CLEVELAND & CO
External in-house counsel

APRA's Reminder on Information Security Requirements

Background

The Australian Prudential Regulation Authority ("**APRA**") has issued a newsletter stressing the importance of placing focus on cyber security whilst conducting independent tripartite cyber assessments on its regulated entities. These assessments aim to ensure that these entities possess the necessary infrastructure to effectively withstand cyberattacks and security threats. Despite being in the process of conducting assessments on around 300 banks, insurers and superannuation trustees, APRA has already noticed the need to remind firms to enhance their cyber resilience and "raise the bar" on their security measures.

Six Findings

APRA has completed around 25% of the full assessment projects and has identified six gap obligations under Prudential Standard CPS 234 Information Security ("**CPS 234**").

1. APRA identified incomplete identification and classification of information assets. To address this, they proposed three suggestions: i) Develop asset classification policies and criteria that consider potential impacts from security breaches, ii) Use information asset inventory repositories for easy asset registration and mapping, and iii) Consider data asset's highest criticality and sensitivity ratings of its constituent components.
2. APRA highlighted the need for better assessment of third-party information security capability. With increased reliance on service providers to manage critical systems, APRA suggests that firms gain an understanding on these providers' capabilities on information security controls by conducting interviews and surveys.
3. APRA identified issues with inadequate definitions and execution of control testing programs. This includes deficiencies like lack of independence and consistency in testing approaches. Firms should reevaluate their testing criteria and approaches.
4. APRA often found incident response plans lacking regular reviews or testing. Additionally, some plans either weren't in place or lacked clearly defined roles and responsibilities.
5. APRA found limited internal audit reviews of information security controls, including third-party-operated controls. In some cases, internal auditors lacked sufficient information to conduct such audits. To address this, APRA suggested implementing adequate board reporting and other measures.
6. APRA noticed inconsistent and untimely reporting of material incidents and control weaknesses. They suggested implementing clear escalation procedures and mechanisms to identify material control weaknesses like control testing and assurance activities.

Next Steps

APRA-regulated entities may need assistance in reviewing their existing processes to ensure compliance with APRA's requirements. They may also need guidance on the level of adequacy required under CPS 234. To read the full newsletter, please click here.

For more information on the information security requirements, Cleveland & Co External in-house counsel™, your specialist outsourced legal team, are here to help.

If you need any help or further information, please contact Tanja Listar:

Tanja Listar - Managing Director, General Counsel APAC
+61 466778482
tlistar@cleveland-co.com

https://cleveland-co.com/
https://uk.linkedin.com/company/cleveland-co