WHAT YOU NEED TO KNOW ABOUT APRA'S PRUDENTIAL STANDARD CPS234 INFORMATION SECURITY

Amstelveen

Who It Applies To

The Standard applies to all APRA regulated entities, which include authorised deposit-taking institutions, general insurers, parent entities of Level 2 insurance groups, life companies, private health insurers and Registrable Superannuation Entity licensees under the Superannuation Industry (Supervision) Act 1993.

Why It's Important

APRA regulated entities manage sensitive information assets. The Standard is aimed at minimising the likelihood and impact of information security incidents, inclusive of those that could occur with related or third parties.

How To Prepare

Key areas to review to prepare effectively for the Standard's implementation are ensuring roles and responsibilities are clear, including those to be performed by the Board, and that systems and processes are in place to enable effective control management, control testing, incident management and regulatory notifications within stipulated timeframes.

When It Applies From

The Standard comes into effect from 1 July 2019. Where an APRA regulated entity's information assets are managed by a third party, then it will apply to those assets from the earlier of either the contract renewal date or 1 July 2020.

What Processes Are Needed

Information security policy frameworks need to be matched to the threat landscape presented to be effective. This requires an information security focus within processes such as incident management, regulatory notifications and the identification, management and testing of controls.

What Capabilities Are Needed

Information security skill and knowledge is required at all levels, including within the Board and internal audit. It is critical that entities match and maintain their resources with the threat landscape that they face, including that related or third parties meet the required standards. This includes ensuring the appropriate capabilities for testing and audit are met.