



Australian Government

AUSTRAC

AUSTRAC INSIGHTS

ASSESSING ML/TF RISK

A
AU
AUS
AUST
AUSTR
AUSTRAL
AUSTRAC
AUSTRAC II
AUSTRAC INS
AUSTRAC INSI
AUSTRAC INSIG
AUSTRAC INSIGH
AUSTRAC INSIGHT
AUSTRAC INSIGHTS
AUSTRAC INSIGHTS • A
AUSTRAC INSIGHTS • AU
AUSTRAC INSIGHTS • AU
AUSTRAC INSIGHTS • AU



HOW TO USE THIS DOCUMENT

Resilience against criminal exploitation is critical for your business' reputation and integrity. It's important to know where your business might be at risk.

This document is designed to help you understand your obligations and AUSTRAC's expectations regarding the assessment of money laundering and terrorism financing (ML/TF) risks to your business.

These insights, developed in the course of our regulatory activity, will help ensure you have a comprehensive ML/TF risk assessment that identifies and manages any vulnerabilities.




AN APPROPRIATE ML/TF RISK ASSESSMENT WILL COMPREHENSIVELY:

- identify and evaluate the ML/TF risk posed to your business, having regard to its nature, size and complexity
- take into account your customer types, the designated services you offer, the methods you use to deliver those services and the foreign jurisdictions you deal with.
- assess the inherent risk, also known as initial risk, before any AML/CTF systems have been applied to reduce the risk.

TO DETERMINE THE INHERENT ML/TF RISK, YOU MUST:

- develop an appropriate risk assessment methodology or model, including a way to measure the likelihood and impact of ML/TF risks
- populate the model with all relevant risks and associated risk attributes, and
- perform the risk assessment and ensuring that its outputs align with the scoring or ranking mechanisms of the methodology/model.

Once you have determined your inherent risks, you must apply systems and controls to reduce, or mitigate, those risks. You can then determine the residual risk. Once you have determined the residual risk you must apply systems and controls to manage those risks.




Inherent risk is the level of ML/TF risk *before* you apply systems and controls to reduce the risk

Residual risk is the level of ML/TF risk *after* you have applied systems and controls to reduce the risk

For detailed guidance on how to develop a risk assessment methodology and conduct a risk assessment, see austrac.gov.au/managing-risk



DOCUMENT YOUR RISK ASSESSMENT, SYSTEMS AND CONTROLS



Once you have completed your risk assessment, you need to document it. If you do not properly document your risk assessment, you cannot develop appropriate risk-based systems and controls in your AML/CTF program.

WE EXPECT YOU TO DOCUMENT:

- the method used to conduct the risk assessment
- an assessment of the likelihood and impact of the inherent ML/TF risk
- a scale for assessing the level of importance of ML/TF risk (for example, low, medium and high)
- how you have considered the following risk factors, as specified by the Anti-Money Laundering and Counter-Terrorism Financing Rules (AML/CTF Rules):
 - the risks associated with your customer types, including politically exposed persons
 - the products and services your business offers and the channels used to distribute them
 - the risks associated with any foreign jurisdictions you operate in.
- how you have considered the nature, size and complexity of your business, and any additional risks posed by the industry you operate in.

Your risk assessment needs to function as a 'living document'. You will not have appropriate risk-based systems and controls in place unless these systems and controls are regularly reviewed and adapted over time, having regard to emerging, developing and changing risks.

Your risk assessment must be based on all available data and should not be limited to the risks posed by how the product or channel functions. You will also need to consider information about trends in usage of the product or channel, transaction monitoring, suspicious matter reporting, internal financial crime reporting, and information from AUSTRAC and law enforcement to fully understand your risks.

APPLY RISK-BASED CONTROLS

Appropriate risk-based systems and controls must have regard to the type of ML/TF risk you identified and be in proportion to the level of risk. For example, in areas assessed as medium or high risk, you would apply more robust and/or strengthened systems and controls.

When determining the nature and robustness of a system or control, you should consider at least the following factors:

- the scope or coverage of the relevant system or control in your business e.g. customers, transactions and/ or employees
- how often the system or control is applied
- the resources and expertise required for carrying out or managing the system or control, and
- the degree of internal reporting and oversight by senior staff for ensuring the effectiveness of the system or control.

As with your risk assessment process, an appropriate risk-based system or control must be sufficiently documented in order to be consistently implemented.



What is the difference between preventative and detective controls?

Preventative controls are those that limit the ability to use your product or channel in a way that would increase the ML/TF risks. This includes things like setting transactions limits or having a management approval process for high-risk customers, products or countries, applying different identification processes for customers you don't deal with in person, or not accepting customers who you deem as too high risk.

Detective controls only seek to monitor activity through your product or channel. This includes things like gathering information about how your products or channels are used, and information from internal records, such as transaction monitoring and suspicious matter reporting.

NOTE: If your controls are detective only and not preventative, they may not correspond with your ML/TF risks and may not reduce your inherent risks.



CONTINUOUSLY REVIEW YOUR ML/TF RISK ASSESSMENT

An assessment of ML/TF risks must be carried out before you introduce new products, new channels or adopt new or developing technologies to deliver services.

You must regularly review the systems and controls that mitigate and manage your risks to ensure they remain aligned with current risks and are working as intended.

If you conclude that you have reduced a risk as a result of a system or control you have

implemented, you must fully document this, including your methodology and rationale.

In addition to periodic reviews of your systems and controls, there are a range of circumstances that can trigger an immediate need to review a product or channel's ML/TF risk assessment and its controls and how they impact your broader AML/CTF program.

PROVIDE ACCESS TO YOUR ML/TF RISK INFORMATION

To enable your risks to be appropriately reviewed, updated, mitigated and managed, you must have processes in place to ensure those with risk management responsibilities have access to full and timely information about your risks.

This information needs to be fully documented, as do risk assessments.

Effective governance and oversight is dependent on the completeness and accuracy of information provided to your senior management, committees and boards. Information flows about your ML/TF risks and AML/CTF controls must be coordinated and structured and not driven by events or incidents.

SET CLEAR ACCOUNTABILITY FOR ML/TF RISKS

After you have identified a risk, you must have processes in place to ensure your systems and controls correspond with that risk. This starts with briefing senior management on updated risk assessments. There must be clear

accountabilities within senior management to take action on updated risk assessments and to introduce systems and controls to mitigate and manage your risks.

FURTHER INFORMATION

FOR MORE INFORMATION, PLEASE SEE [AUSTRAC.GOV.AU/MANAGING-RISK](https://austrac.gov.au/managing-risk)

FOR MORE INFORMATION ON AML/CTF PROGRAMS, PLEASE SEE [AUSTRAC.GOV.AU/AMLCTF-PROGRAMS](https://austrac.gov.au/amlctf-programs)



