

Response To Australian Prudential Regulatory Authority (APRA) Information Paper – Outsourcing Involving Cloud Computing Services

VMware Cloud on AWS

Table of contents

Introduction	3
VMware Cloud on AWS	3
Chapter 1 - Risks Must Be Understood And Managed	4
Chapter 2 - Risk Management Considerations	5
Chapter 3 - Apra Notification And Consultation	13
Conclusion	14

APRA – OUTSOURCING INVOLVING CLOUD COMPUTING SERVICES

- Chapter 1 – Risks must be understood and managed
 - Risks are a function of usage
 - Assessment of materiality
- Chapter 2 – Risk management considerations
 - Strategy
 - Governance
 - Solution selection process
 - APRA access and ability to act
 - Transition approach
 - Risk assessments and security
 - Implementation of controls
 - Ongoing oversight
 - Business disruption
 - Audit and assurance
- Chapter 3 – APRA notification and consultation
 - Materiality and notification
 - Consultation

Introduction

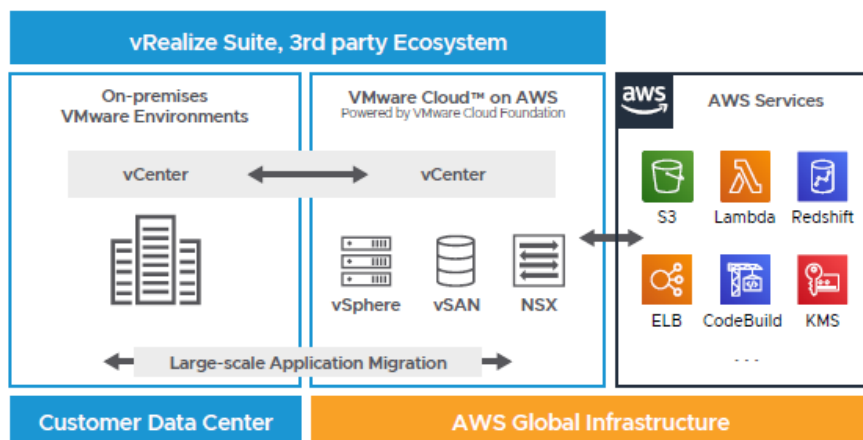
The Australian Prudential Regulation Authority (APRA) released the “Information Paper: Outsourcing involving cloud computing services” in September 2018 to provide guidance to regulated financial entities about cloud computing.

This document contains the VMware Cloud on AWS response to the Information Paper to demonstrate how Australian financial services organizations can leverage VMware Cloud Services to address APRA’s requirements for outsourcing.

VMware Cloud on AWS

VMware Cloud on AWS brings VMware’s enterprise class Software-Defined Data Center software to the AWS Cloud, and enables customers to run production applications across VMware vSphere-based environments, with optimized access to AWS services. Jointly engineered by VMware and AWS, this on-demand service enables IT teams to seamlessly extend, migrate and manage their cloud-based resources with familiar VMware solutions without the hassles of learning new skills or utilizing new tools. VMware Cloud on AWS integrates VMware’s flagship compute, storage and network virtualization products (VMware vSphere, VMware vSAN and VMware NSX) along with VMware vCenter management optimized to run on dedicated, elastic, Amazon EC2 bare-metal infrastructure that is fully integrated as part of the AWS Cloud. This service is delivered and supported by VMware and its partner community. With the same architecture and operational experience on-premises and in the cloud, IT teams can now quickly derive instant business value from use of the AWS and VMware hybrid cloud experience.

VMware Cloud on AWS enables enterprise IT and operations teams to innovate, transform, and add value to the business while continuing to leverage their VMware expertise and without the need to purchase new hardware. With VMware Cloud on AWS you can quickly and confidently migrate applications currently deployed in on-premises and co-located data centers usually without refactoring. In addition, applications deployed in VMware Cloud on AWS become much easier to modernize with high-speed low-latency access to native cloud services from AWS.



CHAPTER 1 - RISKS MUST BE UNDERSTOOD AND MANAGED

APRA REQUIREMENT	VMWARE CLOUD ON AWS RESPONSE
<p>Risks are a function of usage</p> <p>APRA regulated entities should ensure that risks associated with outsourcing arrangements are understood, managed and reported.</p>	<p>Cloud Computing has served as a cornerstone for digital transformation by facilitating innovation and competitiveness, speeding development and providing agile and elastic infrastructure scalability. While the benefits of cloud computing are many, organizations should ensure that the IT assets on cloud are managed in a secure and reliable manner. APRA emphasizes that risks associated with cloud computing and outsourcing arrangements should be understood adequately to ensure that APRA regulated entities can demonstrate operational continuity, maintain data confidentiality, and comply with applicable laws and regulations.</p> <p>VMware supports APRA's view of the importance of adequately understanding risks and supports our customers in meeting APRA's requirements through the VMware Cloud on AWS solution. The solution provides customers with a unique hybrid cloud opportunity that enables workloads to run as easily in a hyperscale environment as they do on-premises, all managed with consistent infrastructure, networking, and security through a single management plane. VMware Cloud on AWS supports a variety of use cases including datacenter consolidation, datacenter extension, application modernization, and disaster recovery. Depending on the nature of the use case, APRA regulated entities should evaluate the risks associated with VMware Cloud on AWS, develop a risk management plan and regularly apprise senior management of the key risks.</p> <p>Security and risk management considerations have been built into VMware Cloud on AWS to ensure risk associated with confidentiality, integrity, and availability are addressed by design. VMware has also implemented a number of security policies for VMware Cloud on AWS to address industry standards and frameworks including ISO 27001 and SOC2. APRA also provides risk categorizations (low, heightened, and extreme inherent) that serve as guidance to identify the workloads to be migrated to clouds. These have been explored in the section below.</p>
<p>Assessment of materiality</p> <p>APRA has classified risks into three broad categories: low inherent risk, heightened inherent risk and extreme inherent risk. APRA's supervisory approach depends on the scale of associated risk.</p>	<p>APRA's classification of low, heightened, and extreme inherent risks depends on the nature of data and applications being hosted and the level of disruption it may cause due to non-availability of data and applications. VMware Cloud on AWS has been developed to support organizations that host mission critical workloads.</p> <p>APRA defines extreme inherent risk arrangements as those that can cause extreme financial and operational impact, such as public cloud arrangements that host system of records and heightened inherent risk arrangements that involve critical and/or sensitive IT assets whose disruption might prevent organizations from meeting their APRA obligations. Examples of these include exposure to environments that are available to non-financial industry entities, unproven track record of a service provider, difficulty in transitioning to an alternate provider and arrangements that may inhibit APRA's oversight.</p> <p>VMware introduces bi-directional workload mobility between any vSphere and cloud. This enables cloud onboarding without retrofitting source infrastructure, supports migration to VMware Cloud on AWS without introducing complex migration challenges and provides ease of moving workloads back to the on-premises environment if needed.</p> <p>In addition to the above, VMware Cloud on AWS has redundancy and blast isolation are built into the cloud service platform architecture to ensure high availability of the VMware</p>

	<p>Cloud on AWS service, including regional independence and separation of console availability and SDDC services availability.</p> <p>VMware Cloud on AWS leverages vSphere Distributed Resource Scheduler (DRS) and vSphere High Availability to automatically restart a workload from any failure in a host to another healthy host in the cluster. VMware Cloud on AWS Elastic DRS enables automatic scaling of the Software Defined Data Center by adding and removing hosts based on policies designed to meet specific goals. VMware Site Recovery is another option that can be utilized to provide an end-to-end disaster recovery solution that can help reduce the requirements for a secondary recovery site, accelerate time-to-protection, and simplify disaster recovery operations. These solutions support the organizations in managing extreme inherent risks and delivering services with minimal disruption.</p> <p>VMware Cloud on AWS also addresses APRA's heightened inherent risk concerns such as exposure to non-financial industry environment, track record of cloud service provider, difficulty in transitioning and jurisdictional and contractual considerations. VMware has a strong track record supporting financial industry entities across various geographies. While VMware also offers solution to non-financial industry entities, our security and reliability features have been built to address leading financial services industry standards security and compliance standards such as ISO 27001/17/18 and SOC 2. You can view our public roadmap at https://cloud.vmware.com/vmc-aws/roadmap which shows how we are building new features and security requirements to address cloud security challenges.</p> <p>In the case of transition capabilities VMware Cloud on AWS lowers the risk related to cloud migrations and transitions as customers do not have to re-factor applications prior to migrating workloads nor engage in large scale transformations, meaning customers always have the choice to move workloads back on-premises or to another vSphere-based cloud environment. It can also be done in hours or weeks, instead of months or years. VMware Cloud on AWS leverages AWS's infrastructure to enable customers to run workloads in multiple availability zones within a region as well as in multiple geographic regions. Therefore, customers have the option to host their workloads in local regions to fulfil compliance obligations.</p>
--	--

CHAPTER 2 - RISK MANAGEMENT CONSIDERATIONS

APRA REQUIREMENT	VMWARE CLOUD ON AWS RESPONSE
<p>Strategy</p> <p>APRA requires its regulated entities to maintain appropriate strategy for adoption of cloud services.</p>	<p>APRA requires its regulated entities to develop a clear organizational strategy for cloud computing that includes technical, organizational, financial, and architectural considerations for transitioning from current state to the desired state and operating model. Unlike migrating to traditional public cloud, migrating to VMware Cloud on AWS may not require significant changes to your existing technical strategy, architecture, or operating model, customers can run workloads in a hybrid environment as they do on-premises. Another important factor that APRA emphasizes is organizational changes to deliver a successful cloud strategy. One of the key advantages of VMware Cloud on AWS is that may require minimal changes to skillset and organizational structure. Customers are able to leverage their existing knowledge and investments made for on-premises vSphere-based workloads and extend it to gain cloud computing advantages without re-training staff or implementing major architectural changes.</p>

	<p>Cost is a significant factor when developing cloud strategy. VMware has developed a variety of ways to allow customers to evaluate the total cost of ownership for VMware Cloud on AWS vs on-premises infrastructure. One such tool is a Total Cost of Ownership (TCO) tool. The TCO tool enables you to size for factors including storage, compute and memory in the logic to provide you with the most optimized server and SDDC recommendation for VMware Cloud on AWS. Once you have completed sizing your workloads, you can calculate your total cost of ownership (TCO) for these workloads and compare it with an on-premises virtual environment. Please see https://vmc.vmware.com/sizer/workload-profiles. Finally, some of the key features that you should consider when evaluating your cloud strategy against VMware Cloud on AWS are on-demand capacity and flexible consumption models and self-service to improve developer productivity. In addition, APIs enable infrastructure as code automation, access to a full range of Amazon cloud services available via high-speed, low latency connectivity to VMware Cloud on AWS for application modernization.</p>
<p>Governance</p> <p>Governance framework for outsourcing arrangements should be adequately defined and implemented.</p>	<p>APRA requires APRA regulated entities to develop an appropriate outsourcing governance framework with decision making authority and oversight responsibilities with respect to outsourcing clearly defined. APRA also recommends that an organization's board/governance authority be informed of all material initiatives involving cloud computing arrangements and to form a view as to the adequacy of the risk and control frameworks to manage the arrangement in line with the risk appetite of the board.</p> <p>VMware supports our customers' governance authority in maintaining oversight over the service by providing wide range of documentation, whitepapers, audit reports, and compliance certifications. VMware implements a shared responsibility model which outlines the roles and responsibilities of customers and VMware and AWS in managing the service end to end. Detailed information on the Shared Responsibility Model has been described in the 'Implementation of Controls' section below. Our service responsibilities are built on our Terms of Service, Service Level Agreement and Service Description. These are designed to help customers develop an internal governance and monitoring framework. You can view these documents at:</p> <ul style="list-style-type: none"> • Service Description: https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/support/vmw-cloud-aws-service-description.pdf • Terms of Service https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/downloads/eula/vmware-cloud-services-universal-tos.pdf • Service Level Agreement https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/support/vmw-cloud-aws-service-level-agreement.pdf <p>We understand that no governance process is complete without adequate due diligence. VMware supports our customers in due diligence exercises where you can request responses to specific service questions in line with your risk and control requirements. VMware is committed to delivering a cloud service that adopts industry good practices to meet a comprehensive set of international and industry-specific security and compliance standards. VMware and AWS adheres to rigorous security standards and are expanding coverage for various industry-specific security and compliance measures. For more information see our security whitepaper at VMware Cloud on AWS Security Whitepaper.</p>

Solution selection process

Selecting the solution involving cloud computing in a systematic and considered manner including comprehensive due diligence.

APRA recommends that APRA – regulated entities select a cloud solution that minimizes risk wherever possible and addresses entity's requirements, including security, risk management, IT architecture, procurement and supplier management.

VMware's ubiquity in the on-premises IT infrastructure market positions the VMware Cloud on AWS as a leading hybrid cloud solution for customers. VMware Cloud on AWS serves as an integrated cloud service offering that is differentiated from other cloud offerings due to ease of use and reduced risk for migrating applications to a hybrid cloud environment utilizing VMware technology and AWS services. The hybrid cloud model provided by VMware Cloud on AWS provides many advantages to seamlessly migrate workloads and scale back. VMware can work with APRA-regulated entities throughout the solution selection process by providing technical guidance wherever necessary, product demonstrations, identifying the best use cases to suit your requirements, identifying partner solutions to enhance your capabilities and providing product and technical documentation to assist in your solution selection process.

APRA recommends that APRA-regulated entities use Australian hosted options if available and consider cloud computing services used by parties that have comparable security and risk requirements (such as other financial sector entities). VMware Cloud on AWS is available in the Sydney region (AWS Sydney data center). Customers requiring hosting their workloads within Australia can consider hosting in the Sydney region to meet APRA requirements.



How does VMC on AWS add value?



Better

- Choose where to run applications based on business needs
- Seamlessly move live and large-scale workloads between vSphere-based private clouds and AWS with no changes to network addresses
- Extend established on-prem enterprise security, governance, and operational policies to the cloud
- Access native AWS services
- Scale IT infrastructure to support seasonal business demand



Faster

- Spin up an entire VMware SDDC in AWS cloud in under 2 hours*
- Scale capacity in minutes to respond to surges in demand
- Accelerate cloud migrations from months and years to weeks and days
- Simplify and accelerate time to protection
- Deliver a seamless path to new modernized applications
- Innovate rapidly by taking advantage of services in the cloud
- Accelerate Global Expansion with the click of a mouse or an API call



Cheaper

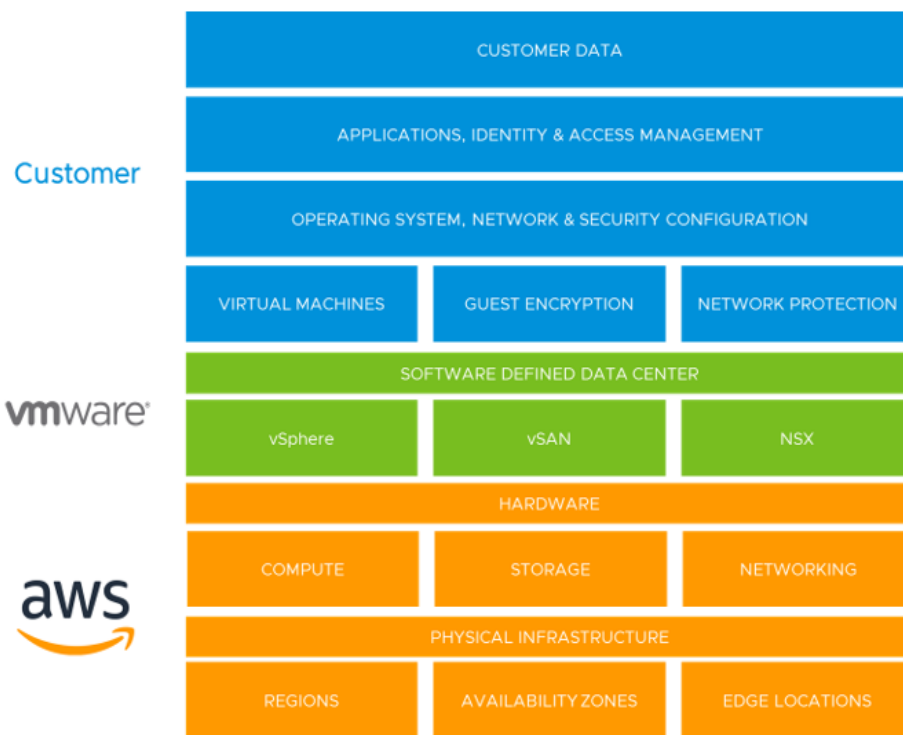
- Lower total cost of ownership with a true hybrid cloud solution when compared to a native public cloud?
- Reduce costs, while simplifying and accelerating workload migrations
- Minimize complexity and risk of migration
- Eliminate maintaining extra capacity on-premises for temporary spikes in workloads
- Extend the value of existing on-premises investments

APRA also recommends considering the design and architectural requirements to minimize the risk of loss of confidentiality, integrity, and availability of the solution. VMware Cloud on AWS allows customers to deploy a starter configuration containing a single host. This allows customers to kickstart the hybrid cloud experience and adopt the service with minimal risk and while evaluating the design and architectural dependencies. The Single Host SDDC starter configuration is appropriate for test and development or proof of concept use cases. Customers can accelerate the deployment of disaster recovery capabilities with VMware Site Recovery, the cloud-based DR service optimized for VMware Cloud on AWS. VMware Cloud on AWS also provides customers with Hybrid Linked Mode which provides a single logical view of on-premises and VMware Cloud on AWS resources.

Finally, APRA also recommends that APRA-regulated entities consider solutions that allow for cloud computing service to be transitioned to an alternative service provider or brought

	<p>in-house if needed. The VMware HCX platform supports APRA-regulated entities with this requirement by providing a hybrid interconnect to enable scalable application migration and mobility within and across data centers and clouds and actively move and rebalance workloads as needed for scale, compliance, security, and cost management.</p>
<p>APRA access and ability to act</p> <p>APRA-regulated entities to include an APRA-access clause in the outsourcing agreement.</p>	<p>APRA requires APRA-regulated entities to undertake contractual undertaking from cloud service providers for APRA's access to relevant information and onsite visits.</p> <p>The VMware Cloud on AWS contractual documentation includes an audit rights provision which can support APRA-regulated entities in meeting this requirement. VMware allows APRA-regulated entities and APRA to examine the relevant documentation and systems to audit the applicable cloud service offering. For further details around specific provisions, please see your contract or reach out to your VMware Account Manager</p>
<p>Transition approach</p> <p>A cautious and measured approach is adopted for transitioning to a cloud computing service.</p>	<p>Migrating workloads to the cloud can be complex and time-consuming. Organizations need to address varying Virtual Machine formats, disparate hardware, network connectivity, and application dependencies. APRA requires organizations to take a cautious and measured approach for transitioning to a cloud computing service, particularly where risks are heightened</p> <p>VMware simplifies customers' migration to VMware Cloud on AWS by providing a consistent infrastructure delivered by the same vSphere-based workload that you use on-premises. VMware also has multiple tools to ease the transition process for customers. VMware HCX and vMotion help provide support for key cloud migration and data center extension use cases. For cloud migration, it serves as the network connection for large scale migration of live applications. For data center extension, it serves as the persistent on-premises to public cloud network interconnect. The service offers bi-directional application mobility between vSphere and VMware Cloud on AWS Software Defined Data Centers (SDDCs). HCX includes capabilities to support VMware vSphere vMotion, bulk migration, high throughput network extension, WAN optimization, traffic engineering, automated VPN with Strong Encryption.</p> <p>VMware also supports customers by providing various tools such as Hands on lab and technical documentation to learn about the service prior to migration and assist in step by step migration process. Below are some of the key considerations that customers can include in their transition approach:</p> <ul style="list-style-type: none"> • Map your application dependences: Before an environment can be effectively sized, application dependencies must be understood to determine the scope of the migration. This process can be significantly simplified by utilizing automated tools such as VMware Network Insight to identify network communication patterns between applications. This can also be utilized to gain insight into data volume between systems and estimate data egress charges, if the dependent system remains on-premises. • Design requirements: Build a cross-functional migration team consisting of Infrastructure administrators and architects, network and security, support and operations, application owners and other stakeholders. • Sizing the environment: After completing the application dependency mapping and initial design, create an inventory of the workloads that are planned to be migrated to VMware Cloud on AWS. Utilize the VMware Cloud on AWS sizer tool

	<p>to build a configuration for the environments to be migrated. This also includes a TCO analysis to build the business case for migration.</p> <ul style="list-style-type: none"> • Pilot the migrations: After dependencies are discovered and mapped, consider separating workloads and applications into one of three categories according to downtime tolerance: prolonged downtime, minimal downtime, or zero downtime. Once these workloads are separated and categorized, we recommend ranking them into groups of migration waves starting with the greatest amount of downtime allowance for the business. • Sequence your migrations: Staging the majority of the migrations within the next waves will rely on the application dependencies, downtime allowance, and change windows. Ensure that the waves are as small as possible by leveraging the appropriate available technologies: Live Migration, Bulk Migration, HCX vMotion with vSphere Replication, etc.
<p>Risk assessments and security</p> <p>Conduct meaningful risk assessments of material service provisions prior to selection, during the service and when a material change occurs.</p>	<p>APRA recommends that APRA-regulated entities conduct periodic risk assessments at a level of granularity that include meaningful understanding of the actual risks and mitigating controls associated with each risk. In doing so, APRA recommends considering the sensitivity and criticality of IT assets involved, the shared responsibility between the cloud service provider and the APRA-regulated entity and developing the control environment proportionate with the risks involved.</p> <p>VMware supports APRA's view of conducting periodic risk assessments to identify key risks and mitigating controls and the communication of key risks to senior management. A risk assessment plan for cloud computing services should not only consider the data and security risks but also the impact on organizational changes, roles, responsibilities, and business processes. Once the risks are identified, appropriate policies, procedures and controls should be put in place to address the risks and where possible monitor the risks on an ongoing basis. The risk assessment framework should also consider the changing legal, statutory, and regulatory requirements as well as the contractual obligations related to service delivery. VMware can support customers in their risk assessment process by providing necessary documentation and support from our technical and compliance experts. VMware has also published a number of whitepapers and technical resources on our portal which provide comprehensive information about the service. Please visit https://cloud.vmware.com/vmc-aws/resources#all-categories.</p>
<p>Implementation of controls</p> <p>Shared responsibility model for implementation of controls between the provider and the customer.</p>	<p>VMware Cloud on AWS implements a shared responsibility model that defines distinct roles and responsibilities of the three parties involved in the offering: Customer, VMware, and Amazon Web Services.</p>



Customer responsibility “Security in the Cloud” – Customers are responsible for the deployment and ongoing configuration of their SDDC, virtual machines, and data that reside therein. In addition to determining the network firewall and VPN configuration, customers are responsible for managing virtual machines (including in guest security and encryption) and using VMware Cloud on AWS User Roles and Permissions along with vCenter Roles and Permissions to apply the appropriate controls for users.

VMware responsibility “Security of the Cloud” – VMware is responsible for protecting the software and systems that make up the VMware Cloud on AWS service. This software infrastructure is composed of the compute, storage, and networking software comprising the SDDC, along with the service consoles used to provision VMware Cloud on AWS.

AWS responsibility “Security of the Infrastructure” – AWS is responsible for the physical facilities, physical security, infrastructure, and hardware underlying the entire service.

For more information on the shared responsibility model, please see our whitepaper at: [VMware Cloud on AWS - Shared Responsibility Model whitepaper](#)

VMware also provides periodic audited reports/certifications including SOC 2 and ISO 27001 that demonstrate the controls over our environment. AWS compliance reports can be accessed via the AWS portal <https://aws.amazon.com/artifact/>. Customers are expected to implement controls over their environment including virtual machines, applications, content, networking, and guest encryption.

<p>Ongoing oversight</p> <p>Monitoring material service providers proactively and on a regular basis.</p>	<p>APRA requires regular monitoring of service providers to ensure services are delivered in line with service level agreement and that associated risks are effectively managed. VMware supports its customers by providing automated tools and dashboards for ongoing monitoring of the service as well as optional solutions including the vRealize Management suite. Some of the key dashboards available in vRealize Operations include:</p> <ul style="list-style-type: none"> • Capacity dashboard: To view the capacity overview of each VMware Cloud on AWS SDDC. Customers can view the capacity of Clusters, Hosts, VMs, Datastores, and Disk groups. • Cost Overview dashboard: To view the organization cost overview and expense trends. The monthly metrics plotted in the trends represent the previous month's bill. The bill start date and end date are available in the properties. • Inventory dashboard: To view the inventory overview of all the SDDCs configured in VMware Cloud on AWS. • Management VM Monitoring dashboard: To monitor the utilization and performance of the key management VMs running in your SDDC. This dashboard ensures that the management components (such as vCenter and NSX) are not facing any resource bottlenecks from the CPU, memory, network, and storage perspectives. • Utilization and Performance dashboard: To view the utilization and performance overview of each SDDC based on heavy hitter VMs and impacted VMs over the last 30 days. This dashboard helps you find the VMs in your environment that are negatively impacting the capacity or performance from a CPU, memory, storage, or network perspective. <p>Customers can also configure various SaaS monitoring tools such as VMware Wavefront (a cloud-native analytics and monitoring platform), vRealize Network Insight (provides security and network visibility across hybrid and multi-cloud environments) and a range of SaaS tools from our Partners (https://cloud.vmware.com/cloud-marketplace/partners#vmware-cloud-marketplace-published-solutions).</p> <p>Customers can also monitor the real-time status of VMware Cloud on AWS services along with past incidents. This is publicly available on https://status.vmware-services.io/. Activity logs for access to VMware Cloud on AWS environments by VMware is captured in the vSphere logs. Customers will see all actions taken by a VMware Admin captured in the logs and fully visible in vRealize Log Intelligence Cloud (VMware Cloud on AWS log aggregation portal).</p> <p>VMware Cloud on AWS also regularly performs updates on your SDDCs. These updates ensure continuous delivery of new features and bug fixes and maintain consistent software versions across the SDDC fleet.</p>
<p>Business disruption</p> <p>Continue to meet its obligations regardless of disruptions resulting from a failure of technology, people, process or service providers.</p>	<p>APRA acknowledges that APRA-regulated entities have gained benefits from high availability features in cloud computing services. However, APRA recommends the regulated entities to not just focus on maintaining high availability but also maintain high recovery capabilities and contingency plans to ensure continued delivery of service in the event of failure.</p> <p>VMware Cloud on AWS is designed to be highly available, as well as to provide multiple disaster recovery mechanisms to recover from multiple concurrent failures. VMware Cloud on AWS leverages AWS' infrastructure and SDDCs can be deployed as Stretched Clusters</p>

	<p>to enable customers to run workloads in multiple availability zones within a region. Each availability zone is designed as an independent failure zone. In case of failure, SDDC Stretched Clusters automatically move customer workloads away from the affected area. VMware Cloud on AWS leverages vSphere Distributed Resource Scheduler (DRS) and vSphere High Availability (HA) to automatically restart a workload from any failure in a specific host on another host in the cluster. In addition, VMware Site Recovery can provide an end-to-end disaster recovery solution that can help reduce the requirements for a secondary recovery site, accelerate time-to-protection, and simplify disaster recovery operations. In the event of a host failure, a new host can be provisioned to a cluster within minutes in order to restore full capacity. The VMware Site Recovery offering provides native hypervisor-based replication using VMware vSphere Replication of workloads between vSphere instances in different regions or customer datacenters.</p> <p>While the above features provide robust availability and recovery capabilities, APRA regulated entities can also host their workloads across AWS availability zones with stretched clusters for VMware Cloud on AWS. The APRA regulated entities retain control and ownership of their customer content and have the ability utilize their own backup and recovery mechanisms including establishing a redundant cloud infrastructure in their own data centers and/or using any one of thousands of VMware partners that run vSphere.</p>
<p>Audit and assurance Provide assurance to the board over management of material service provisions, including assurance over the design and operating effectiveness of controls.</p>	<p>APRA recommends that regulated entities implement adequate internal and external assurance plans over the cloud service and provide assurance to the board over management of material service provisions. VMware provides audited compliance reports as well as self-service tools to enable customers to gather data to build service assurance programs. As indicated in the 'Controls Implementation' section above, VMware Cloud on AWS maintains a shared responsibility model for implementation of controls and providing assurance over the design and operating effectiveness of the controls.</p> <p>As a cloud service provider, VMware provides assurance over the software and systems that make up VMware Cloud on AWS. This software infrastructure is composed of the compute, storage, and networking software comprising the SDDC, along with the service consoles used to provision VMware Cloud on AWS. Our compliance programs are aligned with internationally recognized standards as evidence of our commitment to information security at every level of the organization and ensure that the security program is in accordance with industry leading best practices. Platform and application security standards are consistent with industry-accepted guidance and standards, such as, but not limited to ISO and CIS.</p> <p>VMware Cloud on AWS has established an Information Security Management System (ISMS) based on ISO 27001 standards, as well as ongoing compliance programs (SOC 2 and others) to manage risks relating to confidentiality, integrity, and availability of information. You can see our existing compliance offerings at https://cloud.vmware.com/trust-center. Amazon Web Services is responsible for data center security. For more information on AWS controls, please visit: https://cloudsecurityalliance.org/star/registry/amazon/ https://aws.amazon.com/compliance/data-center/data-centers/</p>

	<p>VMware provides customers with the features to develop controls over their SDDC environment. Customer manage access on their console, including administrator access. VMware has also deployed mechanisms to capture administrator activity. VMware continuously collects and monitors services operation logs using SIEM technologies. The 24x7x365 VMware Security Operations Center uses the SIEM to correlate information with public and private threat feeds to identify suspicious and unusual activities. Customers can utilize detailed SDDC log feeds provided by vRealize LogIntelligence to gather evidence/data for their assurance programs. These features in conjunction with the audited reports provided by VMware can be used to provide assurance to the board over the service arrangements.</p>
--	--

CHAPTER 3 - APRA NOTIFICATION AND CONSULTATION

APRA REQUIREMENT	VMWARE CLOUD ON AWS RESPONSE
<p>APRA Notification and Consultation Notify APRA of any material outsourcing arrangements.</p>	<p>APRA defines material business activity as the one which if disrupted can potentially have significant impact on business operations. APRA requires APRA-regulated entities to notify of any material outsourcing arrangements.</p> <p>While APRA has not provided a definitive guide for materiality assessment, it is up to APRA-regulated entities to determine whether the service constitutes a material business activity. Some of the points that customers should consider during materiality assessment include:</p> <ul style="list-style-type: none"> • Is the service critical to business continuity and the impact on business and IT processes. • Can the service outage cause significant operational/reputational/legal damage • The potential impact of a confidentiality breach or data integrity <p>As indicated in the above section 'assessment of materiality', customers should identify the risk category (low/heightened/extreme inherent risk) for the workloads to be migrated to VMware Cloud on AWS. Customers can also consider scenario analysis to determine the potential business impact if service is disrupted. Where the service is assessed to be material, customers should notify APRA of the outsourcing arrangement.</p> <p>APRA encourages consultation prior to entering into any agreement involving a material business activity. Where the APRA regulated entity's risk assessment results in heightened risk, APRA encourages consultation post the internal governance process and in case of extreme inherent risk early consultation is required. For low inherent risk, if there is no offshoring involved, there is no requirement to consult APRA.</p> <p>VMware can assist you during your materiality assessment and consultation process. We can provide you with audited reports, compliance certifications, assist in your risk assessments and provide technical and product documentation. We also have dedicated team of Technical Account Managers, Architects, Product Managers, and Customer Success Managers to address any queries or concerns about the service provisions or contractual requirements and to share good practices and knowledge to tailor the service to your needs.</p>

	Our service offerings are aligned to your use-cases: disaster recovery, data center extension, cloud migration, and next generation apps. Our technical and industry experts can also support you in identifying suitable migration methodologies, readiness assessment and also assist in the first wave of the migration (Migration Standard), or fully migrate end-to-end (Migration Advanced or Migration Enterprise).
--	--

Conclusion

APRA has observed an increasing use of cloud computing services by APRA-regulated entities as well as growth in heightened inherent risk and extreme inherent risk initiatives. While the 2018 information paper on cloud adopts a more acceptable view towards cloud computing initiatives in comparison to the 2015 paper, it does recommend thoroughly considering the risks, categorize the risks (low, heightened, and extreme) and implement effective governance and necessary measures and controls to manage the risks.

VMware Cloud on AWS supports APRA regulated entities in their cloud journey from planning through to assessment, migration, and managing day-to-day cloud operations. Our solutions help address the key cloud security concerns raised by APRA through industry leading security and resiliency capabilities, leveraging AWS's bare metal infrastructure, bi-directional migration capability, and ease of deployment while balancing scalability. Our solutions allow customers to build, run, and manage modern apps, meeting diverse needs with on-premises and public cloud resources while enabling faster service delivery at lower cost and risk.

VMware is committed to addressing any specific concerns that you may have and can support you in deploying the service in the best possible way to address your architectural and organizational requirements as well as the guidelines mentioned in the APRA's 2018 Information Paper on Cloud Outsourcing. We have published a wealth of resources to help you gain further understanding of the service and the discover of our wide range of security, resiliency, and compliance capabilities.

- VMware Cloud on AWS Getting Started Guide
<https://docs.vmware.com/en/VMware-Cloud-on-AWS/services/vmc-on-aws-getting-started.pdf>
- VMware Cloud on AWS Service Description
<https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/support/vmw-cloud-aws-service-description.pdf>
- VMware Cloud Services Security Overview
<https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/products/cloud-services/vmware-cloud-services-on-aws-security-overview-white-paper.pdf>
- Amazon Web Services: Overview of Security Processes
<https://d1.awsstatic.com/whitepapers/aws-security-whitepaper.pdf>



VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 vmware.com.
Copyright © 2020 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at vmware.com/go/patents. VMware is a registered trademark or trademark of VMware, Inc. and its subsidiaries in the United States and other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies. Item No: Response to APRA Information Paper – Outsourcing Involving Cloud Computing Services