



Channel Newscast

July 2021 – Edition 7

Table of Contents

INTRODUCTION	3
PENALTY UNIT UPDATES.....	4
CHANGES TO WA GOVERNMENT SITE.....	6
MODULE DEDUPLICATION.....	7
CYBERSECURITY MODULE CHECKLIST CAMPAIGN	9
CHANNEL PARTNER TECHNICAL FORUM – JULY 2021.....	10



Introduction

Welcome to the LexisNexis Channel Partner newscast, a regular update on what is happening in the world of LexisNexis' Regulatory Compliance solution.

We will 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.

The newscast will be sent to our channel partners on a monthly basis, after the channel partner forum, so you can stay up to date with the latest topics under discussion.

Penalty Unit updates

The News Alerts have gone out notifying users of the upcoming changes, work to update the Consequences of the Obligations is due to commence on July 20th with an aim to have it completed by August 3rd .

List of impacted modules

- Aged Care
- Anti-Bribery & Corruption
- Anti-Money Laundering & Counter Terrorism Financing
- Asset Management
- Australian Credit Licence (Credit Providers)
- Australian Financial Services Licence (Product Issuers)
- Authorised Deposit-taking Institutions
- Building & Construction
- Charities
- Child Care & Education Services
- Clinical Care & Allied Health Services
- Commonwealth Tertiary Education
- Community Care & Services
- Compulsory Third Party Insurance
- Competition & Consumer
- Corporate Commonwealth Entities
- Credit Reporting
- Cybersecurity
- Education in Non-State Schools
- Electronic Transactions
- Employment
- Environment
- Facilities Management
- Finance & Leasing Companies
- Financial Advisory
- General Insurance
- Governance – VicTrack
- Government Employee Superannuation (Vic) ESSSuper
- Incorporation of Catholic Church Entities
- Infection Control, Disease Management & Biosecurity
- Institutional Investment

- Land & Property
- Life Insurance
- Modern Slavery
- Non-Corporate Commonwealth Entities
- Privacy & Data Protection
- Private Health Insurance
- Queensland Healthcare
- Queensland Local Government – Business & Economic Development
- Queensland Local Government – Events & Recreation
- Queensland Local Government – Governance, Administration & Integrity
- Queensland Local Government – Land Use, Planning, Development & Building Control
- Queensland Local Government – Local Government Finance
- Queensland Local Government – Management of Public Lands & Property
- Queensland Local Government – Public Health & Other Community Services
- Queensland Local Government – Roads & Infrastructure Management
- Queensland Local Government – Waste & Environment Management
- Queensland State Government Entities
- Queensland Water Supply Management
- Retail
- Social Media
- Tax
- Transport & Infrastructure
- Transport & Logistics
- Victorian Local Government
- Victorian State Government
- Workers Compensation Insurance
- Workplace Health & Safety

Changes to WA Government site

Upon detailed review, it was determined that it only impacted the Western Australia State Government module; work to update the Compliance Sources of the Obligations is due to commence on July 20th with an aim to have it completed by August 3rd

Module Deduplication

Updated timeline for Module Deduplication:

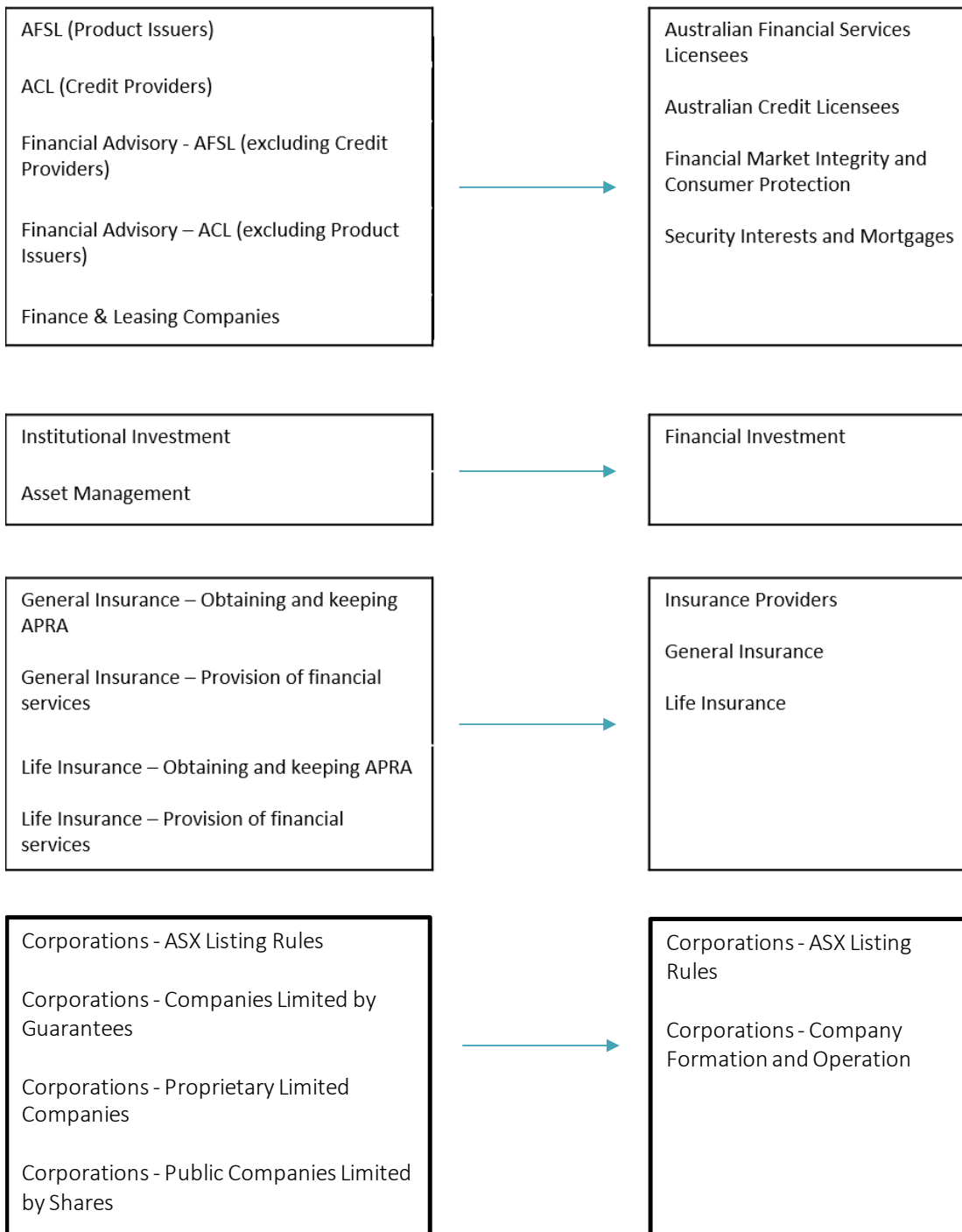
Aug: Customer validations

Aug: Partner workshops – for those where we have mutual customers and their subscriptions are impacted by this

Sep: Go/No Go

If we decide is to proceed then detailed rollout planning will take place in Oct.

Module Deduplications



Cybersecurity Module Checklist Campaign

- Cybersecurity issues continue to impact businesses in Australia and globally.
- Cybersecurity is a module in the Regulatory Compliance content set. This content set includes Australia, NZ, US, UK, Japan, China, HK and Singapore.
- For this campaign, we will share this checklist with the GRCI, RMIA and social media.
- Welcome to share this via Social / Campaign / Sales Enablement Tool.



CYBERSECURITY CHECKLIST

This checklist has been designed to help you identify your cybersecurity requirements.

ASSET MANAGEMENT

Requirement	Needs work	Don't know	Meets requirement
Does the organisation maintain an inventory of all physical devices and systems that store or transmit information on its network?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Does the organisation customise the capabilities of its system inventory to meet its digital security objectives?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Does the organisation maintain a trusted software inventory?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Does the organisation implement controls that are designed to ensure that only trusted software can run on its network?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Does the organisation maintain a current map of the boundaries of its data flow and digital communications network?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Does the organisation customise its data mapping systems and processes to meet its digital security objectives?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Does the organisation maintain a catalogue of external information systems that represent potential threats to digital security?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Does the organisation customise its external information system catalogue to meet its digital security objectives?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Does the organisation assess and categorise the sensitivity of all its digital resources?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Does the organisation define and assign digital security roles and responsibilities to every member of staff and every third party stakeholder?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Does the organisation ensure that each member of staff and each third party stakeholder is aware of their digital security role and is equipped to meet their responsibilities?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

4

Channel Partner Technical Forum – July 2021

The July Channel Partner Technical Forum was held on Wednesday 21st July. Thanks to all who attended. For anyone unable to attend, the recording is available [here](#).

The next Channel Partner Technical Forum is scheduled for Wednesday 18th August.

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

Senior Content Manager

E: kieran.seed@lexisnexis.com.au

Alex Smirniotis

Marketing Manager

E: alexander.smirniotis@lexisnexis.com.au

Michael Nelson

Product Specialist

E: michael.nelson@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.