

# CORRS IN BRIEF

MAY 2009



## IT SECURITY RISK

The Australian Prudential Regulation Authority (APRA) has issued a discussion paper on the management of IT Security Risk. APRA is concerned that the compromising of an APRA regulated institution's IT assets could have a significant detrimental impact on the institution's reputation and could result in a failure to meet key business objectives, including compliance requirements.

APRA has issued a draft prudential practice guide (PPG) and is seeking comment by 5 June 2009. APRA intends issuing a final version of the PPG later in 2009 when it will become binding on APRA regulated institutions.

The PPG is split into eight sections and has five appendices. This article deals with each in turn below.

### IT SECURITY RISK

The PPG defines IT security risk as the potential compromise of a regulated institution's IT assets in relation to:

- (a) **confidentiality:** only authorised access permitted;
- (b) **integrity:** completeness, accuracy and freedom from unauthorised change;
- (c) **availability:** accessibility and usability when required; and
- (d) **accountability:** the ability to attribute the responsibility for an action.

APRA considers that a compromise of one of more these attributes can have a detrimental impact on a regulated institution's IT assets and reputation. The remaining sections of the guide are designed to prevent this from occurring.

### AN OVERARCHING FRAMEWORK

The PPG when implemented will require regulated institutions to maintain a full IT security management framework. APRA sets out a number of common security principles which it envisages regulated institutions should follow. Some examples include timely detection of security breaches, segregation of duties (to prevent one person compromising IT assets) and denial of all features and permissions not required by an individual to conduct their business functions.

APRA has also suggested a number of security policies which regulated entities should establish, such as policies on the selection of staff, acceptable use of IT assets and identification and authorisation.

Regulated institutions will also be required to regularly assess security threats and vulnerabilities and test the effectiveness of its IT security framework. Institutions would need to make any adjustments to the framework as may be necessary from time to time.

### ACCEPTABLE USAGE AND USER AWARENESS

The PPG suggests that institutions would benefit from developing an ongoing security training and awareness program for all of its users. Users would also be required to comply with IT security policies in place from time to time.

### IDENTIFICATION, ACCESS AND AUTHORISATION

APRA considers that regulated entities would normally take appropriate measures to authenticate the identity of users or IT assets. Users would only be granted access where a valid business need exists. The type of authentication required

would normally be commensurate with risk. APRA considers the following scenarios to be situations where a high level of authentication would be required:

- (a) administration or other privileged access to sensitive or critical information assets;
- (b) remote access to sensitive or critical information assets; and
- (c) high-risk activities (eg third part fund transfers).

## LIFE-CYCLE MANAGEMENT CONTROLS

APRA considers that security be considered throughout the lifecycle of each IT asset. Lifecycle stages typically include planning and design; acquisition and implementation; support and maintenance and decommission and disposal. Physical security of IT assets is also considered important, and would normally be commensurate with the sensitivity and criticality of the assets.

## MONITORING AND INCIDENT MANAGEMENT

The PPG sets out some common monitoring processes that regulated institutions would normally have in order to identify events and unusual patterns of behaviour that could impact on the security of IT assets. This would include extensive audit trails.

Incidents are events that potentially compromise the confidentiality, integrity, availability or accountability of IT assets. APRA envisages that regulated institutions manage all stages of the incident lifecycle, from detection to resolution and preventing similar events occurring.

## SECURITY REPORTING AND METRICS

Regulated institutions would be expected to regularly report on the effectiveness of their IT security framework. Metrics could also be used to measure the success of the framework.

## SECURITY ASSURANCE

APRA expects that a regulated institution would seek regular assurance that its IT assets are appropriately secured and that its IT security management framework is effective. This may be conducted by internal audit or appropriately trained independent security experts.

## ATTACHMENTS

The PPG includes the following schedules:

- (a) **Change Management:** ensuring that IT security is maintained throughout any change to an institution's IT environment;
- (b) **Resilience and Recovery:** ensuring that systems remain available, and ensuring that the IT environment can be recovered;
- (c) **Service Provider Management:** ensuring IT security risks are appropriately managed regardless of whether the IT assets are under the direct control of a regulated institution or have been outsourced to a service provider (IT service providers could therefore be required to comply with the new guidelines);
- (d) **Secure Software Development:** security considerations should be included throughout the software development life-cycle; and
- (e) **Customer Protection:** advising customers how to protect themselves against theft and fraud.

## CONCLUSION

The new PPG is a detailed set of requirements which APRA believes that a prudent regulated institution would normally fulfil. Most institutions are fulfilling many of these requirements and for them the introduction of the final PPG will be a gap analysis process to ensure compliance. Its introduction may cause more issues for IT service providers. It is likely that regulated institutions will require IT service providers to comply with the PPG in future.

**For further information, please contact:**

Sydney  
James North  
Partner  
Tel +61 2 9210 6734  
james.north@corrs.com.au

Melbourne  
Philip Catania  
Partner  
Tel +61 3 9672 3333  
philip.catania@corrs.com.au

Brisbane  
Eddie Scuderi  
Partner  
Tel +61 7 3228 9319  
eddie.scuderi@corrs.com.au