LexisNexis® | *Regulatory Compliance*

Channel Newscast

December 2022 – Edition 14

Table of Contents

Introduction 3

New Modules 3

- Casinos 3
- Infrastructure Resilience and Security 4
- Interactive Gambling 6

Marketing & Events 7

Technical Changes 8

New API Guide for Channel Partners 8

Enquiries 9

Introduction

Welcome to the December 2022 edition of the LexisNexis® Channel Partner Newscast, a regular update on what is happening in the world of the LexisNexis Regulatory Compliance solution.

This newscast is designed to provide our channel partners with advice on what's happening with our existing content offering, any future changes that we're considering, and what we're doing to promote the Regulatory Compliance solution out in the wider world.

We hope that you'll find all this useful and that we can continue to work together to give all our customers the best regulatory compliance content in the world through the best GRC/ERM solutions available today.

New Modules

LexisNexis is always exploring new ways to help organisations get a better understanding of their compliance obligations. While we are committed to the process of continuous improvement in our existing content offering, these new modules are available now for Australian customers.

Casinos

The *CASINOS* obligations register informs organisations of what their legal obligations are, and what procedures and processes they should have in place to ensure compliance with state and territory, as well as federal requirements when operating a casino business and providing casino gaming in Australia.

This register comprehensively covers the regulatory framework and licensing requirements relating to the casino industry, how eligible organisations can obtain a casino licence, and the organisation's legal obligations once licensed as a casino operator. It breaks the organisation's legal obligations into the following topics:

- Casino gaming and licensing
- Responsible gambling codes of practice
- Casinos operations and facilities
- Patron welfare and safety
- Casino security
- General offences related to casinos
- Workplace requirements
- Liquor licensing
- Sale and supply of liquor
- Anti-money laundering and counter-terrorism financing
- Reporting, record keeping and taxation

CASINOS answers what the organisation's legal obligations are when operating a casino business and providing casino gaming in Australia, and how the organisation can obtain a licence to operate a casino business and provide casino gaming in Australia. It also covers what processes or procedures should be in place to ensure compliance, and what the consequences are if the legal obligations are breached.

Infrastructure Resilience and Security

The *INFRASTRUCTURE RESILIENCE AND SECURITY* obligations register explains the obligations of relevant entities under the Australian critical infrastructure protection regime.

The register addresses the obligations of each category of the relevant entity, which can vary according to whether the entity is a:

- **Responsible entity**, which is an organisation that has a prescribed relationship with the asset and carries the greatest legal responsibility for its protection
- **Direct interest holder**, which is an organisation that holds an interest of at least 10% of the asset or holds enough interest to exert influence or control over the asset
- **Asset operator**, which is an organisation that operates the asset or part of the asset, or
- **Managed service provider**, which is an organisation that manages, manages an aspect, or manages an aspect of the operation of all or part of an asset

In addition, *INFRASTRUCTURE RESILIENCE AND SECURITY* addresses industry-specific infrastructure resilience obligations applicable to relevant entities and other organisations operating in the telecommunications and financial services sectors.

1. Register of Critical Infrastructure

Each organisation must recognise critical infrastructure assets and its role (or roles) as a relevant entity in relation to those assets.

The responsible entity and direct interest holders for each critical infrastructure asset must register the asset with the Cyber and Infrastructure Security Centre (CISC) unless an exemption applies. Having registered a critical infrastructure asset, the organisation must notify CISC of changes to any registered information.

2. Reporting and Information

The responsible entity for a critical infrastructure asset must notify the Australian Cyber Security Centre (ACSC) of any cyber security incident that affects the asset and meets prescribed impact thresholds.

Each relevant entity for a system of national significance must report information about the nature, operation, security and other qualities of computer systems to the Australian Signals Directorate.

The SOCI Act applies protections to information collected or communicated in compliance with the Act. Each organisation that possesses protected information must only use or disclose that information under authorised circumstances.

3. Cyber Security

The responsible entity for a system of national significance must meet enhanced cyber security obligations. These include a requirement to prepare an incident response plan that will govern the entity's activities when a cyber security incident occurs.

In addition, the responsible entity for a system of national significance must conduct cyber security exercises and vulnerability assessments as directed by the Secretary.

4. Risk Management

The responsible entity for a designated asset must prepare a Critical Infrastructure Risk Management Program (CIRMP). The CIRMP must govern how the entity will mitigate and minimise the risks that arise from hazards affecting that asset.

Having adopted a CIRMP, the responsible entity must review and update the program routinely. The entity must submit annual reports of the state of the program to the Secretary.

5. Government Powers

The SOCI Act empowers the Minister and the Secretary to issue directions to relevant entities to achieve national security objectives. Compliance with directions is compulsory.

Each relevant entity must act in accordance with risk reduction directions and information requests. Relevant entities must also install monitoring software on computer systems in accordance with system information software notices.

The SOCI Act also establishes a regime designed to enable the government authorities to respond to serious cyber security incidents. When this regime is activated, the Minister and Secretary may issue directions designed to mitigate the impacts of recent, ongoing or imminent cyber security threats.

6. Telecommunications Sector

The Telecommunications Sector Security Reforms (TSSR) creates a regulatory framework to manage the security of Australia's telecommunications industry. Administration of TSSR is performed by CISC and the Office of the Communications Access Coordinator (CAC).

Carriers, carriage service providers (CSPs), carriage service intermediaries (CSPIs), and nominated carriage service providers (NCSPs) each have obligations under the TSSR. These obligations exist in parallel with an organisation's responsibilities as a relevant entity.

All organisations subject to the TSSR must take every reasonable step to secure their networks from unauthorised access and interference. Depending on their role under the TSSR, an organisation may also be required to notify authorities of planned network changes and comply with ministerial directions.

7. Financial Services Sector

Financial market infrastructures (FMIs) are the mechanisms and entities that enable trading in Australian capital markets. FMIs include important payment systems, central counterparties, trade repositories, and clearing and settlement facilities.

Relevant entities and other organisations that control an FMI must comply with resilience and security standards created by the Reserve Bank of Australia (RBA). FMI controllers must also notify the Australian Prudential Regulation Authority (APRA) or the Australian Securities and Investments Commission (ASIC) of significant security breaches.

Interactive Gambling

The *INTERACTIVE GAMBLING* obligations register informs operators of interactive gambling what their legal obligations are, and what procedures and processes they should have in place to ensure compliance with federal and state/territory requirements when offering or providing interactive gambling services in Australia.

This register comprehensively covers the types of interactive gambling activities that are allowed in Australia, how eligible operators can obtain a licence or authority to offer or provide interactive gambling services, and the legal obligations of licensed operators. It breaks the operator's legal obligations into the following topics:

- Interactive gambling services in Australia
- Interactive gambling licensing in the Australian Capital Territory
- Interactive gambling licensing in New South Wales
- Interactive gambling licensing in the Northern Territory
- Interactive gambling licensing in Queensland
- Interactive gambling licensing in South Australia
- Interactive gambling licensing in Tasmania
- Interactive gambling licensing in Victoria
- Interactive gambling licensing in Western Australia
- National Self-exclusion Register
- Players, prizes and winnings
- Interactive gambling taxes
- Interactive gambling advertising and marketing
- Responsible gambling and consumer protection measures
- Interactive gambling offences
- Anti-money laundering and counter-terrorism financing
- Financial reporting and record-keeping
- Interactive gambling investigations and enforcement by the ACMA
- Privacy and cyber security

INTERACTIVE GAMBLING addresses what the operator's legal obligations are when offering or providing interactive gambling services to customers in Australia, how the operator can obtain a licence or authority to offer or provide interactive gambling services to customers in Australia, what processes or procedures should be in place to ensure compliance and what the consequences are if the legal obligations are breached.

Marketing & Events

International AML-CFT Checklist

In November, we launched the International AML-CFT Compliance Checklist in Australia and New Zealand.

AML-CFT is a topic that continues to dominate the news headlines across the world. Penalties for non-compliance continue to escalate, the AML legal landscape constantly changes and the need to comply with AML-CFT regulations is more important than ever before.

This checklist helps your customers identify their international AML-CFT requirements. It covers AML-CFT Governance, Registration with AML-CFT Authorities, Due Diligence, Suspicious Matter & Reporting, and more.

Here is the link to share this whitepaper in Australia: **https://www.lexisnexis.com.au/en/insights-and-analysis/research-and-whitepapers/2022/your-free-international-aml-cft-checklist**

Here is the link to share this whitepaper in New Zealand: **https://www.lexisnexis.co.nz/en/insights-and-analysis/blogs/whitepaper/AML-CFT-Checklist**

PODCAST - Speaking of Compliance with Beau Murfitt, Camms

Demystifying ESG Reporting Frameworks

ESG (Environmental, Social, Governance) programmes are becoming more and more prevalent for businesses across the globe, but in Australia, there's no formal adoption requiring an organisation to prepare statements on how they're performing on ESG.

In this episode, our host Michael Nelson sits down with Beau Murfitt, Chief Strategy and People Officer with Camms, to discuss ESG in the Australia and New Zealand context, explore which frameworks are gaining momentum as the legislative landscape evolves, and steps your organisation can take to ensure your ESG programme aligns with the framework you report on.

Click the image below to listen on YouTube, and if you're interested in developing a podcast for your customers with us, please contact our Channel Partner Marketing Executive, Michele Fairbank at **michele.fairbank@lexisnexis.co.nz**.

Technical Changes

Corporations [7156] Module Updates - COMPLETE

The Customer Working Group has voted on the remaining set of obligations for the Corporations module, took place on 08/11/22. Please see below how the module will be restructured:

Date: 08/11/22

Module: Corporations [7156]

Topics:

* ASX Listing Rules [14910] – No change
* Companies Limited by Guarantees [22839]: To be archived
* Public Companies Limited by Shares [7253]: To be archived
* Proprietary Limited Companies [7205]: To be renamed to Company Formation and Operation, the Topic ID remains unchanged

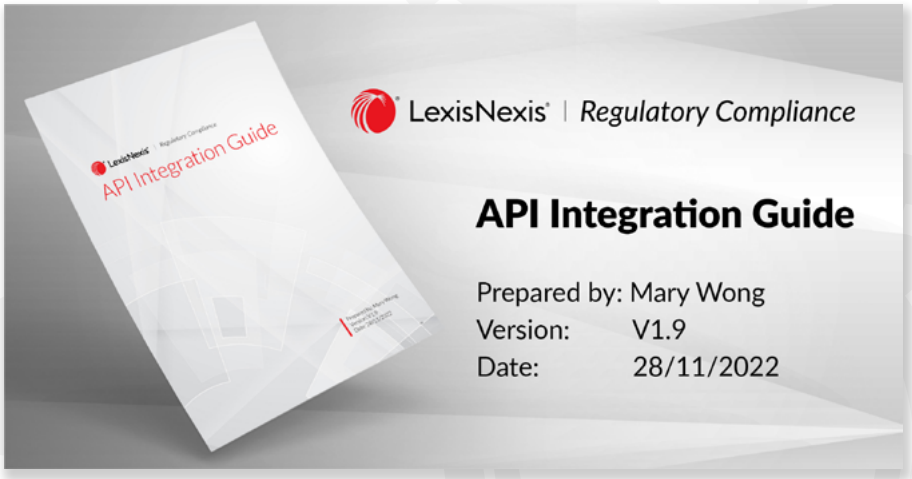
Subscription changes: None as the restructure is within 1 module

We have added a new parameter for the CSV output file to have BOM character included as part of the CSV download.

New API Guide for Channel Partners

The purpose of this document is to provide the REST APIs implementation methods which provide programmatic access to read LexisNexis subscription data by API customers.

DOWNLOAD HERE >>



Enquiries

Veronica Rios
Director, Global Associations and Strategic Partnerships
E: veronica.rios@lexisnexis.com.au

Mary Wong
Principal Product Manager
E: mary.wong@lexisnexis.com.au

Kieran Seed
Head of Content
E: kieran.seed@lexisnexis.com.au

Alex Smirniotis
Head of Marketing
E: alexander.smirniotis@lexisnexis.com.au

Michael Nelson
Senior Product Specialist
E: michael.nelson@lexisnexis.com.au

Monil Shah
Product Adoption Specialist
E: monil.shah@lexisnexis.com.au

W: https://www.lexisnexis.com.au/en/products-and-services/regulatory-compliance/channelpartner

About LexisNexis Regulatory Compliance

LexisNexis Regulatory Compliance is a legal obligations register and alerting solution that combines regulatory content with technology to empower you to take control of your compliance obligations.

LO012023MS