Australia and New Zealand Public Sector Agency FastStart Guide

Challenges and Opportunities

February 2020

Notices

This document is provided for informational purposes only. It represents AWS's current product offerings and practices as of the date of issue of this document, which are subject to change without notice. Customers are responsible for making their own independent assessment of the information in this document and any use of AWS's products or services, each of which is provided "as is" without warranty of any kind, whether express or implied. This document does not create any warranties, representations, contractual commitments, conditions or assurances from AWS, its affiliates, suppliers or licensors. The responsibilities and liabilities of AWS to its customers are controlled by AWS agreements, and this document is not part of, nor does it modify, any agreement between AWS and its customers.

Contents

Introduction

This AWS Agency FastStart guide is designed to help public sector organisations in Australia and New Zealand to get started quickly and easily with AWS.

Customers tell us that there is a lot of information available about the AWS platform, but it can be difficult to know where to start. This guide provides answers to frequently asked questions and guidance for where to get more information.

Some questions will be more relevant to technical staff, while other questions will be more relevant to those in management, executive, finance or procurement functions.

Business Challenges

How do I set budgets and allocate billing for AWS resources by team, department, or project?

AWS Cost Management provides a broad overview of how to manage costs in AWS. To avoid unexpected charges, AWS Budgets allows you to create custom budgets and set-up alerts when your costs or usage exceed (or are forecast to exceed) your budgets.

The AWS Cost Management Blog provides a walk-through in setting a custom total monthly cost budget using the monthly budget feature in AWS Budgets.

If you have multiple AWS accounts, you can use the consolidated billing feature in AWS Organizations to allocate billing by account. Alternatively, you can use cost allocation tags to track your costs on a detailed level.

How do I establish a Total Cost of Ownership for our AWS workloads?

It is important to weigh the financial considerations of owning and operating a data centre (or colocation facility) versus using cloud infrastructure. Get started at the AWS Economics page.

Our TCO Calculator allows you to estimate the cost savings when using AWS and provides a detailed set of reports that can be used in executive presentations.

The AWS Pricing Calculator allows you to estimate the cost of your architecture solution and fits your unique agency needs with AWS products and services. Our Simple Monthly Calculator provides an estimate of usage charges for AWS services based on your requirements.

How do I procure, consume and pay for cloud services?

Australian public sector organisations – federal/state/territory agencies, public universities, and other government-owned agencies – may be eligible or required to join the Digital Transformation Agency's (DTA) Whole of Federal Government Arrangement (WofG Arrangement). For more information, refer to DTA's WofG Arrangement guidance. To join the WofG Arrangement, please email DTA directly.

How to Buy covers important considerations when buying cloud. This includes how to justify your move to AWS, operational and cultural implications, purchasing strategies, architectural considerations, and further improvements to enable innovation and save future costs.

How do I help my organisation understand the benefits of cloud?

To help you communicate the benefits of cloud to your organisation, our six advantages of cloud computing provides an excellent summary. It can also be useful to demonstrate, through our case studies, how other public sector agencies have achieved business agility, cost savings, innovation, and high availability with the AWS Cloud.

AWS enterprise strategist Mark Schwartz explores the benefits of the cloud at an executive level in the AWS Enterprise Strategy Blog.

People Challenges

How do I help my people improve their cloud skills?

There are several options for helping you and your teams develop cloud skills:

- AWS Training and Certification will help you arrange online or in-person training for AWS certifications. This training is also available from AWS partners such as A Cloud Guru or Linux Academy.
- AWS Partner Network (APN) members are focused on your success, helping customers take full advantage of all the business benefits that AWS offers.
- If you or your team would like AWS certification, there are various learning paths available. These include role-based paths for architects or developers, and topic paths such as, machine learning, advanced networking, and security.

How do I develop a training plan for my organisation?

The People pillar of the Cloud Adoption Framework will help you develop a people strategy/plan to increase cloud skills in your organisation.

Your strategy could include the training options outlined in the previous section. You could also engage AWS's training experts to help you build a custom training plan. Talk to your AWS account team to arrange a meeting.

National Australia Bank (NAB) created a cloud guild to transform how they upskill staff. This video presentation provides an overview of NAB's strategic training engagement with AWS and how it transformed the bank's learning culture.

The AWS Enterprise Strategy Blog contains several entries that could help you develop a training strategy:

- You Already Have the People You Need to Succeed with the Cloud
- Getting Started with Training for the Cloud
- Cloud Culture and Training

Governance Challenges

How do I develop a delivery pipeline with clearly defined approval gates and release mechanisms?

Achieving greater agility is one of the main business drivers for any move to the cloud. However, you can maintain governance and control over changes. Our Change Management whitepaper outlines how to automate processes and govern changes.

DevOps is also an important part of change management in the cloud. To meet the demands of an agile business, teams need to deploy applications in a consistent, repeatable, and reliable manner. Our DevOps whitepaper provides detailed change management information.

How do I reach compliance targets and monitor the compliance of my systems in AWS?

AWS Artifact is your go-to, central resource for compliance-related information that matters to you. It provides on-demand access to AWS's security and compliance reports and select online agreements. Reports include our Service Organization Control (SOC) reports, Payment Card Industry (PCI) reports, and certifications from accreditation bodies across geographies and compliance verticals that validate the implementation and operating effectiveness of AWS security controls.

These include documents related to AWS's certification for programs including:

- AWS's PROTECTED certification by the Australian Cyber Security Centre (ACSC) and Information Security Registered Assessors Program (IRAP) suite of documents, relevant to Australian public sector agencies.
- The AWS FedRAMP Partner Package is intended for use by partners and customers when building applications and solutions on AWS that need to pursue a FedRAMP assessment and accreditation.
- AWS's PCI DSS Attestation of Compliance (AOC) and Responsibility Summary, of relevance to AWS customers with a card data environment (CDE) that stores, transmits, or processes cardholder data in the AWS Cloud.

The AWS Compliance FAQ provides information about how to complete compliance questionnaires, how to comply with regulatory requirements, and commonly-asked questions about compliance frameworks.

There is also a wealth of information available about specific certification programs. This could include information relevant to Australian government agencies (AWS and the ASD Essential Eight), the healthcare industry (AWS HIPAA Compliance), or agencies required to comply with the European Union's General Data Protection Regulation (GDPR).

AWS Config tracks AWS resource configurations. It can be used to verify that existing and newly launched AWS resources conform to your organisation's security guidelines and best practices, without creating a bureaucracy or manually inspecting cloud resources.

There are also AWS Solutions available that can help you with the governance of your cloud resources. The Real Time Insights solution provides valuable insight into who is accessing your resources and how your resources are being used.

How do I develop a mechanism for governing solution design and architectures?

The Well Architected Framework can help your cloud architects build secure, high-performing, resilient, and efficient infrastructure for their applications. Based on five pillars — operational excellence, security, reliability, performance efficiency, and cost optimisation — the Framework provides a consistent approach for customers and partners to evaluate architectures, and implement designs that will scale over time.

AWS Service Catalog can be used to create and manage catalogues of IT services that are approved for use on AWS. These IT services can include everything from virtual machine images, servers, software, and databases to complete multi-tier application architectures.

Infrastructure as Code has emerged as a best practice for automating the provisioning of infrastructure services. For more information, please refer to our Infrastructure as Code whitepaper.

How do I understand which of our workloads can be moved to cloud, and how much effort will be required?

The path to cloud adoption is unique for every public sector organisation. The stages of adoption described in the Cloud Migration guide can be a useful way to understand some of the steps involved. To help you develop an efficient and effective plan for cloud adoption and migration, please refer to the survey in our Cloud Adoption Readiness Tool. When formulating a migration strategy, please refer to our 6 Application Migration Strategies: "The 6 R's" page.

To design and manage an accelerated path to successful cloud adoption, the AWS Cloud Adoption Framework can help you build a comprehensive approach across your organisation, and throughout your IT lifecycle. The framework organises guidance into six areas of focus, called perspectives. Each perspective covers distinct responsibilities owned or managed by functionally related stakeholders. Business capabilities are covered by the Business, People, and Governance Perspectives ; while technical capabilities are covered by the Platform, Security, and Operations Perspectives.

To assist with your migration, a number of services are available:

- AWS Database Migration Service can help you discover the true costs of your current compute and storage environment, and assist you in building and validating your cloud business case.
- TSO Logic provides accurate, data-driven recommendations to right-size and right-cost compute.
- CloudEndure automates large-scale migrations from physical, virtual, and cloud-based infrastructure to AWS.

Platform Challenges

How can my organisation maintain velocity and agility while maintaining governance of AWS use?

As operational footprints scale on AWS, a common theme across public sector agencies is the need to maintain control over cloud resource usage, visibility, and policy enforcement at scale. Our Governance at Scale whitepaper provides more detailed information.

How can I implement guardrails in AWS to make it easy to do the right thing?

In addition to the suggestions outlined in the Governance at Scale whitepaper, a number of services are available:

- AWS Config enables you to assess, audit, and evaluate the configurations of your AWS resources. It continuously monitors and records your AWS resource configurations and allows you to automate the evaluation of recorded configurations against desired configurations.
- AWS Systems Manager provides visibility and control of your infrastructure on AWS. Systems Manager provides a unified user interface so you can view operational data from multiple AWS services and allows you to automate operational tasks across your AWS resources.
- AWS Service Catalog enables you to create and manage catalogues of IT services that are approved for use on AWS. These IT services can include everything from virtual machine images, servers, software, and databases to complete multi-tier application architectures.
- AWS Control Tower provides the easiest way to set up and govern a new, secure, multi-account AWS environment based on best practices.
- AWS Security Hub provides a comprehensive view of your high-priority security alerts and compliance status across AWS accounts.

How do I better understand architectural best practices in the cloud?

The Well Architected Framework has been developed to help cloud architects build secure, high-performing, resilient, and efficient infrastructure for their applications. Based on five pillars — operational excellence, security, reliability, performance efficiency, and cost optimisation — the Framework provides a consistent approach for customers and partners to evaluate architectures, and implement designs that will scale over time.

Additionally, there are many resources available on the AWS Architecture page, including reference architectures, quick start guides, whitepapers, and answers to common customer questions. AWS Solutions also provides solutions that are vetted

by AWS architects and designed to be operationally effective, reliable, secure, and cost effective.

How do I establish network connectivity between AWS and existing resources?

The AWS Virtual Private Cloud (VPC) Connectivity Options whitepaper provides an overview of the various options to facilitate network connectivity discussions as well as pointers to additional documentation and resources with more detailed information or examples. This response on AWS Answers covers the options available for connecting multiple VPCs within the same AWS Region.

You can use AWS Direct Connect to establish a private, logical connection from your remote network to your AWS environment. It is available at various locations around the world. In Australia, we currently have locations in Sydney, Canberra, Melbourne, and Perth, available in data centres from providers like NEXTDC and Equinix. For a step-by-step guide on provisioning an AWS Direct Connect connection, please refer to this Knowledge Centre article.

For more information on establishing network connectivity between AWS and your existing environment, please review this Extending Data Centres to Cloud - Connectivity Options & Best Practices NET302 *re:Invent 2018* presentation. To understand the fundamentals of AWS VPC, please review this re:Invent 2015 presentation.

How do I better understand foundational design patterns, like CIDR ranges, AMI usage, disaster recovery and backups, and logging?

The Getting Started Resource Centre will help you understand AWS fundamentals. From core concepts to beginner tutorials, it provides the information you need to start building on AWS.

For key considerations and recommendations on designing and sizing individual VPCs, refer to AWS Single VPC Design. To understand how to expand to multiple VPCs, refer to this response on AWS Answers. You may need to consider AWS Transit Gateway, a service that enables you to connect your VPCs and on-premises networks to a single gateway.

An Amazon Machine Image (AMI) provides the information required to launch an Amazon Elastic Compute Cloud (Amazon EC2) instance. You must specify an AMI when you launch an instance. There are a number of best practices for how to design and build AMIs. Please refer to this response on AWS answers for further details.

For a practical guide on how to programmatically create AMIs for your environment, please refer to the guide on the AWS DevOps Blog.

The logging and monitoring of API calls are key components in security and operational best practices, as well as requirements for industry and regulatory compliance. For an overview of common compliance requirements related to logging, and how to satisfy these requirements in your AWS environment, please refer to our Security at Scale: Logging in AWS whitepaper.

Many public sector agencies are extending their backup targets to the cloud. While the cloud offers better scalability than on-premises, building cloud-enabled backup solutions requires careful consideration of existing IT investments, recovery objectives, and available resources. The AWS Backup & Restore site will help you build scalable, durable, and secure data-protection solutions.

Security Challenges

How can I build secure and compliant architectures on AWS?

Start by referring to the Reference Architecture outlined in the IRAP PROTECTED Package, available on AWS Artifact. This architecture demonstrates how multiple AWS services can be brought together to support a typical multi-tier web application with associated security and management services that meet ISM PROTECTED control requirements.

AWS and the Australian Signals Directorate Essential Eight is a blog post that can help agencies understand how to implement the Essential Eight with AWS's services and support. The whitepaper Understanding the ACSC's Cloud Computing Security for Tenants in the Context of AWS may also be of interest.

How will our security operations team work? What kind of mechanisms can help us in incident response?

To understand how to apply best practices in the design, delivery, and maintenance of secure AWS environments, refer to the Security Pillar of the Well Architected Framework.

The AWS Security Incident Response Guide provides an overview of the fundamentals of responding to security incidents within your AWS environment.

To understand how automation can assist with security, the AWS DevOps Blog contains a practical guide on Implementing DevSecOps Using AWS CodePipeline. This 2019 AWS Sydney Summit presentation provides detail on how Australia Post built an effective automated remediation pipeline.

How does encryption and key management work on AWS?

AWS Key Management Service (KMS) allows you to create and manage keys and control the use of encryption across a wide range of AWS services and in your applications. There are also whitepapers available on KMS best practices, and KMS cryptographic details.

If you need to create and manage the hardware security modules (HSM) that store your encryption keys, AWS CloudHSM is a cloud-based HSM that enables you to easily generate and use your own encryption keys on the AWS Cloud. It is a fully-managed service that automates time-consuming administrative tasks, such as hardware provisioning, software patching, high-availability, and backups.

For more detail, please review the Encrypting Everything with AWS presentation by AWS Senior Principal Engineer Colm MacCárthaigh at *AWS re:Inforce 2019*.

How can we ensure security controls are met and enforced?

Security of Your AWS Accounts

AWS Security Hub provides a comprehensive view of your high-priority security alerts and compliance status across AWS accounts. It provides a single place that aggregates, organises, and prioritises your security alerts, or findings, from multiple AWS services, such as Amazon GuardDuty, Amazon Inspector, and Amazon Macie, as well as from AWS Partner solutions.

AWS Config enables you to assess, audit, and evaluate the configurations of your AWS resources. Config continuously monitors and records your AWS resource configurations and allows you to automate the evaluation of recorded configurations against desired configurations.

Security automation is also a key principle. It helps reduce operational overhead and creates repeatable, predictable approaches to monitoring and responding to events. This entry on the AWS Security Blog provides a walk-through of a scenario using events from Amazon GuardDuty to automatically log suspicious hosts.

Security of Your Servers and Applications on AWS

The Amazon Inspector security assessment service can evaluate the operating environments and applications you have deployed on AWS for common and emerging security vulnerabilities automatically. For implementation information, refer to this entry on the AWS Security Blog.

How do I manage identity, authentication, and authorisation in our AWS environment?

AWS Identity and Access Management (IAM) enables you to manage access to AWS services and resources. You can create IAM policies to manage permissions for IAM users and groups that allow or deny access to AWS resources. To quickly get started with IAM and establish an initial set of controls that protect your infrastructure, empower users, and allow for growth and change in your organisation's use of AWS, refer to this guidance.

In addition to IAM, other AWS Identity, Directory, and Access services help you manage authentication, authorisation, and governance in the AWS Cloud:

- AWS Directory Service for Microsoft Active Directory enables your directory-aware workloads and AWS resources to use managed Active Directory in the AWS Cloud.
- AWS Single Sign-On (SSO) makes it easy to centrally manage SSO access to multiple AWS accounts and business applications. Users can sign in to a user portal with their corporate credentials and access their accounts and applications from one place.

- Amazon Cognito lets you easily add user sign-up and sign-in to your mobile and web apps. You also can authenticate users through social identity providers, such as Facebook and Amazon, or enterprise identity providers through SAML.

The Security Perspective of the AWS Cloud Adoption Framework will help you structure the selection and implementation of security controls that meet your organisation's needs.

How can I manage data sovereignty in AWS?

The Data Privacy FAQ answers data privacy questions, including who owns customer content, disclosure of customer content, and where customer data is stored.

Additionally, the whitepaper Using AWS in the Context of Common Privacy & Data Protection Considerations provides information to assist agencies that want to use AWS to store or process content containing personal data, in the context of common privacy and data protection considerations.

To enforce data sovereignty, you could implement Service Control Policies (SCP) using AWS Organizations. Please refer to these example SCPs to restrict region access.

For a deeper discussion about data residency, please refer to our Data Residency whitepaper.

Operational Challenges

How do I run and manage production systems in AWS?

In the AWS Well Architected Framework, the Operational Excellence Pillar whitepaper provides guidance to help you apply best practices in the design, delivery, and maintenance of AWS environments. The AWS Enterprise Strategy blog also provides guidance on running IT operations in the cloud.

How do I maintain a service catalogue in AWS?

AWS Service Catalog allows agencies to create and manage catalogues of IT services that are approved for use on AWS. These IT services can include everything from virtual machine images, servers, software, and databases to complete multi-tier application architectures. The Service Catalog can also be deployed with AWS Control Tower and with the AWS Landing Zone solution.

If you would like to offer your users access to fully-featured application architectures, these can be written in AWS CloudFormation. This service provides a common language to describe and provision all the infrastructure resources in your cloud environment. CloudFormation allows you to use a simple text file to model and provision, in an automated and secure manner, all the resources needed for your applications across all regions and accounts. This file serves as the single source of truth for your cloud environment.

The programmatic nature of AWS also allows for easy integration of third-party service catalogues. This can allow your users to request approved AWS products through your existing IT service management (ITSM) tools without logging into an AWS account. For example, the AWS Service Catalog Connector for ServiceNow, allows an organisation to synchronise AWS Service Catalog portfolios with its ServiceNow Service Catalog.

How do I manage monitoring and alerting in AWS?

For best practices and strategies to use when designing cloud architectures for reliability, refer to the Reliability Pillar of the AWS Well Architected Framework.

Amazon CloudWatch is a monitoring and observability service built for DevOps engineers, developers, site reliability engineers (SRE), and IT managers. CloudWatch provides you with data and actionable insights to monitor your applications, respond to system-wide performance changes, optimise resource utilisation, and get a unified view of operational health.

To alert on alarms raised by CloudWatch, you can use AWS Simple Notification Service (SNS) – a highly available, durable, secure, fully managed pub/sub

messaging service that can be used to fan out notifications to end users using mobile push, SMS, and email.

GE Transportation delivered a presentation at *re:Invent 2017* on Operation Monitoring and Alerting at Scale in GE Transportation (ENT340). They discussed how they addressed operational challenges monitoring applications and platforms for availability, performance, and compliance.

How can I develop our interim and target operating models?

To design and manage an accelerated path to successful cloud adoption, the AWS Cloud Adoption Framework can help you build a comprehensive approach across your organisation, and throughout your IT lifecycle. Using the AWS CAF helps you realise measurable business benefits from cloud adoption faster and with less risk.

If you are interested in the AWS CAF, Enterprise Workshops are available from AWS Professional Services and accredited APN partners. To learn more, talk to your AWS representative or contact us.

To learn about how the adoption of a Cloud Operating Model can accelerate your cloud transformation, please refer to Cloud Operating Models for Accelerated Cloud Transformation.

Document Links by Section

Business Challenges

- AWS Cost Management: https://aws.amazon.com/aws-cost-management/
- AWS Budgets: https://aws.amazon.com/aws-cost-management/aws-budgets/
- AWS Cost Management Blog: https://aws.amazon.com/blogs/aws-cost-management/launch-variable-budget-targets-for-cost-and-usage-budgets/
- Consolidated billing: https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/consolidated-billing.html
- Cost allocation tags: https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/cost-alloc-tags.html
- AWS Economics: https://aws.amazon.com/economics/
- TCO Calculator: https://aws.amazon.com/tco-calculator
- Pricing Calculator: https://calculator.aws/
- Simple Monthly Calculator: https://calculator.s3.amazonaws.com/index.html
- DTA WofG Arrangement guidance: https://www.dta.gov.au/help-and-advice/ict-procurement/tools-sourcing-digital-products-and-services/ict-panels-and-arrangements/buying-aws-products
- DTA Email: ictprocurement@dta.gov.au
- How to Buy: https://aws.amazon.com/how-to-buy/
- The six advantages of cloud computing: https://docs.aws.amazon.com/whitepapers/latest/aws-overview/six-advantages-of-cloud-computing.html
- Public Sector case studies: http://aws.amazon.com/solutions/case-studies/government-education/
- AWS Enterprise Strategy Blog: https://aws.amazon.com/blogs/enterprise-strategy/cfo-series-an-executive-view-of-lean-and-agile-it/

People Challenges

- AWS Training and Certification: https://www.aws.training/
- A Cloud Guru: https://aws.amazon.com/partners/find/partnerdetails/?n=A%20Cloud%20Guru&id=001E000001HPUEeIAP
- Linux Academy: https://aws.amazon.com/partners/find/partnerdetails/?n=Linux%20Academy%2C%20Inc.&id=001E000000fg8VOIAY
- AWS Partner Network: https://aws.amazon.com/partners/find-a-partner

- Learning Paths: https://aws.amazon.com/training/learning-paths/
- Cloud Adoption Framework: https://do.awsstatic.com/whitepapers/aws_cloud_adoption_framework.pdf
- AWS Cloud Adoption Framework: https://do.awsstatic.com/whitepapers/aws_cloud_adoption_framework.pdf
- NAB Training video: https://www.youtube.com/watch?v=nvPm-NM-WUg
- You Already Have the People You Need to Succeed with the Cloud: https://aws.amazon.com/blogs/enterprise-strategy/you-already-have-the-people-you-need-to-succeed-with-the-cloud/
- Getting Started with Training for the Cloud: https://aws.amazon.com/blogs/enterprise-strategy/getting-started-with-training-for-the-cloud/
- Cloud Culture and Training: https://aws.amazon.com/blogs/enterprise-strategy/category/enterprise-strategy/culture-and-training/

Governance Challenges

- Change Management Whitepaper: https://d1.awsstatic.com/whitepapers/change_management_in_the_cloud.pdf
- DevOps Whitepaper: https://d1.awsstatic.com/whitepapers/AWS_DevOps.pdf
- AWS Artifact: https://aws.amazon.com/artifact/
- AWS Compliance FAQ: https://aws.amazon.com/compliance/faq/
- AWS and the ASD Essential Eight: https://aws.amazon.com/blogs/publicsector/aws-and-the-australian-signals-directorate-essential-eight/
- AWS HIPAA Compliance: https://aws.amazon.com/compliance/hipaa-compliance/
- European Union's General Data Protection Regulation (GDPR): https://aws.amazon.com/compliance/gdpr-center/
- AWS Config: https://aws.amazon.com/blogs/aws/track-aws-with-config/
- AWS Config Blog: https://aws.amazon.com/blogs/aws/aws-config-rules-dynamic-compliance-checking-for-cloud-resources/
- Real Time Insights: https://aws.amazon.com/solutions/real-time-insights-account-activity/
- Well Architected Framework: https://aws.amazon.com/architecture/well-architected/
- AWS Service Catalog: https://aws.amazon.com/servicecatalog/
- Cloud Migration Guide: https://aws.amazon.com/cloud-migration/
- Cloud Adoption Readiness Tool: https://cloudreadiness.amazonaws.com/

- Application Migration Strategies: "The 6 R's": https://aws.amazon.com/blogs/enterprise-strategy/6-strategies-for-migrating-applications-to-the-cloud/
- AWS Cloud Adoption Framework: https://aws.amazon.com/professional-services/CAF/
- AWS Database Migration Service: https://aws.amazon.com/dms/
- TSO Logic: https://tsologic.com
- CloudEndure: https://www.cloudendure.com

Platform Challenges

- Governance at Scale Whitepaper: https://d1.awsstatic.com/whitepapers/Security/AWS_Governance_at_Scale.pdf
- AWS Systems Manager: https://aws.amazon.com/systems-manager/
- AWS Service Catalog: https://aws.amazon.com/servicecatalog/
- AWS Control Tower: https://aws.amazon.com/controltower/
- AWS Security Hub: https://aws.amazon.com/security-hub/
- Well Architected Framework: https://aws.amazon.com/architecture/well-architected/
- AWS Architecture: https://aws.amazon.com/architecture
- AWS Solutions: https://aws.amazon.com/solutions
- AWS Virtual Private Cloud Connectivity Options Whitepaper: https://docs.aws.amazon.com/whitepapers/latest/aws-vpc-connectivity-options/introduction.html
- AWS Answers response: https://aws.amazon.com/answers/networking/aws-single-region-multi-vpc-connectivity/
- Knowledge Centre article: https://aws.amazon.com/premiumsupport/knowledge-center/provision-direct-connection/
- *re:Invent 2018* presentation – Extending Data Centres to Cloud - Connectivity Options & Best Practices NET302: https://www.youtube.com/watch?v=LNYY3bMSiHM
- *re:Invent 2015* presentation – The fundamentals of AWS VPC: https://www.youtube.com/watch?v=5_bQ6Dgk6k8
- Getting Started Resource Centre: https://aws.amazon.com/getting-started/
- AWS Single VPC Design: https://aws.amazon.com/answers/networking/aws-single-vpc-design/
- AWS Transit Gateway: https://aws.amazon.com/transit-gateway/

- Amazon Machine Image: https://aws.amazon.com/answers/configuration-management/aws-ami-design/
- AMI guide on AWS DevOps Blog: https://aws.amazon.com/blogs/devops/how-to-create-an-ami-builder-with-aws-codebuild-and-hashicorp-packer/

Security Challenges

- Security Pillar of the Well Architected Framework: https://d1.awsstatic.com/whitepapers/architecture/AWS-Security-Pillar.pdf
- AWS Security Incident Response Guide: https://d1.awsstatic.com/whitepapers/aws_security_incident_response.pdf
- Implementing DevSecOps Using AWS CodePipeline: https://aws.amazon.com/blogs/devops/implementing-devsecops-using-aws-codepipeline/
- AWS Sydney Summit – Australia Post presentation: https://anz-resources.awscloud.com/aws-summit-sydney-2019-secure/automated-security-remediation-3
- AWS Key Management Service: https://aws.amazon.com/kms/
- AWS Key Management Service best practices: https://d1.awsstatic.com/whitepapers/aws-kms-best-practices.pdf
- KMS cryptographic details: https://d1.awsstatic.com/whitepapers/KMS-Cryptographic-Details.pdf
- AWS CloudHSM: https://aws.amazon.com/cloudhsm/
- Encrypting Everything with AWS presentation: https://www.youtube.com/watch?v=oqHLLbOoxDg
- AWS Security Hub: https://aws.amazon.com/security-hub/
- AWS Config: https://aws.amazon.com/config/
- AWS Security Blog: https://aws.amazon.com/blogs/security/how-to-use-amazon-guardduty-and-aws-web-application-firewall-to-automatically-block-suspicious-hosts/
- Amazon Inspector: https://aws.amazon.com/inspector/
- AWS Security Blog: https://aws.amazon.com/blogs/security/how-to-remediate-amazon-inspector-security-findings-automatically/
- AWS Identity and Access Management: https://aws.amazon.com/iam/
- AWS Identity and Access Management guidance: https://aws.amazon.com/answers/security/aws-iam-in-practice/
- AWS Identity, Directory, and Access services: https://aws.amazon.com/identity/
- AWS Directory Service for Microsoft Active Directory: https://aws.amazon.com/directoryservice/

- AWS Single Sign-On: https://aws.amazon.com/single-sign-on/
- Amazon Cognito: https://aws.amazon.com/cognito/
- The Security Perspective of the AWS Cloud Adoption Framework: https://do.awsstatic.com/whitepapers/aws_cloud_adoption_framework.pdf
- Data Privacy FAQ: https://aws.amazon.com/compliance/data-privacy-faq/
- Using AWS in the Context of Common Privacy & Data Protection Considerations Whitepaper: https://d1.awsstatic.com/whitepapers/compliance/Using_AWS_in_the_context_of_Common_Privacy_and_Data_Protection_Considerations.pdf
- AWS Organizations: https://aws.amazon.com/organizations/
- Data Residency Whitepaper: https://d1.awsstatic.com/whitepapers/compliance/Data_Residency_Whitepaper.pdf

Operational Challenges

- Operational Excellence Pillar Whitepaper: https://d1.awsstatic.com/whitepapers/architecture/AWS-Operational-Excellence-Pillar.pdf
- AWS Enterprise Strategy Blog: https://aws.amazon.com/blogs/enterprise-strategy/tag/it-operations/
- AWS Service Catalog : https://aws.amazon.com/servicecatalog/
- AWS Control Tower: https://aws.amazon.com/controltower/
- AWS Landing Zone: https://aws.amazon.com/solutions/aws-landing-zone/
- AWS CloudFormation: https://aws.amazon.com/cloudformation/
- AWS Service Catalog Connector for ServiceNow: https://aws.amazon.com/blogs/aws/new-aws-service-catalog-connector-for-servicenow/
- AWS Well Architected Framework Reliability Pillar: https://d1.awsstatic.com/whitepapers/architecture/AWS-Reliability-Pillar.pdf
- Amazon CloudWatch: https://aws.amazon.com/cloudwatch/
- AWS Simple Notification Service: https://aws.amazon.com/sns/
- *re:Invent 2017* presentation – Operation Monitoring and Alerting at Scale in GE Transportation (ENT340): https://www.youtube.com/watch?v=asCEyfPMv2s
- Cloud Adoption Framework: https://aws.amazon.com/professional-services/CAF/
- Contact us: https://aws.amazon.com/contact-us/

Contributors

Contributors to this document include:

- James Kingsmill, AWS Solutions Architect
- John Hildebrandt, AWS Head of Security Assurance, Australia and NZ
- Cameron Tod, AWS Solutions Architect
- Aun Iftikhar, AWS Solutions Architect
- Ricardo Schmidt, AWS Solutions Architect

Document Revisions

Date	Description
October 2019	First publication.
October 2019	Added guidance around security compliance and IRAP.
February 2020	Added contributors.