

Module	ANTI-MONEY LAUNDERING & COUNTER TERRORISM FINANCING
Jurisdictions	CTH, NSW, VIC, SA, TAS, WA, NT, QLD, ACT
Legal Expert	ANDREW HAM Partner at Hunt and Hunt Lawyers https://www.hunthunt.com.au/people/andrew-ham/ https://www.linkedin.com/in/andrewnham/

Module Scope

Is your organisation currently or does it intend to become an authorised deposit taking institution, a bank, a building society, a credit union?

Alternatively does your organisation currently offer or does it intend to offer any of the following?

- › remittance services (money transfers)
- › exchange digital currency (eg cryptocurrency) for money, or exchanging money for digital currency
- › loans or finance
- › investments or securities
- › life insurance and sinking fund policies
- › superannuation fund management (except self-managed superannuation funds)
- › foreign currency exchange
- › issuing travellers cheques
- › issuing money or postal orders with values of A\$1000 or more
- › issuing (not just selling) stored value cards such as travel cards and retail gift cards with values of A\$5000 or more, or A\$1000 or more if they can be withdrawn in cash
- › custodial and depository services (including safe deposit boxes)
- › preparing payroll for other businesses
- › providing pensions or annuities or retirement savings account services
- › financial advisory services provided by the holder of an Australian Financial Services Licence (AFSL) where the service is arranging for clients to receive a designated service
- › specialised financial services involving forfaiting, bills of exchange, promissory notes, letters of credit, factoring, derivatives, foreign exchange contracts, bearer bonds, finance leases or similar.
- › buying and selling bullion such as gold, silver, platinum or palladium.
- › betting accounts and services
- › exchanging gaming chips, token or currency
- › paying out winnings, or awarding a prize, in respect of a game or bet
- › games of chance, or a mix of chance and skill that are played for money (not including lotteries, raffles or bingo games)
- › gaming machines (such as poker machines).

Does your organisation understand its obligations under the Anti-Money Laundering and Counter-Terrorism Financing Act 2006?

Does your organisation currently have an Anti-Money Laundering and Counter-Terrorism Financing compliance program and systems in place?

Module Application

The *ANTI-MONEY LAUNDERING AND COUNTER TERRORISM FINANCING* module informs a reporting entity required to establish and maintain a compliant structural framework and program designed to detect and deter instances of money laundering and the financing of terrorism through or via the reporting entity.

A reporting entity can be a financial institution, a designated non-financial business or profession, a high value dealer, a casino, or any entity that is declared to be a reporting entity. All reporting entities operating in Australia should be subscribing to this module.

The *ANTI-MONEY LAUNDERING AND COUNTER TERRORISM FINANCING* module covers the obligations that are primarily imposed on Australian reporting entities by the;

- Anti-Money Laundering and Counter Terrorism Financing Act 2006 (Cth) (the AML/CTF Act);
- Anti-Money Laundering and Counter Terrorism Financing Rules Instrument 2007 (No1) (Cth) (AML/CTF Rules); and
- Financial Transaction Reports Act 1988 (Cth) (FTF Act);
 - Obligations under the FTF Act do not apply to transactions when the AML/CTF Act applies.

The Australian anti-money laundering and counter terrorism financing sector is regulated by the Australian Transaction Reports and Analysis Centre (AUSTRAC). The broad and overriding objectives of the legislation are to;

- Detect and deter money laundering and the financing of terrorism in Australia;
- Maintain and enhance Australia's international reputation by adopting recommendations of the Financial Action Task Force (an intergovernmental body); and
- Contribute to public confidence in the Australian financial system.

The *ANTI-MONEY LAUNDERING AND COUNTER TERRORISM* module covers the requirements for reporting entities to co-ordinate with other organisations, AML/CFT supervisors, and government agencies such as law enforcement and regulatory bodies to achieve the stated objectives by ensuring compliance with all legal obligations.

- The module covers the core obligations that reporting entities are required to comply with and practical guidance as to how organisations can achieve this compliance. The core obligations are;

- › **Conducting customer due diligence;** There are 3 types of customer due diligence – standard, simplified and enhanced. Customer due diligence is conducted both initially and on a continuing bases by way of account monitoring.
- › **Suspicious activity reports;** The reporting entity must report information about suspicious transactions or activities.
- › **Prescribed transaction reports;** Prescribed transactions must be reported. They are an important information source on the movement of funds across borders and the movement of physical cash within Australia.
- › **Record keeping;** Records must be created and retained for time periods directed by AML/CFT rules.
- › **Risk assessment;** Risk assessments must be undertaken and applied to risk ratings of resourcing and decision making.
- › **Cross-border transportation of cash;** Reports in the prescribed form of any movement of currency equal to or more than \$10 000 into or out of Australia are required.

To comply with these core obligations the reporting entity is obligated to establish, implement and maintain an AML/CFT program within their organisation. The module details how an organisation will comply with this obligation. The program must comply with the legislated regulations, particularly with regard to;

- › Outlining the policies, procedures and controls in place to detect money laundering and financing of terrorism within the reporting entity;
- › Managing and mitigating the risk of the reporting entity facilitating money laundering and terrorism financing;
- › Assessment of the adequacy and effectiveness of the implemented systems against the AML/CFT stated criteria;
- › Staff compliance and training;
- › The practical documentation of day-to-day operations; and
- › Effective controls to monitor compliance.

The consequences to a reporting entity found to have breached express anti-money laundering and counter terrorism obligations, as covered in the module, can include;

- › The issue of a formal warning;
- › The issuing and acceptance of an enforceable undertaking, and an order in the court for breach of that undertaking;
- › A High Court injunction for restraint or performance;
- › The application of a pecuniary penalty; and
- › Imprisonment for an offending individual.

The **ANTI-MONEY LAUNDERING AND COUNTER TERRORISM FINANCING** module covers the legal obligations of reporting entities. The module does not focus on the specific obligations of individuals or employees of organisations or reporting entities.

About LexisNexis Regulatory Compliance

LexisNexis Regulatory Compliance® helps you forge a clear path to compliance.

With LexisNexis® content know-how at the core, our compliance registers, alerts, and information-driven solutions make compliance uncomplicated for GRC professionals across the globe.