Internal Affairs
Te Tari Taiwhenua

Te Kāwanatanga o Aotearoa
New Zealand Government

Guidance

Online Casino Operators

This guidance should be read together with the Risk Assessment and AML/CFT Programme Guidance.

May 2026

AML ONLINE

Guidance: Online Casino Operators

Complying with the Anti-Money Laundering and Countering Financing of Terrorism Act 2009

Introduction

1. This guidance has been prepared by the Department of Internal Affairs (the **Department**) to support potential future online casino operators to comply with the requirements of the Anti-Money Laundering and Countering Financing of Terrorism (**AML/CFT**) Act 2009 (the **Act**).

2. An online casino operator will be a 'reporting entity' under the Act.

3. A risk-based approach is central to the effective implementation of the Act, it requires reporting entities to identify, assess and understand the money laundering and terrorism financing risks they face and then implement mitigation measures commensurate with those risks.

4. The extension of obligations to online casino operators recognises the ways they are used and the associated money laundering and terrorism financing risks.

5. This guidance has been produced by the Department for online casino operators under section 132(2) of the Act. It provides an overview of the requirements of the Act and is supported by other guidance relating to specific obligations under the Act. This guidance does not constitute legal advice.

6. The examples provided in this guidance are suggestions to help online casino operators meet their obligations under the Act. They are no exhaustive and are only illustrative in nature.

7. Sections 57(2) and 58(2)(g) of the Act require reporting entities to have regard to this guidance. It is important that you have read and taken this guidance into account when complying with your obligations. After reading this guidance, if you still do not understand any of your obligations you should contact the Department or seek legal advice.

Purpose of the Act

8. The purposes of the Act are:
   - to detect and deter money laundering and terrorism financing,
   - to enhance New Zealand's international reputation by adopting, where appropriate in the New Zealand context, recommendations issued by the Financial Action Task Force (**FATF**),[1] and
   - to contribute to public confidence in the financial system.

What is online casino gambling?

9. Under section 5 of the Act and Online Casino Gambling Act 2026, online casino gambling:
   (a) means gambling at a distance by interaction through a communication device, including using the communication device –
      (i) to participate in gambling that relies on a random number generator or other wholly or partly chance-based outcome generation (such as slot machines or lotteries); or
      (ii) to participate in casino table gambling (such as blackjack, poker,[2] or baccarat); or
      (iii) to bet, pay, or stake consideration on the outcome of a computer-simulated sporting event.

10. It does not include –
      (i) class 3 gambling in the form of a lottery conducted by any gambling operator that holds a class 3 operator's licence that allows the gambling operator to conduct a lottery (as those terms are defined in section 4(1) of the Gambling Act 2003):
      (ii) gambling that is declared not to be online casino gambling by regulations made under section 79(1)(a) of the Online Casino Gambling Act 2005.

---

[1] FATF is an interagency government body that sets standards for combatting money laundering, terrorism financing, proliferation financing and other related threats to the integrity of the international financial system.

[2] As defined under the Online Casino Gambling Act 2026.

What are my obligations under the Act?

11. Under the Act, you must:

	What needs to be done?	When does it need to be done?	Additional information
Establish an AML/CFT programme	**Appoint an Anti-Money Laundering and Countering Financing of Terrorism compliance officer**	Before you apply for an online casino licence and then ongoing as required	A compliance officer must be an employee, report to a senior manager (or be a senior manager themselves) and can be shared in a designated business group (DBG)
	Conduct a risk assessment	Before you develop your AML/CFT programme and ongoing as required. The Department's Online Gambling Sector Risk Assessment will support you to conduct your risk assessment	Can be done by the reporting entity, DBG or third party
	Develop an AML/CFT programme	After you carry out your risk assessment then ongoing as required	Can be done by the reporting entity, DBG (parts of) or third party
Administer and maintain your AML/CFT programme	**Training and vetting of staff**	Ongoing as required	Can be done by the reporting entity, DBG or third party
	Conduct customer due diligence	When you establish a business relationship with your customer or in other situations depending on risk[3]	Can be done by the reporting entity, DBG or third party. The responsibility lies with the reporting entity

[3] In the context of online casino gambling, a business relationship may be established when a customer creates an account with the online casino operator.

	Keep records	Ongoing and records must be kept for at least five years	Responsibility of the reporting entity, and/or DBG
	Ongoing customer due diligence and account monitoring	Ongoing	Responsibility of the reporting entity, and/or DBG
	Review AML/CFT programme	At regular intervals specified in your AML/CFT programme	Can be done by the reporting entity, DBG or third party
Annual report	**Submit an annual report**	Submit to the Department by 31 August each year	Responsibility of the reporting entity, and/or DBG
	Audit your risk assessment and AML/CFT programme	Every three years, unless a four-year timeframe applies	Auditor must be independent and appropriately qualified
Report to the Financial Intelligence Unit	**Suspicious activity reports (SARs)**	As soon as practicable, but not more than three working days after there are reasonable grounds for suspicion	Responsibility of the reporting entity, and/or DBG. Submit to the FIU using goAML
	Prescribed transaction reports (PTRs)	Within 20 working days from the date the transaction took place	Responsibility of the reporting entity, and/or DBG. Submit to the FIU using goAML

Appoint a compliance officer[4]

You must appoint a compliance officer who will be responsible for administering and maintaining the AML/CFT programme. The employee appointed to this role should report to a senior manager or be a senior manager themselves.

Conduct a risk assessment[5]

A reporting entity must undertake an assessment of the money laundering and terrorism financing risks it faces in the course of its business.

The risk assessment must be in writing and have regard to various specified factors, including the New Zealand Police Financial Intelligence Unit National Risk Assessment and the Department's Sector Risk Assessment.

Develop an AML/CFT programme[6]

Your AML/CFT programme must be based on your risk assessment and be in writing. It must include relevant procedures, policies and controls for ensuring all compliance obligations are adequately and effectively met.

Administer and maintain your AML/CFT programme

Once an AML/CFT programme is developed, a reporting entity's compliance officer is responsible for administering and maintaining the AML/CFT programme.

[4] Refer to section 56(2) to 56(4) of the Act.

[5] Refer to section 58 of the Act.

[6] Refer to section 57 of the Act.

Conduct customer due diligence[7]

Reporting entities must conduct CDD (at the required level) before establishing a business relationship with a customer. The Act requires a reporting entity to carry out CDD on:

- a customer
- any "beneficial owner" of a customer
- any person acting on behalf of a customer.

Enhanced CDD may also be required during a business relationship in certain higher risk situations.

Keep records[8]

Reporting entities must keep records for five years. Maintaining these records ensures you can effectively implement your AML/CFT obligations, particularly ongoing CDD and account monitoring. It also enables you to demonstrate compliance with your AML/CFT obligations and explain the reasons for the decisions you have made.

Ongoing customer due diligence and ongoing account monitoring[9]

Once you have established a business relationship with a customer, you must conduct risk-based ongoing CDD and account monitoring. This will ensure that the business relationship and the transactions relating to it are consistent with your knowledge about the customer, their business and risk profile. It will also assist you to identify any grounds for reporting suspicious activity.

[7] Refer to Part 2, subpart 1 of the Act.

[8] Refer to sections 49-55 and 57(1)(e) of the Act.

[9] Refer to sections 31 and 57(1)(c) of the Act.

Monitor and manage compliance with your AML/CFT programme[10]

You must have adequate and effective procedures, policies and controls to monitor and manage compliance with your AML/CFT programme.

Review your risk assessment and AML/CFT programme[11]

12. Your risk assessment and AML/CFT programme must be kept up to date, effective and respond to any new or evolving money laundering or terrorism financing risks your business may face.

Annual Report and Audit

Submit an annual report[12]

Reporting entities must prepare and submit an annual report to the Department. The annual report is a key part of your requirements under the AML/CFT Act. It provides an opportunity for you to review your risk assessment and AML/CFT programme. The report must take into account the results and implications of any audit and any information prescribed by regulations.

The annual report must be submitted in the prescribed form and at a time appointed by the Department.

How to submit an annual report to the Department

You will need to submit your annual report using AML Online. Further information about how to submit your annual report can be found on the Department's website.

Independent audit[13]

You must have your risk assessment and AML/CFT programme audited by a person who is independent and appropriately qualified to conduct the audit. An independent audit must be conducted every three years unless a four-year timeframe applies. Refer to the AML/CFT Audit Guidance for further information.

[10] Refer to section 57(1)(l) of the Act.

[11] Refer to section 59 of the Act.

[12] Refer to section 60 of the Act.

[13] Refer to section 59(2) of the Act.

Money Laundering and Terrorism Financing Risks associated with Online Casino Operators

13. Online casino operators need to be aware of the ways in which criminals can misuse their services to launder money or finance terrorism. Identifying the risks is the first step towards combatting money laundering and terrorism financing.

14. Online casino operators have a unique view of their customers, their activities and transactions. This provides an opportunity to detect criminal activity that might not be visible to banks or other reporting entities who interact with the same customer.

What is money laundering?

15. Money laundering is the process that criminals use to "clean" the proceeds of their crime (money and/or assets) by moving them into the legitimate economy. Criminals avoid detection by using different methods to disguise and conceal the origin of the proceeds of crime, so it appears the proceeds come from legitimate sources. This enables criminals to profit from the crime.[14]

What is terrorism financing?

16. Terrorism financing is the funding or provision of material support for terrorism acts or sustaining the ongoing operations of terrorism activities. Unlike money laundering, the funds used for terrorism financing may be legitimately sourced. Terrorists and their sympathisers use similar methods to disguise and conceal the recipients of their funds.[15]

What is proliferation financing?

17. Proliferation financing occurs when funds or financial services are provided to help with developing, buying, or moving nuclear, chemical, or biological weapons – weapons of mass destruction in circumstances prohibited by New Zealand law. Similar to terrorism financing, the funds may have legitimate sources, but the ultimate goal is to disguise and conceal the recipients of these funds, using similar methods to money laundering.

[14] Money laundering is an offence under section 243 of the Crimes Act 1961.
[15] Terrorism financing is an offence under section 8 of the Terrorism Suppression Act 2002.

Nature, size and complexity

18. Online casino operators should consider how the nature, size and complexity of their business may be perceived by a money launderer.

19. The New Zealand Police Financial Intelligence Unit National Risk Assessment 2024[16] highlighted an increase in money laundering risk through online gambling. The Department's Online Gambling Sector Risk Assessment indicates that the level of risk varies, depending on the operator, the services provided, the payment methods accepted and the effectiveness of an online casino operators' procedures, policies and controls.

20. Online casino operators may be vulnerable to money laundering and terrorism financing for the following reasons:
    (a) the use of domestic and international stored value instruments to fund online gambling activities
    (b) the use of e-wallets or cryptocurrency as a means of payment to fund online gambling accounts
    (c) the access to a wide selection of customers (overseas-based customers)
    (d) transactions involving customers in high-risk jurisdictions
    (e) use of new payment technologies (online trading platforms)
    (f) the ability to move large sums of money
    (g) the ability to place bets with deposited funds
    (h) the ability to facilitate illegal transfers between parties through direct transfers
    (i) obscuring funds in online gambling accounts without automatic withdrawal
    (j) non-face-to-face delivery

21. Online casino operators should therefore be alert to red factor indicators, including:
    - Customers undertaking multiple low value transactions to avoid reporting thresholds
    - Customers utilising multiple accounts to help one player win and other lose to turn the funds into legitimate gambling winnings
    - Customers making payments into a bank account from an online gambling account without any payments made to the online gambling site (money in, money out)
    - Customers placing large bets on low-risk games
    - Customers making substantial deposits or withdrawals within a short timeframe
    - A customer's transaction is unusually large or not what is expected from the type of customer

[16] National Risk Assessment (NRA) | New Zealand Police

Know your red flags

22. It is important that online casino operators are aware of the red flags which may indicate that a customer is engaged in money laundering, terrorism financing or proliferation financing and should prompt further examination. If legitimate activity cannot be established, an online casino operator may need to submit a SAR and/or cease transacting for the customer.

23. It is important to understand that each risk and red flag does not operate in isolation but in **combination** with the others. Where two or more red flags apply, the level of risk compounds.

24. **Note:** the red flags in this guidance are for information purposes only, they are not exhaustive and are illustrative in nature.

Reporting requirements

25. The Act requires all reporting entities to file SARs and PTRs to the New Zealand Police Financial Intelligence Unit (**FIU**) under the Act. To file a SAR or PTR, reporting entities must be registered with goAML.

26. A SAR must be submitted within 3 working days after forming a suspicion and PTRs must be submitted within 20 working days after the transaction.

Further information

27. If you require further information, please contact the Department of Internal Affairs at amlcft@dia.govt.nz or refer to the following:

- Relevant FATF guidance material
- National Risk Assessment
- Online Gambling Sector Risk Assessment
- Assessing Country Risk Guidance
- AML/CFT Programme Guidance
- AML/CFT Risk Assessment Guidance

Disclaimer

> **Note:** This guidance has been produced by the Department of Internal Affairs under section 132(2) of the Act for online casino operators. This guidance does not set out all obligations under the Act, its associated regulations and codes of practice. This guidance does not constitute legal advice.

Version History

Version	Date	Author	Description of changes
1.0	May 2026	Department of Internal Affairs	Initial version