, rather than relying solely on trigger-based reassessment. Your risk appetite and the nature of the role should guide this decision.

Where ongoing PDD identifies that a person is no longer suitable for a role, you must take appropriate action as outlined in your EDD Program. This may include additional training, reassignment to a lower risk role or, in serious cases, removal from the role entirely.

All ongoing PDD actions, findings and outcomes should be documented and retained as part of your AML/CTF Program records. AUSTRAC requires these records to be kept for seven years after they are no longer relevant.

NON-COMPLIANCE MANAGEMENT

Your EDD Program should also include or cross-reference a documented system for managing personnel who fail to comply with your AML/CTF Program without reasonable excuse.

This is a separate consideration from ongoing PDD - a person may remain suitable for their role but still fail to follow procedures - and should set out the escalation steps your business will take, ranging from refresher training and formal warnings through to reassignment of duties or disciplinary action.

INTEGRATION WITH TRAINING PROGRAMS

Your EDD Program and your AML/CTF training plan should not operate in isolation. The risk level you assign to each role through your EDD Program should directly inform the depth, frequency and content of the training that person receives.

For example, a person in a high risk role with direct customer interaction and access to transaction monitoring systems will require more detailed and more frequent training than a person in a lower risk administrative role.

The outcomes of your training program - including assessment results, completion rates and any gaps identified - should feed back into your ongoing PDD as indicators of a person's competence and continued suitability for the role.

Where a person moves from a lower risk role to a medium or higher risk role, training relevant to the new role and its associated ML/TF/PF risks must be delivered before that person commences the new duties, not after.

KEEP RECORDS

All EDD Program records, including screening outcomes, risk assessments and ongoing PDD actions, must be retained for seven years after they are no longer relevant, in accordance with the record-keeping requirements under the AML/CTF Act and Rules.

CONCLUSION

Your business' approach to 'knowing your employees' and where the potential risks lie in your business is a critical part of your AML/CTF Program.

By following the above approach, you can:

- understand the risks presented by the roles in your business;
- align your EDD Program to these risks; and
- meet your obligations under the AML/CTF Act and Rules.

Need assistance with employee due diligence? Contact LCA today to arrange a consultation with our AML/CTF specialists.

Lane Consulting & Advisory

20B Armstrong Street Middle Park, Victoria 3206

0421 671 571

contact@laneconsultingandadvisory.com

https://laneconsultingadvisory.com