SECURITY FRAMEWORK FOR APRA
AUSTRALIAN PRUDENTIAL REGULATORY AUTHORITY (APRA) GUIDELINES
EXECUTIVE SUMMARY
The Australian Prudential Regulatory Authority (APRA) CPS 231 Outsourcing\(^1\) and SPS 231 Outsourcing\(^2\) in August 2014 and November 2012 respectively, documented requirements relating to the risk management of outsourcing arrangements including cloud computing. More recently as of July 2015, given the increased demand of cloud, APRA has revised these arrangements and identified mitigation techniques documented in an Information Paper titled, “Outsourcing Involving Shared Computing Services (Including Cloud).” The Information Paper outlines key principles that should be considered when contemplating the use of shared computing services and cloud.

Given the sheer number of service configurations available with the AWS platform, many financial services institutions (FSIs) may question whether their AWS implementation will address the APRA guidelines. The “Accenture Security Framework for AWS – APRA Guidelines” whitepaper outlines the technology controls set out by the APRA Information Paper and describes the AWS services and third-party products that can be implemented to address the APRA technology control guidelines set out in CPG 234 – “Management of Security Risk in Information and Information Technology,”\(^3\) as they pertain to the Information Paper. The methodology used to come up with the security controls aligns closely with the holistic AWS Cloud Adoption Framework (CAF).

The Accenture Security Framework for AWS provides a mechanism for FSIs to:

- Adopt AWS services and use them in a manner that helps organisations address the technology-compliant controls described within the APRA guidelines.
- Secure both sensitive and non-sensitive data as setup and classified pertaining to CPG 235 – “Managing Data Risk,”\(^4\) while leveraging the flexibility, agility and cost savings of the cloud.

Based on the experience of both Accenture Security and Cloud Architects for AWS, the full report: 1) outlines a simplified approach to implement the appropriate AWS services and platform and 2) summarises the applicable AWS services and how they can be arranged to help FSIs address the key controls listed for each of the technology key control requirements described in the CPG 234 document.

**Guiding Principles for Accenture Security Framework for AWS**

The Accenture Security Framework for AWS’s overarching principle is to leverage agile development methodologies coupled with AWS services. The Framework also provides FSIs with the confidence to manage material workloads in AWS by employing security controls that provide the same mechanisms FSIs are accustomed to in their own environments, specifically aligned to the areas recommended by APRA.

The Framework guides the creation of a cloud-based environment for material workloads that follows traditional IT security models, leveraging an enterprise’s existing tools and processes. Using the AWS platform, the FSI can continue to leverage its existing investments and build an effective approach to security in the cloud.

Agile methodologies for application development and continuous integration provide enterprises with new approaches to managing security in the cloud. The Framework’s guiding principle for data security focuses on how to manage “infrastructure as code” through the software development and deployment lifecycle. Application and infrastructure development and configuration changes are fed

---

\(^1\) [Prudential Standard CPS 231 for Outsourcing](#) - This Prudential Standard requires that all outsourcing arrangements involving material business activities entered into by an APRA-regulated institution be subject to appropriate guidelines documented.

\(^2\) [Prudential Standard SPS 231 for Outsourcing](#) - This Prudential Standard requires that all outsourcing arrangements involving material business activities entered into by a RSE licensee be subject to appropriate due diligence, approval and ongoing monitoring.

\(^3\) [Prudential Practice Guide - CPG 234 – Management of Security Risk in Information and Information Technology](#)

\(^4\) [Prudential Practice Guide - CPG 235 – Managing Data Risk](#)
into the template and a completely new environment is built rather than making changes to an existing environment. This approach also enables new ways to perform resilience, disaster recovery and backups.

### Overview for Accenture Security Framework for AWS

The Accenture Security Framework for AWS employs a layered approach to security, building on security features as required by the particular workload. These include controls for: network flow (see Figure 1); data protection/access management (see Figure 2); and auditing and configuration management (see Figure 3).

**Figure 1:** Network flow controls

**Figure 2:** Data protection and access management

**Figure 3:** Auditing and configuration management

### APRA Key Technology Controls Overview

The APRA key technology controls are summarised below in the table below, which focuses on the Access Control technology components as they pertain to the technology controls described in the CPG 234 in descriptive nature against the Accenture Security Framework for AWS and the AWS services used to address the controls.

### Conclusion

The Accenture Security Framework for AWS helps provides the Financial Services sector with the confidence to build out a secure and resilient AWS platform to support all workloads within the organisation, in order to manage their data securely while supporting the adoption of cloud-native development and security techniques.
<table>
<thead>
<tr>
<th>Outsourcing Involving Shared Computing Services</th>
<th>APRA CPG 234 Technology Risk Controls</th>
<th>Accenture Security Framework for AWS Component</th>
<th>AWS Services</th>
<th>Third-Party Services</th>
</tr>
</thead>
</table>
| Controls | Data Protection and Access Controls  
- Role-Based Access Controls  
- Externalisation of Keys  
- Authentication and Access Controls | AWS IAM Users  
AWS IAM Roles  
AWS IAM Keys  
AWS CloudHSM  
AWS Key Management Service (KMS) |  |
| Identification and Authentication Techniques | Data Protection and Access Controls  
- Role-Based Access Controls  
- Externalisation of Keys  
- Authentication and Access Controls | AWS IAM Users  
AWS IAM Roles  
AWS IAM Keys  
AWS CloudHSM  
Security Assertion Markup Language (SAML)  
Multi-Factor Authentication Network Address Translation (NAT) Gateway  
AWS KMS  
AWS CloudTrail | Ping  
Microsoft Active Directory  
[operating system authentication] Bastion Host Remote Desktop |
| Data Leakage | Data Protection and Access Controls  
- Encryption and Tokenisation  
- Encrypted Storage Volumes  
- Encryption in Transit | AWS CloudHSM  
AWS KMS  
Amazon EBS Full Disk Encryption  
Amazon S3 Encryption  
AWS Certificate Manager |  |
| Cryptographic Techniques to Restrict Data | Data Protection and Access Controls  
- Encryption and Tokenisation | Amazon Relational Database Service (RDS)  
EBS Full Disk Encryption  
AWS CloudHSM  
AWS KMS | Native DN Transparent Database Encryption CipherCloud |
| IT Asset Lifecycle Management Controls | Auditing and Configuration Management  
- Tamper-Proof Metrics | AWS Compliance Reports |  |
| Physical Security | Auditing and Configuration Management  
- Tamper-Proof Metrics |  |  |
| Secure Software Development | Auditing and Configuration Management  
- Configuration and Change Management  
- Continuous Deployment  
- Hydration | AWS  
CodeCommit  
AWS CodeDeploy  
AWS CodeWorkflow  
Auto Scaling groups  
AWS CloudWatch  
AWS CloudFormation | GitHub  
Jenkins |
<table>
<thead>
<tr>
<th>Outsourcing Involving Shared Computing Services</th>
<th>APRA CPG 234 Technology Risk Controls</th>
<th>Accenture Security Framework for AWS Component</th>
<th>AWS Services</th>
<th>Third-Party Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>Legacy Technologies</td>
<td>Separation and Flow Controls</td>
<td>IAM Accounts Amazon Virtual Private Cloud (VPC) Security Groups</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Emerging Technologies</td>
<td>Separation and Flow Controls</td>
<td>IAM Accounts Amazon VPC Security Groups</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Monitoring and Incident Management</td>
<td>Monitoring Process</td>
<td><strong>Auditing and Configuration Management</strong>&lt;br&gt;• Alarms and Actions</td>
<td>AWS CloudWatch AWS CloudTrail</td>
<td>Nagios ZenOss Splunk</td>
</tr>
<tr>
<td>Incident Management</td>
<td><strong>Auditing and Configuration Management</strong>&lt;br&gt;• Alarms and Actions&lt;br&gt;• Log and Capture Flows&lt;br&gt;• Configuration and Change Management</td>
<td>AWS CloudWatch AWS CloudTrail Amazon AMI Amazon Snapshot AMI</td>
<td></td>
<td>Splunk</td>
</tr>
<tr>
<td>Accountability and Audit Trails</td>
<td><strong>Auditing and Configuration Management</strong>&lt;br&gt;• Alarms and Actions&lt;br&gt;• Log and Capture Flows</td>
<td>AWS CloudWatch AWS CloudTrail</td>
<td></td>
<td>Splunk CyberArk PUAM QualysGuard</td>
</tr>
<tr>
<td>IT Security Reporting and Metrics</td>
<td>Regular Reporting</td>
<td><strong>Auditing and Configuration Management</strong>&lt;br&gt;• Alarms and Actions&lt;br&gt;• Log and Capture Flows</td>
<td>AWS CloudWatch AWS CloudTrail</td>
<td>Splunk</td>
</tr>
<tr>
<td>Effective Security Metrics</td>
<td><strong>Auditing and Configuration Management</strong>&lt;br&gt;• Alarms and Actions&lt;br&gt;• Log and Capture Flows&lt;br&gt;• Tamper-Proof Metrics</td>
<td>AWS CloudWatch AWS CloudTrail</td>
<td></td>
<td>Splunk</td>
</tr>
</tbody>
</table>
**Contact**
Campbell Abbey, Accenture AWS Business Group, APAC lead, Accenture
email: c.abbey@accenture.com

**About Accenture**
Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions – underpinned by the world’s largest delivery network – Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With more than 394,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives. Visit us at www.accenture.com.

**About Accenture AWS Business Group (AABG)**
The Accenture AWS Business Group, a jointly invested relationship between AWS and Accenture, offers integrated consulting and technology solutions designed to help enterprise clients throughout the globe, take advantage of the flexibility and economics of an “as-a-service” operating model where IT and business services are delivered on-demand, via the AWS Cloud. Visit AABG at www.accenture.com.au/accentureaws

This document makes descriptive reference to trademarks that may be owned by others. The use of such trademarks herein is not an assertion of ownership of such trademarks by Accenture and is not intended to represent or imply the existence of an association between Accenture and the lawful owners of such trademarks.

Copyright © 2017 Accenture. All rights reserved. Accenture, its logo, and High Performance Delivered are trademarks of Accenture.