A&O Consulting

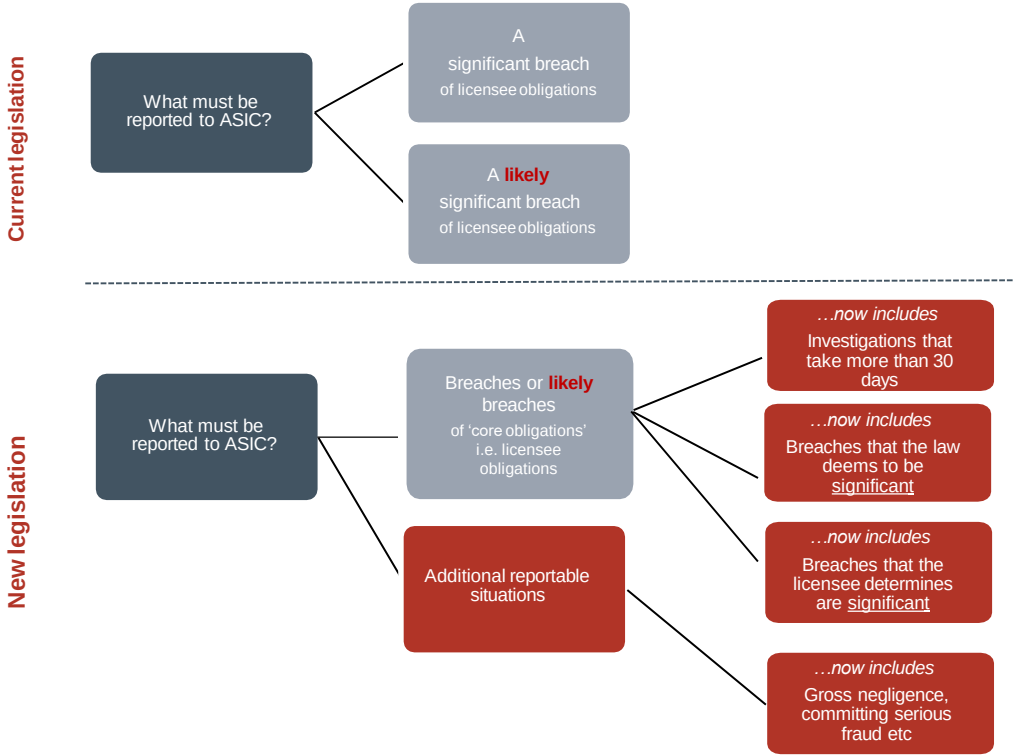
Business integrity from ALLEN & OVERY

Planning your response to the new Breach Reporting regime

June 2021

Sizing the challenge

Financial service organisations have always operated in a complex compliance regime, where breaches will inevitably occur. However, under the new regime, **even minor or technical breaches may now trigger mandatory self-reporting**.



Key points

- From 1 October 2021, AFS licensees and credit licensees must self-report any breaches or likely breaches of a core obligation, as well as additional reportable situations.
- Core obligations are defined in s912A of the Corporations Act for AFS licensees, and s50A(3) of the National Credit Act for credit licensees.
- The reporting timeline has been increased from 10 business days to 30 calendar days. Licensees must lodge breach reports within 30 days after the licensee first knows that, or is reckless with respect to whether, there are reasonable grounds to believe a reportable situation has arisen.
- Importantly, a new class of breaches is being introduced which is automatically taken (i.e. "deemed") to be significant. One major bank forecasts this change will increase the volume of its mandatory self-reporting **twenty-fold**.
- In addition, AFS licensees and credit licensees will also be required to self-report any breach investigation that continues for more than 30 days. This provision is designed to promote speedy internal investigations.
- The time at which an investigation commences is a 'matter of fact and is not a matter for subjective determination by the licensee'.

Key changes to consider

ASIC has released a draft regulatory guide (Regulatory Guide 78) and a draft information sheet (Information Sheet 000) with proposed guidance. The key takeaway? Acting quickly and decisively is essential.

Compliance impact of the expanded concept of 'reportable situation'

- With the vastly expanded breadth of matters that will now be subject to regulator scrutiny, many licensees need to enhance incident management processes – in particular those documenting identification, investigation and remediation processes, as well as determinations of additional reportable situations and significance.
- A point of keen industry interest will no doubt be ASIC's evolving expectations for batch reporting. In instances where a single system error in high frequency areas (such as trade reporting) produces multiple technical breaches, individual reporting will be burdensome for licensees and the regulator alike.

Introduction of an objective test ('deemed significance')

- A recommendation from the ASIC Enforcement Taskforce Review observed that licensees making a qualitative assessment of a breach or likely breach led to delays and inconsistencies in reporting. The new 'deemed significant breaches' reporting obligation ensures a reduced scope for subjectivity, establishing a class of breaches which are automatically taken to be significant.
- **Deemed significant breaches include breaches:**
  - of a civil penalty provision (e.g. failure to maintain adequate PI insurance)
  - of s1041H(a) of the Corporations Act / s12DA(1) of the ASIC Act (misleading or deceptive conduct); or
  - that result, or are likely to result, in material loss or damage to clients, or to members of a managed investment scheme or superannuation entity
- This, coupled with the increased volume of reports, will no doubt impact the model of centralised Breach Reporting Forums currently used by some licensees. For large licensees in particular, we expect to see a continued shift towards First Line Teams owning day-to-day breach reporting processes and regulator engagement, supported by Second Line expertise and oversight.

Requirement to report investigations that continue for more than 30 days

- Delays in breach reporting was a theme pointedly covered in the Royal Commission commentary, and this provision incentivises prompt internal processes as licensees seek to minimise reporting triggered by this new requirement.
- The term 'investigation' is not defined. In the draft regulatory guide, ASIC provided that a relevant factor to having conducted an investigation is whether there has been some information gathering or human effort applied by the licensee to determine whether a breach has occurred.
- Operationally, licensees will need to have a clear map of process and pressure points that will impact ability to complete investigations within the 30 days. This may mean building new, or significantly uplifting existing, incident management systems.

Prescribed form for breach reports

- There have been early indications from ASIC on prescribed form, with the draft Regulatory Guide setting out an overview of the reportable situation form.
- Licensees will need to consider how they configure their systems to capture information in ways that align with these prescribed fields for efficient process.
- Deviations from the prescribed form are unlikely to be permitted (or well received).

Customer communications

- In addition to the new obligations to report breaches to ASIC, there are also notify, investigate and remediate requirements relating to suspected misconduct of financial advisors and mortgage brokers.
- These client notification requirements reaffirm that these areas remain squarely in the cross-hairs as problem areas for policy makers and regulators.

The risks of non-compliance

The strengthening of the legislation has resulted in heightened risks of non-compliance.

The obligation

Each AFS licensee and credit licensee has a legal obligation to self-report if there are reasonable grounds to believe a reportable situation has arisen.

The penalties

The maximum civil penalty for not reporting a reportable situation in accordance with your obligation as an AFS licensee or credit licensee is:

a) *For an individual* – the greater of 5,000 penalty units and 3X the benefit derived and detriment avoided

b) *For a body corporate* – the greatest of:

- 50,000 penalty units;
- 3X the benefit derived and detriment avoided; and
- 10% of the annual turnover for the 12-month period ending at the end of the month in which the body corporate contravened (capped at 2.5 penalty units).

The broader consequences

Visibility of the Licensee

ASIC has been clear that robust breach arrangements are a critical component of adequate risk management systems. Further, it considers that unreasonable reporting delays may indicate an organisation does not have adequate compliance processes, systems and resources in place, itself amounting to a breach of s912A.

Visibility to the regulator

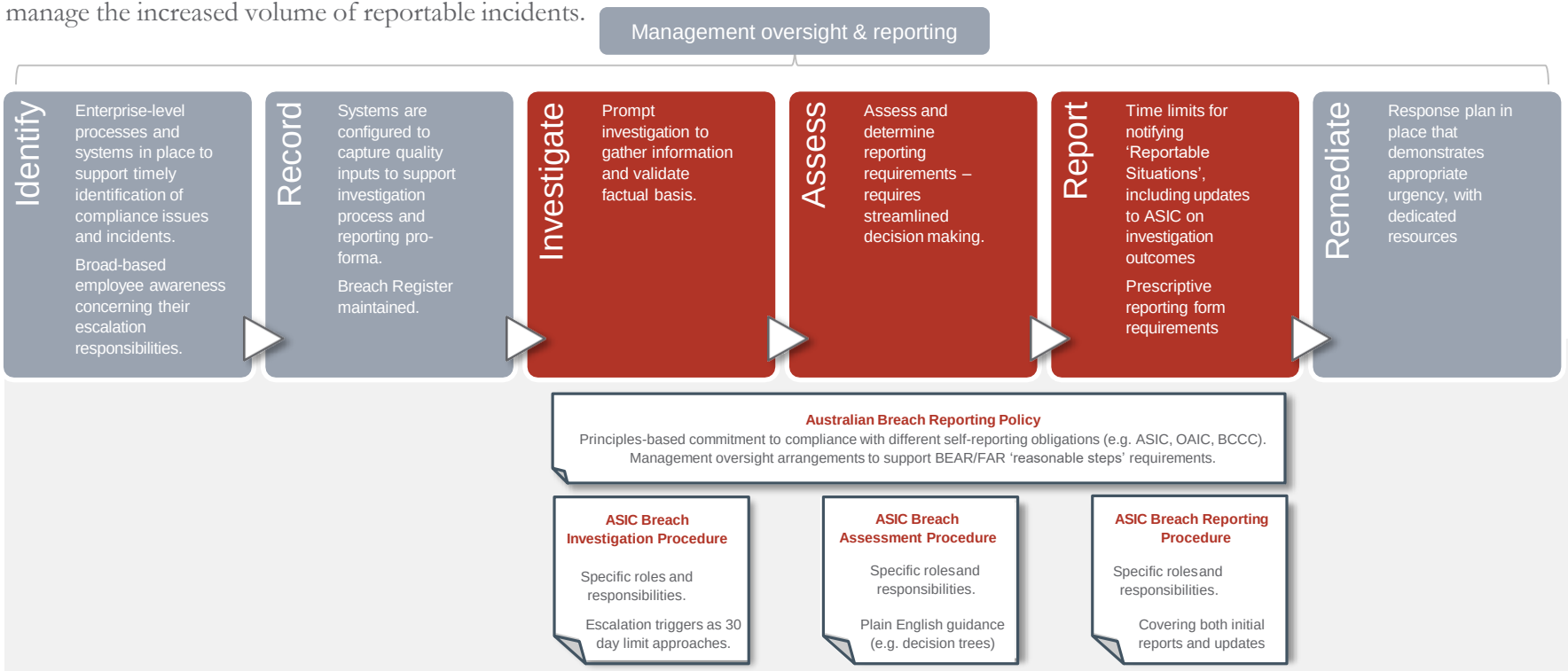
ASIC will be leveraging data analytics capabilities across breach reporting data to identify systemic and repeat issues, both within a corporate group and across industry. Licensees need to ensure they are proactively self-identifying breaches, undertaking timely remediation (especially customer remediation) dealing with root causes and monitoring for emerging thematics – before the regulator does.

Visibility to the community

It is not yet clear exactly what ASIC's publication of the breach reporting information will look like. Noting the stated legislative intent to 'enhance accountability and provide an incentive for improved behaviour', it is fair to assume that data will be presented in a way that will enable individual licensees to be identified as outliers.

Planning your response

The new breach reporting obligations will impact several stages of the incident management lifecycle. The greatest impact will be in the Investigation, Assessment and Reporting stages. For many licensees, existing processes and systems will need significant improvements to manage the increased volume of reportable incidents.



How we can help you

There are a number of ways A&O Consulting can support your response to the new breach reporting requirements.
Please reach out to us if you'd like more information on the below services, or just to chat about the type of support you may need.

Here are some of the ways A&O Consulting can help:

- ✓ Review your global incident management framework, and develop a complementary **Australian Breach Reporting Policy** relating to your Australian operations
- ✓ Develop an **ASIC Breach Investigation Procedure** customised to your operational requirements
- ✓ Develop an **ASIC Breach Assessment Procedure** including plain English guidance on the new requirements in a user-friendly format – (e.g. decision-trees). The Procedure will cover both statutory requirements and regulatory guidance
- ✓ Develop an **ASIC Breach Reporting Procedure** customised to your operational requirements. The Procedure will cover both statutory requirements and regulatory guidance
- ✓ Develop **enterprise-level training materials** covering each employee's general incident identification responsibilities, as well as the key aspects of the new Breach Reporting regime, so they understand the significance of their responsibilities
- ✓ **Deliver enterprise-level training** – in person or remotely (depending on location)
- ✓ Develop **1LoD and/or 2LoD-focused training materials** covering procedural roles and responsibilities relating to Breach Investigation, Breach Assessment and Breach Reporting. The proposed workshop format will contain a number of scenario-based interactive exercises, with the proposed deliverable format being a powerpoint deck and full speaking notes
- ✓ **Deliver 1LoD and/or 2LoD training** (face-to-face) in your required locations.

Reach out to our team:

Lee Alam
Managing Director
Tel +61 2 9373 7722
lee.alam@allenovery.com

Kate Morris
Executive Director
Tel +61 2 9373 7721
kate.morris@allenovery.com

Rosie Williams
Senior Consultant
Tel: +61 2 9373 7656
rosie.williams@allenovery.com