



Isle of Man
Government

Reiltys Ellan Vannin

GSC AML Forum

18th July 2025



Welcome

Agenda

GSC Update	An update on the GSC.
NRAS Typologies	National Risk Appetite Statement
FIU Typologies Overview	Typologies Highlighted by the Isle of Man Financial Intelligence Unit
~~~~~ <b>Break</b> ~~~~~	Break for refreshments, with SLIDO running
<b>Outreach</b>	Summary of Outreach in 2025 so far.
<b>AML Inspections Team</b>	Software Supplier licence - AML/CFT



# Isle of Man National Risk Appetite Statement (NRAS)

*Working Together to Identify and Manage Risks*

Shannon Reid, AML/CFT Technical Advisor

# What is the NRAS?

A formal statement of the Isle of Man's risk appetite within the eGaming sector as well as any other business sectors that may have activity linked to eGaming.

Its purpose is to enhance the Island's risk mitigation framework.

Developed in response to emerging threats from transnational organised crime, particularly in East and Southeast Asia.

Supported by a Typologies Document from the Financial Intelligence Unit (FIU).

Applies to all entities undertaking activity in the Island. Particularly important for any business intersecting with the eGaming industry.



# Why is the NRAS Important?

1

Reinforces the Island's commitment to international standards and a robust economic environment.

2

Provides clarity and consistency for industry and regulators.

3

Helps protect the Island's reputation and financial integrity.

4

Aids in disrupting criminal exploitation of legitimate sectors.



# Key Messages from the NRAS

1

Limited appetite for business in the eGaming sector where there is ownership and/or control from East or Southeast Asia.

2

Where there is an accumulation of higher risk factors there is an extremely limited appetite within the regulators to grant a licence.

3

If there is an accumulation of risk factors present within the same relationship, action must be taken.



# What Operators need to do

## Immediate policy updates:

- Treat the NRAS as a trigger event requiring immediate incorporation into:
  - Business risk assessments (BRA)
  - Customer risk assessments (CRA)
  - Policies and procedures

## Risk mitigation:

- Apply appropriate mitigating measures to existing relationships where higher risk factors are identified.
- Avoid entering into new relationships where risks cannot be effectively mitigated.

## Ongoing monitoring:

- Continuously assess customer and business relationships against the NRAS and FIU typologies.
- Ensure internal governance and decision-making reflect the national risk appetite.





# What the GSC will do

## Licensing decisions:

- Will not authorise new business where there is an accumulation of high-risk factors that fall outside the national risk appetite.
- Review existing licences where such risk factors are present.

## Supervisory oversight:

- Ensure that regulated entities have updated their policies, procedures, and risk assessments in line with the NRAS and FIU typologies.



**Note: The GSC's AML/CFT Guidance has been updated to incorporate the NRAS.**

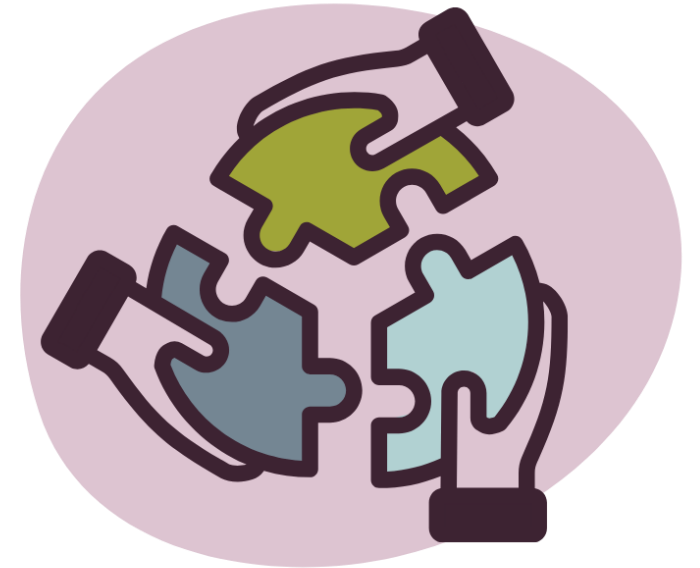
# Working Together

Strategic and operational collaboration between:

- Government and regulators
- Industry stakeholders
- FIU and law enforcement

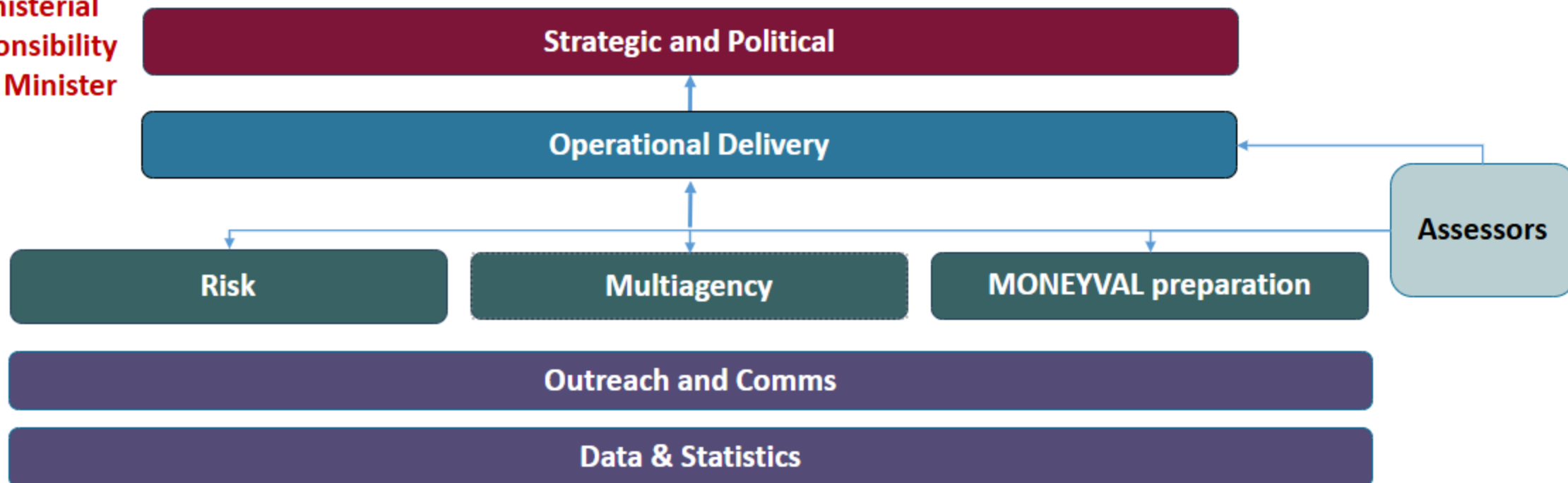
Shared responsibility to:

- Identify and assess risks
- Apply proportionate controls
- Maintain a resilient and reputable business environment



# Governance Structure

Ministerial  
responsibility  
DHA Minister



# What's Next?

A broader NRAS expected  
later in 2025

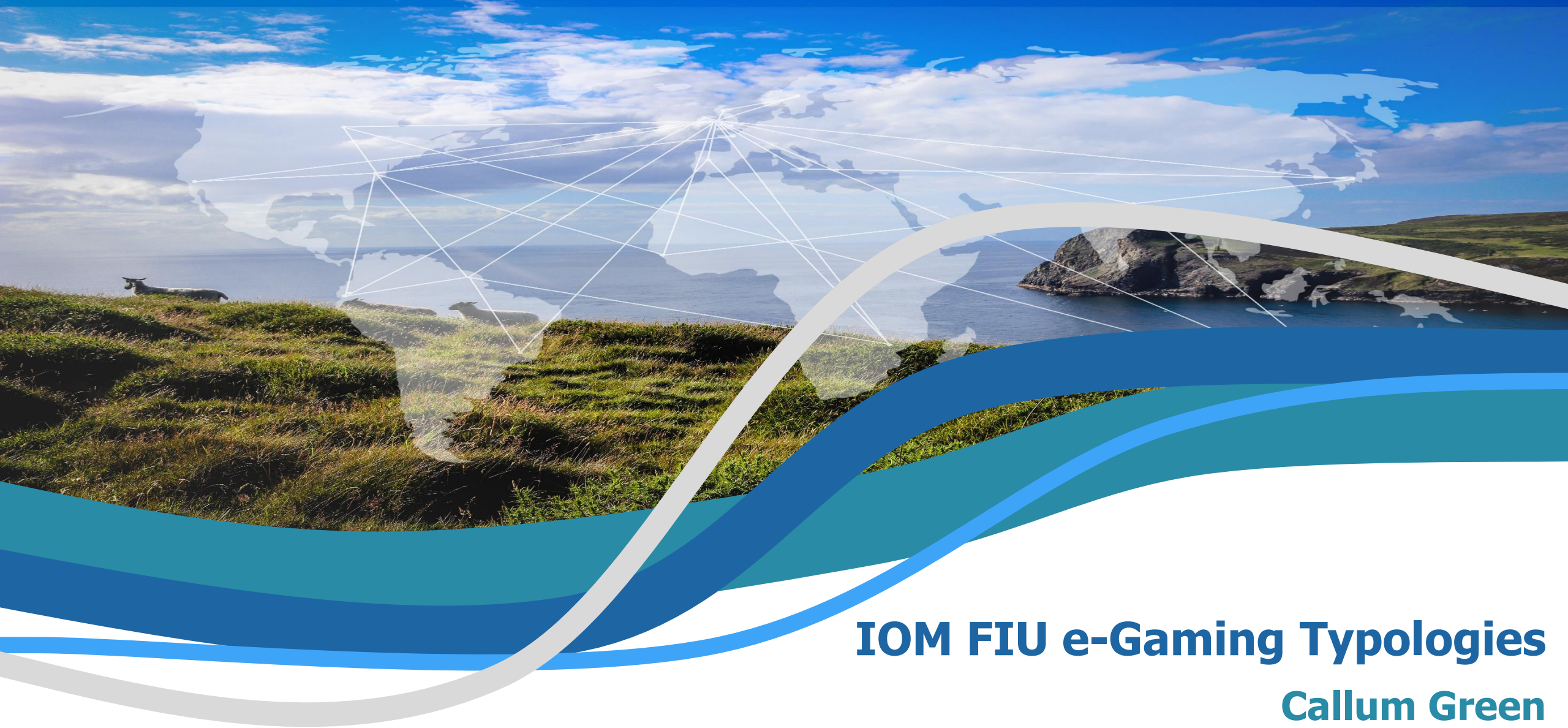
Continued engagement  
and feedback from  
industry is encouraged

FAQs & Guidance Updates



FIU Presentation on Typologies document on misuse of eGaming:

- Inform internal risk assessments;
- Enhance staff training;
- Strengthen transaction monitoring and reporting frameworks;
- Support a risk-based approach.



# IOM FIU e-Gaming Typologies

Callum Green

July 2025



Isle of Man  
**Financial Intelligence Unit**  
*Ellan Vannin Unnid Tushtag Argidoil*

Official



# IOM FIU e-Gaming Typology

## Key Points

- Created to increase awareness of ML, TF, and PF risks for the e-Gaming sectors and service providers linked to this sector.
- As stated in the Isle of Man National risk appetite statement and open-source media the e-Gaming sector has been subject to infiltration from organised criminal transnational groups. The regulated sector and law enforcement agencies remaining vigilant to the threat is key to prevent further exploitation.
- The IOM FIU notes TF and PF risks can sometimes be overlooked but present a greater risk of harm. An example of an emerging threat is the exploitation of businesses by North Korean state actors, who are seeking remote employment as IT workers. **The salary they earn from their employment is sent back to Pyongyang to finance North Korea's nuclear weapons program** ([Article](#))



**Online Gambling:  
Red Flags and Typologies  
for Money Laundering, Terrorist  
Financing, and Proliferation Financing**  
May 2025

[Typology Link](#)

# Typology One Summary

- **Customer A** opened a gambling account with **Firm B**. **Customer A** immediately deposited a large amount of funds from a debit card. An internal trigger was hit requiring additional customer due diligence information before play could continue.
- **Firm B** made a request to **Customer A** to provide ID, proof of address, and source of funds information in the form of the debit card used to make the deposits. Customer A was initially evasive, but provided the documents requested.
- **Firm B** identified that the ID, and address documentation were falsified. Investigation showed IP location information for **Customer A** did not match the address provided. **Customer A** did not respond when questioned further.
- **Firm B** received a chargeback request from the issuer of the debit card stating the card had been stolen.
- **Firm A developed a suspicion they had received the proceeds of crime and made a disclosure to the FIU.**



# Red Flag Indicators

1

**Deposit of a large amount of funds in a short period**

2

**Reluctance to initially provide CDD and no response to further questions**

3

**Identification of the falsification of CDD documents**

4

**IP location did not match address provided**

5

**Receipt of a chargeback and notification payment method had been stolen**



# Typology Two Summary

- **Supplier C** is an IOM GSC licenced software supplier. They provided e-Gaming software to an international client, **Company D**, who are based in Thailand.
- **Company D** is a newly incorporated company with local directors/UBOs with limited e-Gaming experience. When the software supply agreement was initially signed **Supplier C** questioned how **Company D** were going to afford their fees as they lacked an established player base. **Company D** stated they were part of a group who would initially fund this but refused to provide detailed documentation.
- **Supplier C** noted **Company D's** website was relatively basic.
- **Supplier C** following the provision of services identified adverse media stating that **Company D** was linked through the group company to a criminal organisation engaged in investment scams.
- **Supplier C** formed the suspicion that they had received the proceeds of crime in return for the software provided.
- **Supplier A made a disclosure to the FIU and terminated the relationship.**



# Red Flag Indicators

1

**Company D is newly incorporated and has a lack of personal funds to purchase gambling software**

2

**Directors/UBOs have limited prior experience in the e-Gaming field**

3

**Non-provision of documentation for group companies to potentially disguise SOF**

4

**Company D's website is relatively basic and may not be fit for purpose**

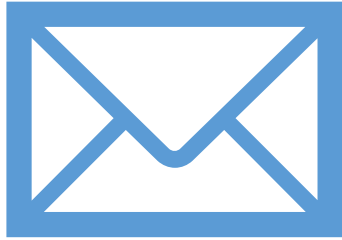
5

**Adverse media linking company to an organised crime group in South Asia**

# Any Questions?



# Contact Information & Feedback Link



**IOM FIU Email**

**fiu@gov.im**

Isle of Man FIU Outreach Feedback





**Isle of Man**  
**Government**

*Reiltys Ellan Vannin*

**BREAK**





**Isle of Man**  
**Government**

*Reiltys Ellan Vannin*

# Outreach Presentation

Charis

# What data do we collect?

Strix Data

Outreach  
Feedback Survey  
(AML Forum)

Drop-in  
sessions

Other  
feedback

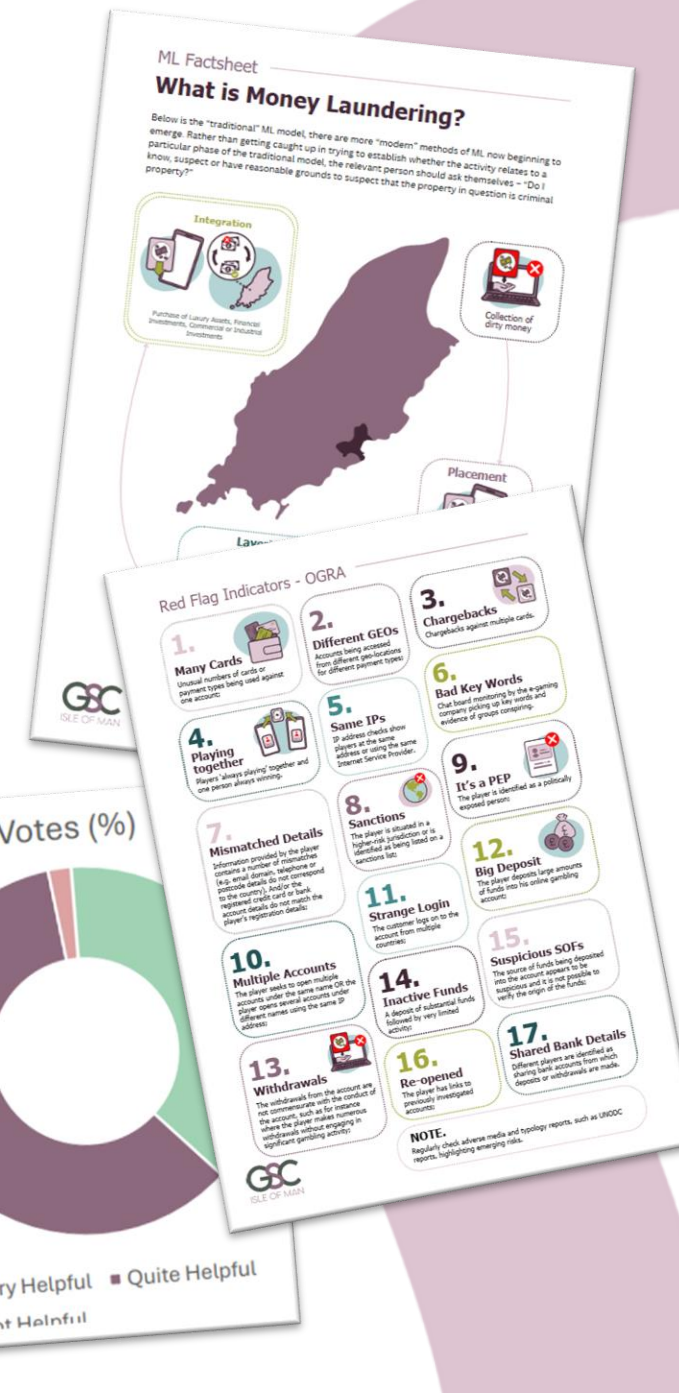
International  
reports

Inspections  
findings

National  
(cross-agency)  
data

Enforcement  
findings

And more...



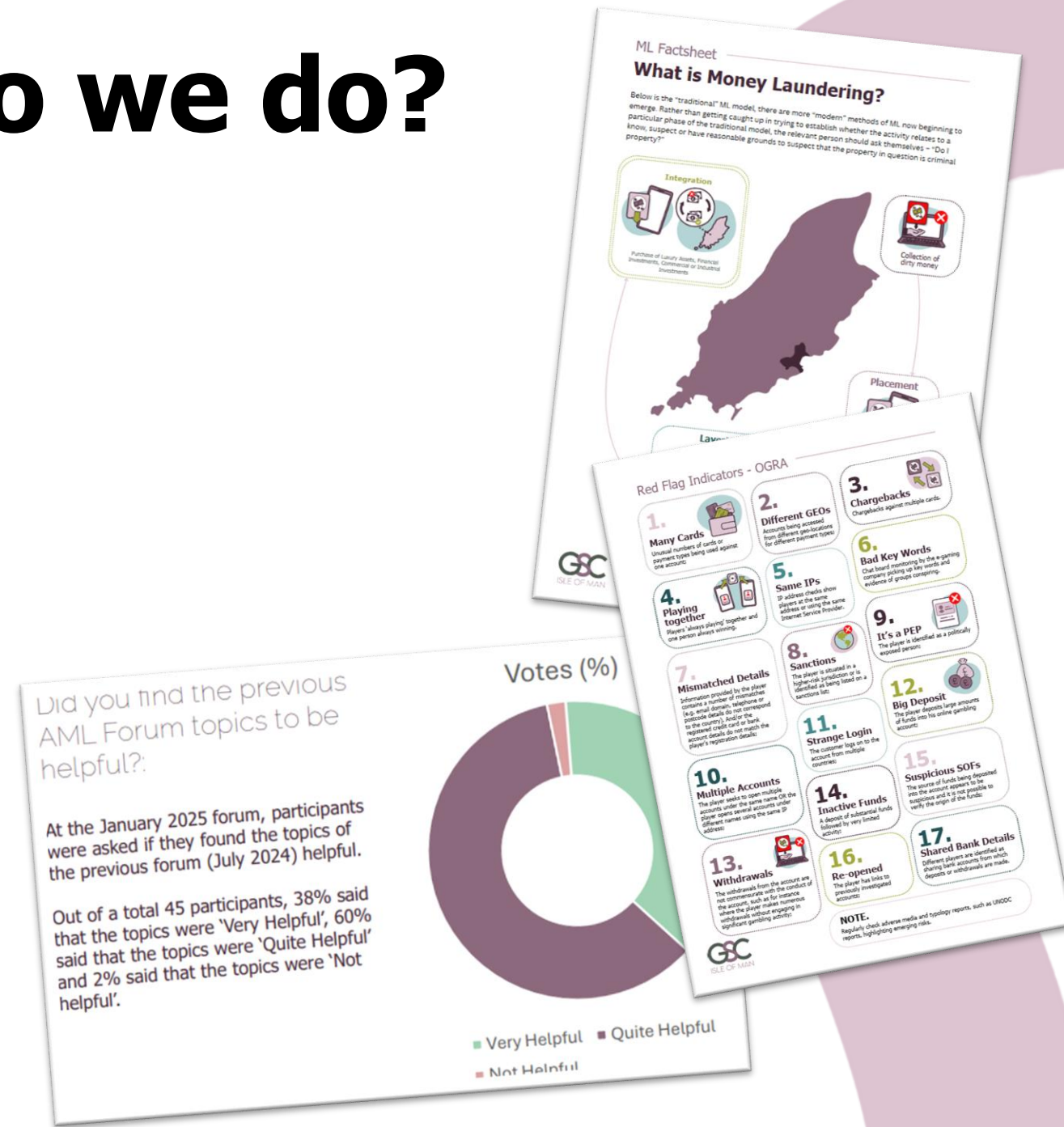
# What do we do?

## Sharing Data With Industry

- Outreach and Survey Reports shared
- Enforcement Findings shared

## Internal Statistics

- Using Power BI for reporting within the organisation and best practice
  - Data dashboards created for internal use





# Using Data – Internal Analytics

**Power BI reporting project in collaboration with the FSA.**

## Modelling

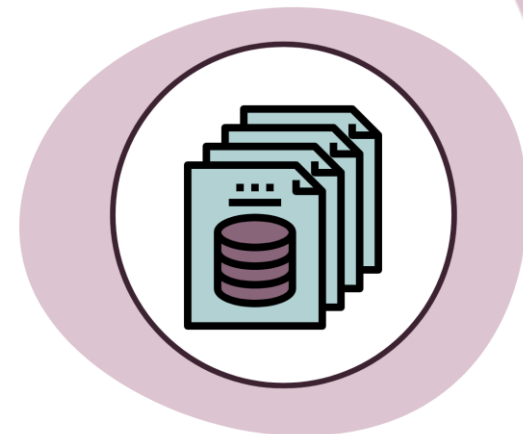
Combine data sources and format to make easier analysing and visualising

## Visualisation

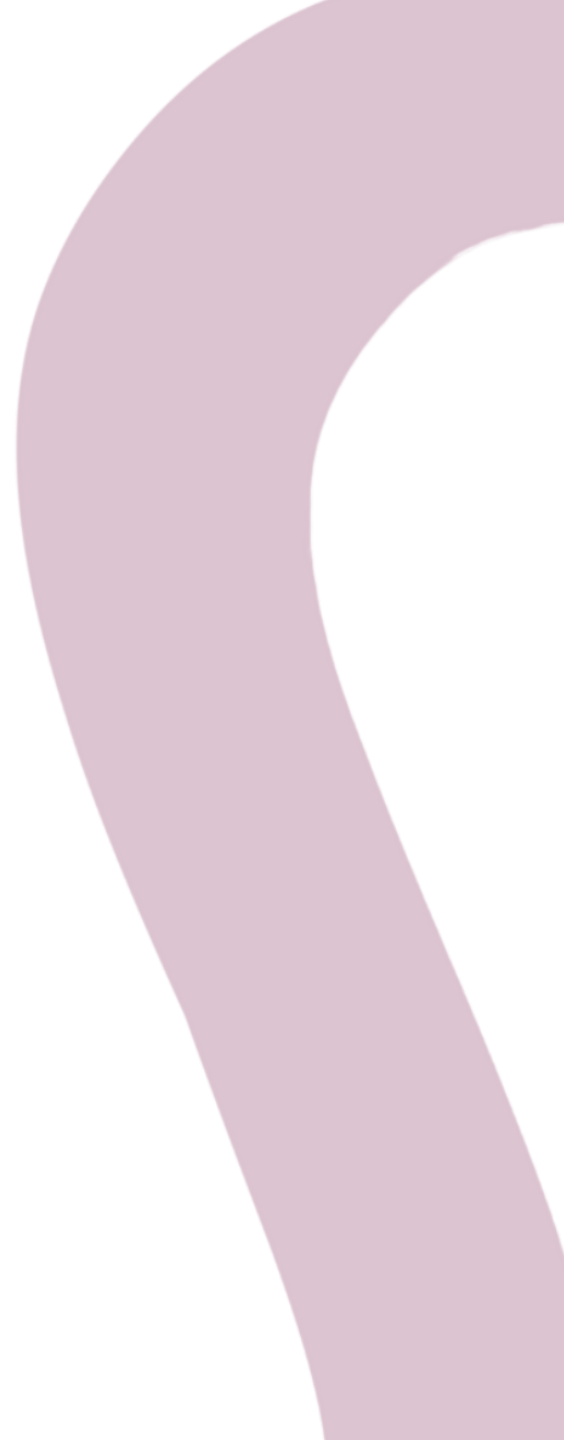
Reports, figures, tables as well as simple summary statistics (averages, percentage differences)

## Sharing

Amongst the GSC inspectors, senior management and more.



**What have we been up to?**



# What have we been up to?

- Video series on AML CFT inspections completed
- Training undertaken with Banking Sector (ongoing)
- Factsheets released on ML/TF/PF flags/typologies
- More reports & news blogs
- Drop-in sessions
- Internal training for GSC staff
- Revised guidance docs & some design overhauls
  - Added consistency and Clarity to publications

# What do we plan to do?

- Continue webinar/video series on topics you are interested in
- A second set of drop-in sessions (September)
- Event(s) aimed at C-level/Directors
- More workshops (topics TBC)
- Continue to revise website and publications for consistency & clarity based on your feedback
- More outreach to banks & law sectors



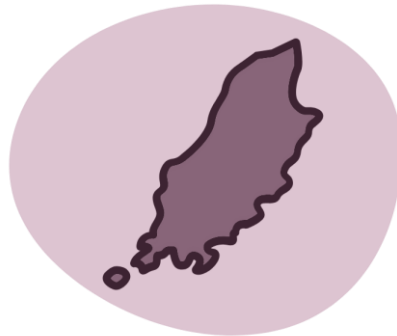
# News & Events

**Banking Outreach**

**Law Society Talks**

**Drop-in Sessions,  
Workshops,  
Webinars**

**Country Training**



**Countering  
Financial Crime  
Conference  
(3rd September)**





**Isle of Man**  
**Government**

*Reiltys Ellan Vannin*

# **AML/CFT Inspections Team**

Paul Skinner & Tommy Corlett

# OGRA Software Supplier Licence

## References

- Guidance for Software Suppliers
- Guidance for Virtual Assets & Goods
- FIU Red flags typology report
- GSC website – AML/CFT publications



The Legal Basis of conducting an AML/CFT inspection on a software supplier licensee



The AML/CFT inspection process



Red Flags / High Risk Factors



Case study example



National Risk Appetite statement

# The Legal Basis

## Online Gambling Regulation Act 2001 (OGRA) – Software Supply (SSL)

### Licence Conditions

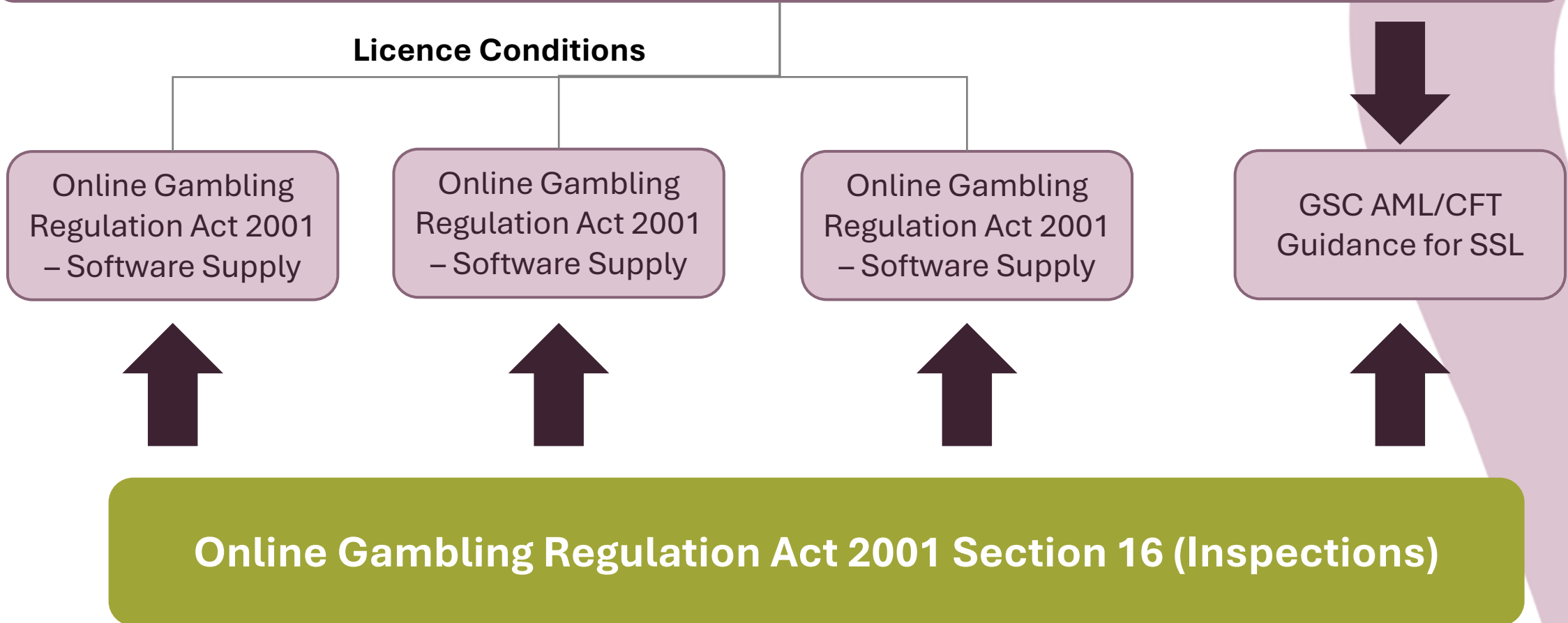
Online Gambling  
Regulation Act 2001  
– Software Supply

Online Gambling  
Regulation Act 2001  
– Software Supply

Online Gambling  
Regulation Act 2001  
– Software Supply

GSC AML/CFT  
Guidance for SSL

Online Gambling Regulation Act 2001 Section 16 (Inspections)





# AML/CFT Inspections Process

1

## Pre-Inspection

- AML/CFT self-assessment
- Relevant policies and procedures
- Risk Assessments
- Training logs
- Disclosure registers

2

## Onsite

- Risk-based approach
- AML/CFT staff
- Suspicious Activity Reporting

3

## Post-inspection

- A request for further outstanding documents from onsite inspection
- Draft report
- Final report

# Risk factors

Business proposals or OGRA licence applications from people with a lack of experience in the industry and/or lack of technical expertise

Opaque or unexplained source of funds or wealth – pushback against attempts to clarify

Adverse media

Beneficial owners or business structures with links to countries listed in the Cabinet Office's National Risk Appetite document

Newly incorporated third parties

Third parties with limited online presence or unsophisticated websites

Inconsistencies or unexplained changes in business proposals and licence applications

Business profits out of line with expectations (e.g. new business or unsophisticated platforms generating much higher income than anticipated)

Complex B2B arrangements and relationships

B2B relationships with a lack of coherent rationale

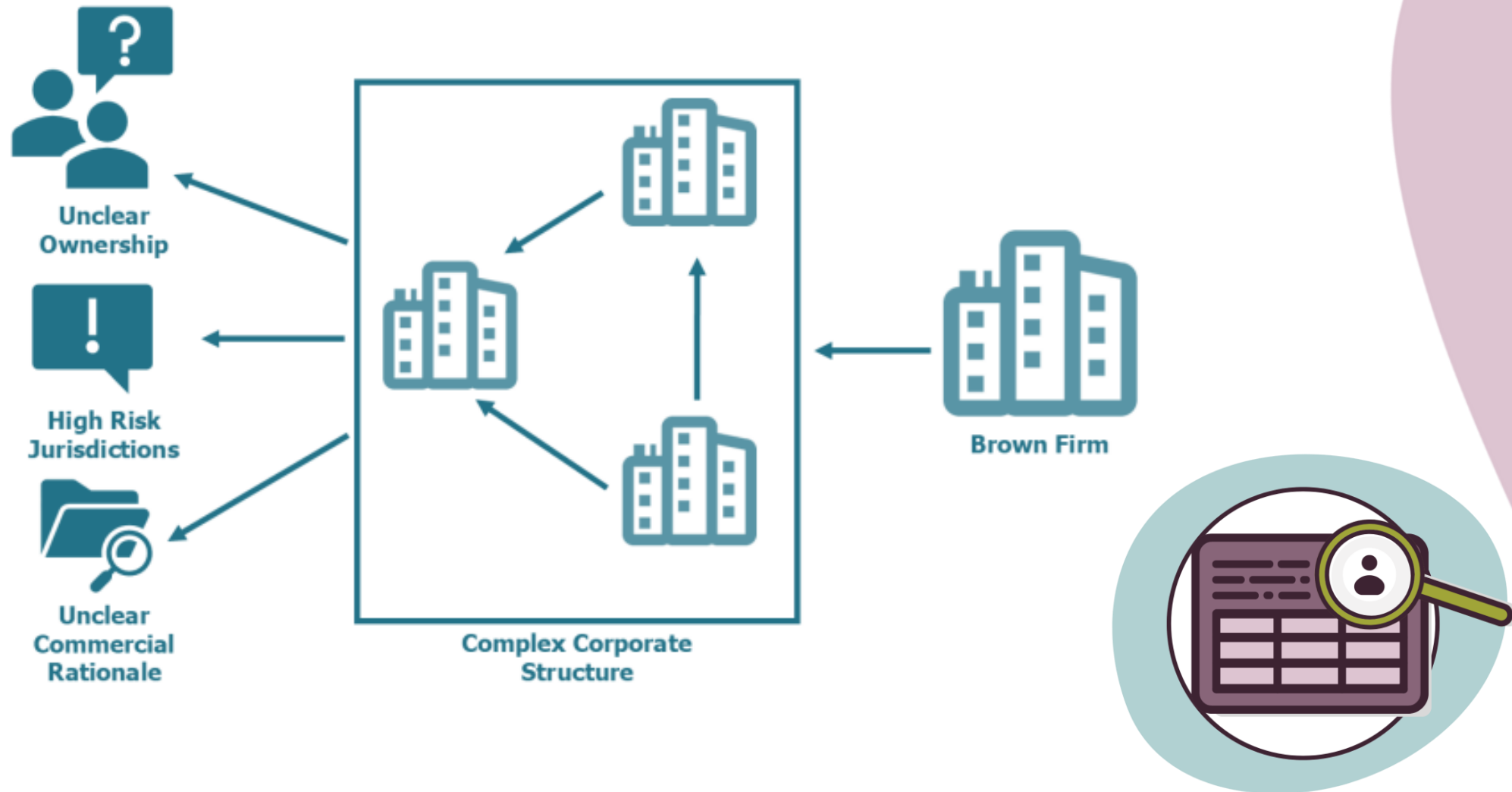
Commercially questionable business activity (e.g. purchasing other businesses at inflated prices)

B2B relationships with online gambling operators active in un- or under-regulated jurisdictions

B2B payments in cryptocurrency

B2B payments through money transmission services, particularly when doing so is commercially questionable (higher cost than bank-to-bank transfers)

# Case Study



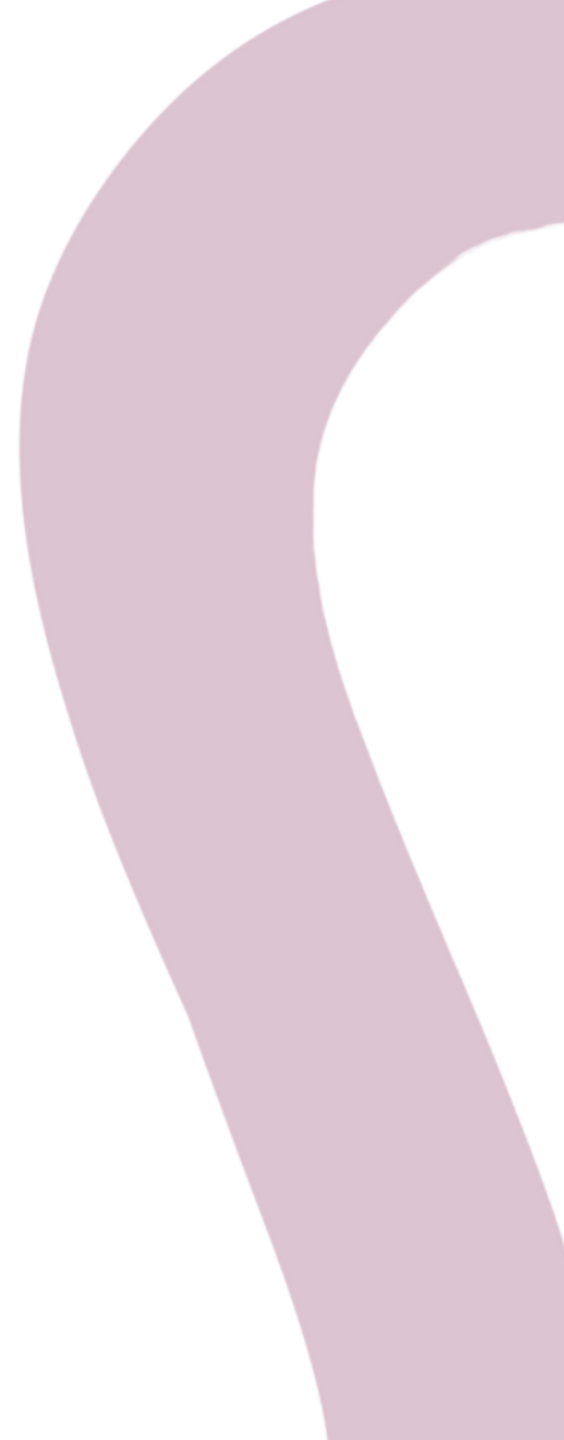
# National Statement on eGaming and Financial Crime

Activities, Risk Appetite  
and Mitigation

MAY 2025



# **Closing Remarks**





# Reminder!



# Where to find us...

- Blog available under "About the GSC".
  - Press releases, GSC news and Public Statements are available under "GSC News" which can be found on the Gambling homepage
  - Webinars and other videos are available under "Videos"
  - YouTube Channel - [youtube.com/@IOMGSC](https://youtube.com/@IOMGSC)
- LinkedIn updated regularly with GSC updates
  - [/company/isle-of-man-gambling-supervision-commission](https://company/isle-of-man-gambling-supervision-commission)
- Countering Financial Crime LinkedIn page
  - [/company/isle-of-man-countering-financial-crime](https://company/isle-of-man-countering-financial-crime)
- Newsletter Sign-up Form
  - <https://dashboard.mailerlite.com/forms/1118744/133525586866865391/share>

**Newsletter  
Sign-up Form**

