Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian Cyber Security Centre

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY — CISA

Business Continuity in a Box

Guidance: Continuity of Applications

Content Complexity
MODERATE ● ● ○

cyber.gov.au

Contents

Disclaimer

The information herein is being provided “as is” for information purposes only. The authors do not endorse or favour any commercial entity, product, company, or service, including any entities, products, or services linked or otherwise referenced within this document.

Introduction

Purpose

Application continuity is critical to any organisation in maintaining service availability and integrity. To reduce downtime, costs and business impact of incidents, organisations should quickly stand up interim solutions if their normal operating environment is lost, unavailable or compromised. Depending on an organisation's business requirements, this may include internal services such as payroll or file sharing, or more expansive requirements such as engagements with external providers, customers or the public.

Continuity of Applications focuses on establishing interim business-critical applications during a cyber incident. The package assists organisations to quickly and securely design and deploy an interim cloud solution for hosting core applications.

Before deploying the interim cloud solution, organisations must assess any risks associated with organisational data being stored on an interim cloud solution, including any additional security controls that may be required.

For guidance on how to assess and manage risk, see:

- Assess and Manage Risk at business.gov.au/risk-management/risk-assessment-and-planning/assess-and-manage-risk

Overview

Options for Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) and Infrastructure-as-a-Service (IaaS) are discussed within this guidance, with a primary focus on IaaS.

This guidance – developed by the Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC) with contributions from the United States Cybersecurity and Infrastructure Security Agency (CISA) – does not provide prescriptive or long-term architectures. Instead, it provides an interim solution for the deployment and operation of critical business applications where an organisation's systems may have been affected by a cyber incident.

The concepts and examples in this document use relevant cloud hosting providers' 'rehosting' guidance – also known as 'lift and shift' – for interim system deployment.

How to use this document

This document provides guidance for deploying an interim cloud-based business continuity solution that leverages the benefits of a cloud-hosted system or applications. Implementation of this guidance requires an intermediate level of knowledge of cloud services. This guidance is not for systems and services currently undergoing redevelopment or redesign to leverage the benefits of cloud hosting, nor new systems and services provisioned directly to a cloud environment.

This document is divided into three consecutive stages. It is recommended the reader review the document in its entirety before commencing Stage 1. It is possible some organisations will not need to implement all three stages of this guidance. This will depend on an individual organisation's needs and requirements established in Stages 1 and 2.

Guidance

Stage 1: Determine your critical applications

Identifying critical business functions and their associated applications is integral to resuming operations. Critical business functions are those activities that are vital to an organisation's survival and to the resumption of business operations

Typically, critical business functions are those that:

1. Are most impacted by downtime or unavailability
2. Play a key role in maintaining business operations and deliverables
3. Fulfill legislative and/or regulatory obligations
4. Safeguard an irreplaceable asset

Identification and classification of functions:

1. Identify the critical business functions of your organisation.
2. Classify these critical business functions into the following categories:
    iii. High (most critical)
    iv. Medium
    v. Low (least critical)

Based on the above factors, decide which functions are to be prioritised and included in the following stages.

Stage 2: Determine your continuity path

When deciding on the best interim solution for an organisation, key factors may include cost, and ease of deployment and operation. SaaS, PaaS and IaaS are the three main cloud computing services with each providing different features, functionalities and benefits. The most appropriate offering is dependent on an organisation's requirements for hosting, storing, managing and processing information and data.

Software as a service

To ensure ease of deployment across many corporate applications, one of the most common cloud services is SaaS – it offers both consumers and businesses cloud-based tools and applications for everyday use. Common examples include the Microsoft 365 suite of productivity software, and MYOB or Xero for financial management.

SaaS services are readily available as an off-the-shelf solution for most users. In many cases companies offer a trial period followed by a monthly pay-as-you-go service, though they tend to create a lock in effect that means it can be difficult to export data. Organisations should generally consider the use of SaaS when looking for a more permanent cloud solution.

Platform as a service

PaaS allows developers to host, build and deploy their consumer-facing apps on a platform. Generally, PaaS management and ownership stays with the developers, affording little to no control to organisations regarding patching and updates of the underlying host infrastructure. PaaS can also be slower to deploy than IaaS and SaaS, due to the development time.

Infrastructure as a service

IaaS platforms allow an organisation to manage their business resources such as their network, servers and data storage on the cloud. IaaS is a pay-as-you-go service, which allows for cancellation any time after the initial 30-day trial period. This makes it beneficial as a short-term business continuity solution.

As an interim solution, an IaaS platform will most closely mimic the existing computing infrastructure that would normally be hosted locally on an organisation's premises. As IaaS can offer the ability to replicate and recover core services in a rapid and straightforward manner, the remainder of this guidance concentrates on the deployment of an IaaS cloud solution.

Stage 3: Deploying an IaaS application environment

This section provides a high-level implementation framework for deploying IaaS as a solution. This guidance includes a list of steps to follow, along with a set of assumptions and constraints that should be considered before starting the deployment.

Assumptions

This guidance assumes personnel implementing the interim IaaS solution have:

- An understanding of cloud computing concepts and architectures, including IaaS
- Access to the necessary cloud hosting provider services and tools to deploy the solution
- A good understanding of any organisation-specific configuration settings that need to be applied to the IaaS solution

Constraints

The following constraints should be considered before deploying the interim IaaS architecture:

- The IaaS solution must adhere to the security and compliance requirements of the organisation
- The IaaS solution must meet any performance and availability requirements set by the organisation
- The IaaS solution must be scalable for the organisation's requirements and easily maintainable

Architecture principles

Cloud-based IaaS and PaaS deployments are subject to several additional threats not commonly addressed in an on-premises architecture. This is typically due to the presence of compensating features for on-premises systems, which include single network entry points, trusted user base, and limited physical server access. As such, directly migrating an on-premises system to a cloud-based IaaS solution could immediately expose the rehosted system and potentially the organisation to unaddressed risks.

To minimise these risks, this guidance introduces several architecture principles to allow the rapid migration of a system, effecting minimal changes to the system and increasing security by leveraging additional security capabilities available within various cloud platforms. The principles within this guidance each have key considerations, which often in themselves can be broken into architecture principles. For simplicity, only the high-level principles are defined, with additional information in the details of each principle. An overview of the three (3) principles is provided.

Maintain security boundaries

The principle of maintaining security boundaries emphasises the need to preserve the existing security boundaries established in the on-premises hosted system during the migration to a cloud IaaS platform. For example, databases residing on a server for the on-premises hosted solution will remain on an equivalent IaaS host rather than being migrated to an SQL PaaS.

By maintaining existing security boundaries, the organisation can retain the same level of control and visibility over its critical business systems, ensuring a consistent security posture. This principle allows for a smoother migration process, as it minimises the need for significant architectural changes whilst still taking advantage of the benefits provided by cloud IaaS platforms.

Enhance security controls

The principle of enhancing security controls highlights the importance of leveraging additional security capabilities available within cloud IaaS platforms to strengthen the overall security posture of the migrated system. Cloud platforms offer various security features, such as network security groups, security services, and identity and access management tools.

During the migration process, it is essential to identify gaps with the on-premises hosted system and design appropriate controls or compensating controls using the available cloud platform features. By taking advantage of these enhanced security controls, the organisation can address the additional threats introduced by cloud deployments and mitigate the associated risks effectively.

Ensure compliance and governance

This principle emphasises the need to maintain regulatory compliance and adhere to the organisation's governance requirements. Moving to a cloud IaaS platform introduces additional compliance considerations such as data sovereignty, data protection, and other industry-specific regulations.

To ensure appropriate compliance and governance arrangements, it is crucial to fully understand the applicable regulations and requirements of the organisation before migrating the system to the cloud. This assessment should inform the design and implementation of security controls and processes that align with organisation and regulatory compliance needs. Additionally, organisations should establish proper monitoring and auditing mechanisms to maintain compliance in a cloud-hosted environment.

Process

Planning

1. Select the cloud service provider (CSP) based on your organisation's operational requirements
2. Define the target architecture for the system
3. Develop a plan for preparation, migration, security and compliance, and review and optimisation

Infrastructure deployment

4. Procure a subscription from the selected CSP
5. Set up and configure necessary resources to meet operational needs
6. Implement additional security features to address any new threats resulting from the interim cloud implementation

Data migration

7. If possible, restore data from available backups
8. If necessary, ensure systems are connected to a centralised user directory

Security and compliance

9. Implement security controls suggested within the examples and patterns, including encryption, privileged administration workstations, gateway, and federated identity security patterns
10. Validate the security controls through testing and auditing from within the cloud service provider portals and tools
11. Implement additional compliance measures, such as implementing applicable security controls, logging and monitoring, and reporting

Review and optimisation

12. Particularly in the initial stages of deployment, perform regular reviews of the migrated systems to determine where resources can be optimised, and costs reduced
13. Document the new architecture and additional changes made to accommodate for the change to a cloud hosting provider

Components

IaaS implementations, regardless of selected CSP are comprised of several components or resources. When migrating on-premises systems to IaaS platforms, it is essential to understand the differences in components and their corresponding security controls to ensure secure operation of the system.

By understanding and addressing the unique security considerations for each component and the system, organisations can implement effective security controls and measures to protect their cloud IaaS solutions.

Virtual infrastructure

Virtual machines (VM) are the primary compute resources in a cloud IaaS environment. They host operating systems, applications, and services required for system functionality. When migrating on-premises hosted systems, equivalent VMs should be provisioned to maintain system architecture.

Implement security controls for VMs, such as:

- Hardened Images: Utilise hardened VM images or templates that follow security best practices for the specific operating system and application stack.
- Patch Management: Consistently apply security patches and updates to VMs to address known vulnerabilities.
- Anti-Malware/Antivirus: Install and configure anti-malware or antivirus software on VMs to detect and prevent malicious activities.
- Least Privilege: Assign appropriate permissions and access controls to VMs to restrict access to only approved administrators and users.

Storage

Cloud platforms offer several types of storage services to store and manage data, such as:

- Object Storage: Object storage services, such as Amazon S3, Azure Blob Storage, or Google Cloud Storage, allow storage and retrieval of unstructured data, such as documents, images and multimedia files.
- Block Storage: Block storage is suitable for VMs requiring persistent storage. This provides low-latency access and is suitable for hosting data, such as operating system disks and databases.
- File Storage: Leverage file storage services, such as Amazon EFS, Azure Files, or Google Cloud File store to provide shared file systems accessible by multiple VMs.
- Backup and Recovery: Implement regular backup and recovery mechanisms for critical data and configurations. Leverage snapshotting, replication, or cloud-native backup solutions provided by the CSP and if possible, copy the backups to a separate location.
- Encryption: Enable encryption for data at rest in storage services to protect sensitive information from unauthorised access.

Identity and access management

Identity and access management (IAM) is a critical component for controlling user access and managing authentication and authorisation in a cloud environment.

User and Access Management

- User Provisioning: Implement a centralised user management system or integrate with an existing identity provider to enable user account management, authentication, and authorisation.
- Multi-Factor Authentication (MFA): Enforce the use of MFA for user and administrator accounts to add an extra layer of security beyond passwords.
- Role-Based Access Control (RBAC): Define roles with granular permissions and assign to users based on job responsibilities.
- Access Reviews: Conduct regular access reviews to ensure user permissions are up to date and aligned with business requirements.
- Privileged Access Management
- Privileged Account Management: Implement a privileged access management solution to control and monitor privileged account usage. Utilise just-in-time access and session recording to limit the exposure of administrative privileges.
- Privileged Access Reviews: Regularly review and recertify privileged accounts and permissions to maintain appropriate access controls.

Security

Implementing robust security measures is crucial to protect the cloud environment and the hosted system from potential threats and vulnerabilities.

Network Security

- Virtual Private Cloud (VPC): Utilise VPCs to quickly isolate the cloud environment and establish network segmentations. Configure subnets, network access control lists (ACLs), and security groups to control inbound and outbound traffic.
- Firewalls: Implement virtual firewalls to filter internet traffic and network and server firewalls to filter and control traffic flow between network components. If the on-premises environment separated the network into zones, ensure the architecture is maintained through use of subnets and additional virtual firewalls if needed.
- Intrusion Detection and Prevention Systems (IDS/IPS): Deploy IDS/IPS solutions to detect and prevent network-based attacks, anomalous traffic, and known attack signatures. Unless an IDS/IPS solution existed for the on-premises system, implementation of this capability should at minimum, be deployed between the internet and hosted network.

Data Protection

- Encryption: Utilise encryption mechanisms, such as transport layer security (TLS) to protect data in transit between components and applications. Implement encryption for data at rest for sensitive data stored in storage services or databases.
- Data Loss Prevention (DLP): Deploy DLP controls to detect and prevent the unauthorised transmission or storage of sensitive data. Use predefined policies or custom rules to identify and mitigate data leakage risks.
- Data Backup and Recovery: Establish a regular backup and recovery strategy for critical data to ensure business continuity in the event of data loss or system failure.

Endpoints

Endpoints refer to the devices or client systems used to access the cloud-hosted system.

- Endpoint Security: Implement endpoint protection measures, including antivirus software, host-based firewalls, and secure configurations, on devices used to access the cloud environment.
- Secure Remote Access: Utilise secure remote access technologies, such as virtual private networks (VPNs) or bastion hosts, to establish secure connections between client systems and the cloud environment.

IaaS architectural patterns

The following guidance provides three high-level architectural patterns that can be utilised in planning the organisation's interim IaaS cloud solution. The patterns provide details of common architectures for systems, which are deployed in on-premises environments, and can be rehosted to an equivalent cloud-hosted solution. Each architecture represents an approach to structuring a system within the cloud environment.

Presented after this high-level guidance, are examples of deployments for an n-tier architecture within Azure, Amazon Web Services (AWS), and Google Cloud to demonstrate the additional services that should be considered to secure the system.

Single-tier architecture

A single-tier architecture is a simple, standalone setup where the client, server and data storage components are all combined in a single server. This model is typically implemented for small applications.

Advantages

- Easy to set up and manage due to its simplicity.
- Cost-effective for small-scale applications.

Disadvantages

- As the application grows, scalability can become a challenge.
- Since all components reside in a single location, security and fault tolerance is sacrificed or significantly reduced compared with other architectures.

Single-tier

A single-tier provides a combination of user interface, business processing logic, and data store in the form of a file system or database. All system and user actions are processed here.

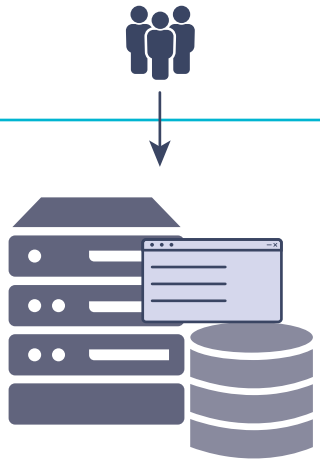

Figure 1 - Single tier system architecture

Two-tier architecture

In a two-tier architecture, the client and server components are separated, typically by a client tier (user interface) that communicates directly with the data tier (database or file store).

Advantages

- Better performance and scalability than single tier, as the client and server are separated.
- Enables scalability of each tier or independent management, potentially resulting in lower cost for greater performance gains.

Disadvantages

- Lack of separation between the application logic and database can lead to slower performance as the application grows.
- Greater likelihood of security issues as there is a direct link between the client and database.

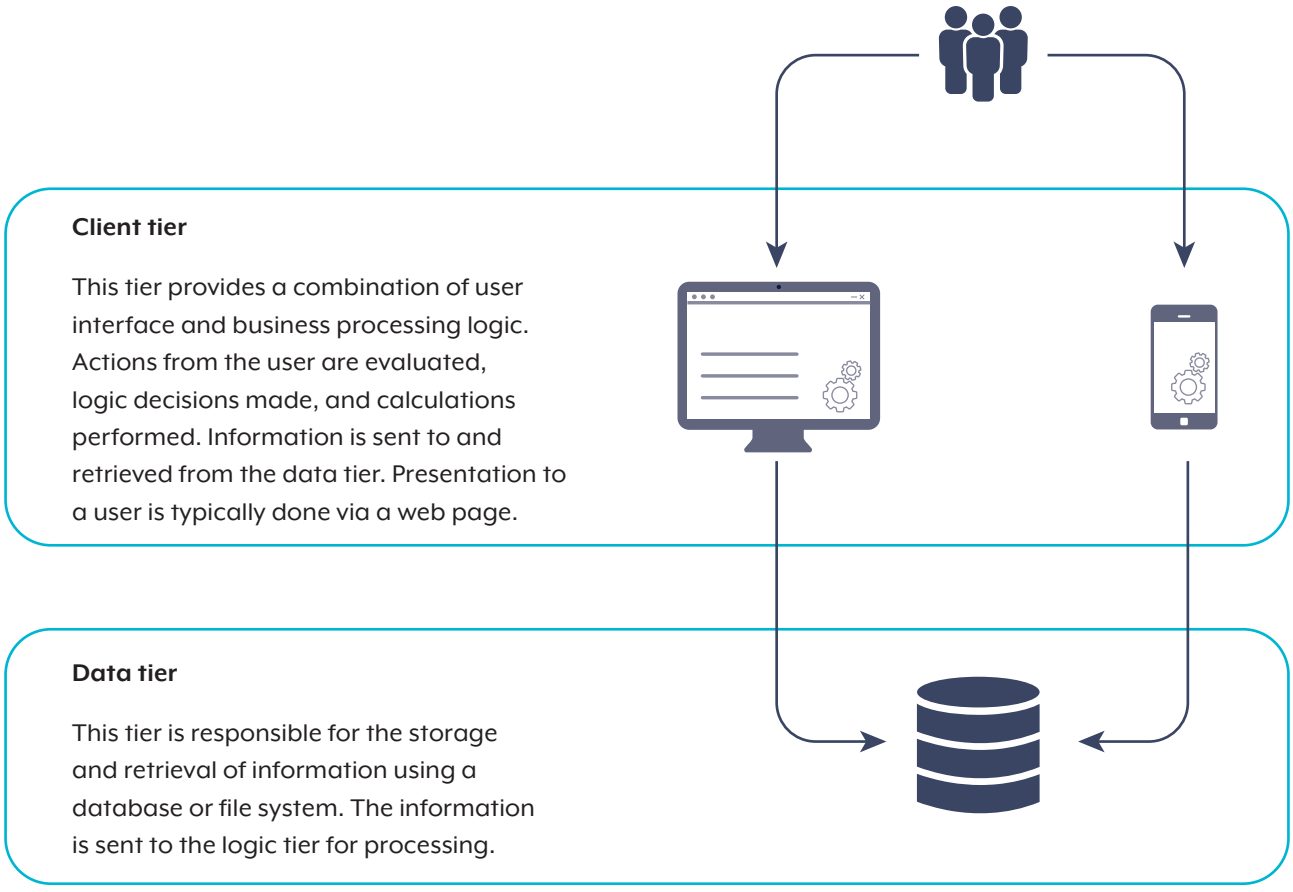

Figure 2 - Two-tier system architecture

N-tier architecture

An n-tier architecture (also known as multi-tier architecture) divides a system into three or more separate tiers. A common model for this architecture is a system consisting of a presentation layer (client/user interface), an application layer (business logic), and a data layer (database or file store).

Advantages

- High scalability and flexibility, as each tier can be managed, scaled, and updated independently.
- Provides increased security as each tier acts as a boundary, making it more difficult for an attacker to compromise the entire system.

Disadvantages

- More complex to design, deploy and manage due to the separation of components.
- Requires careful design to ensure performance and responsiveness, particularly as network latency can become a factor.

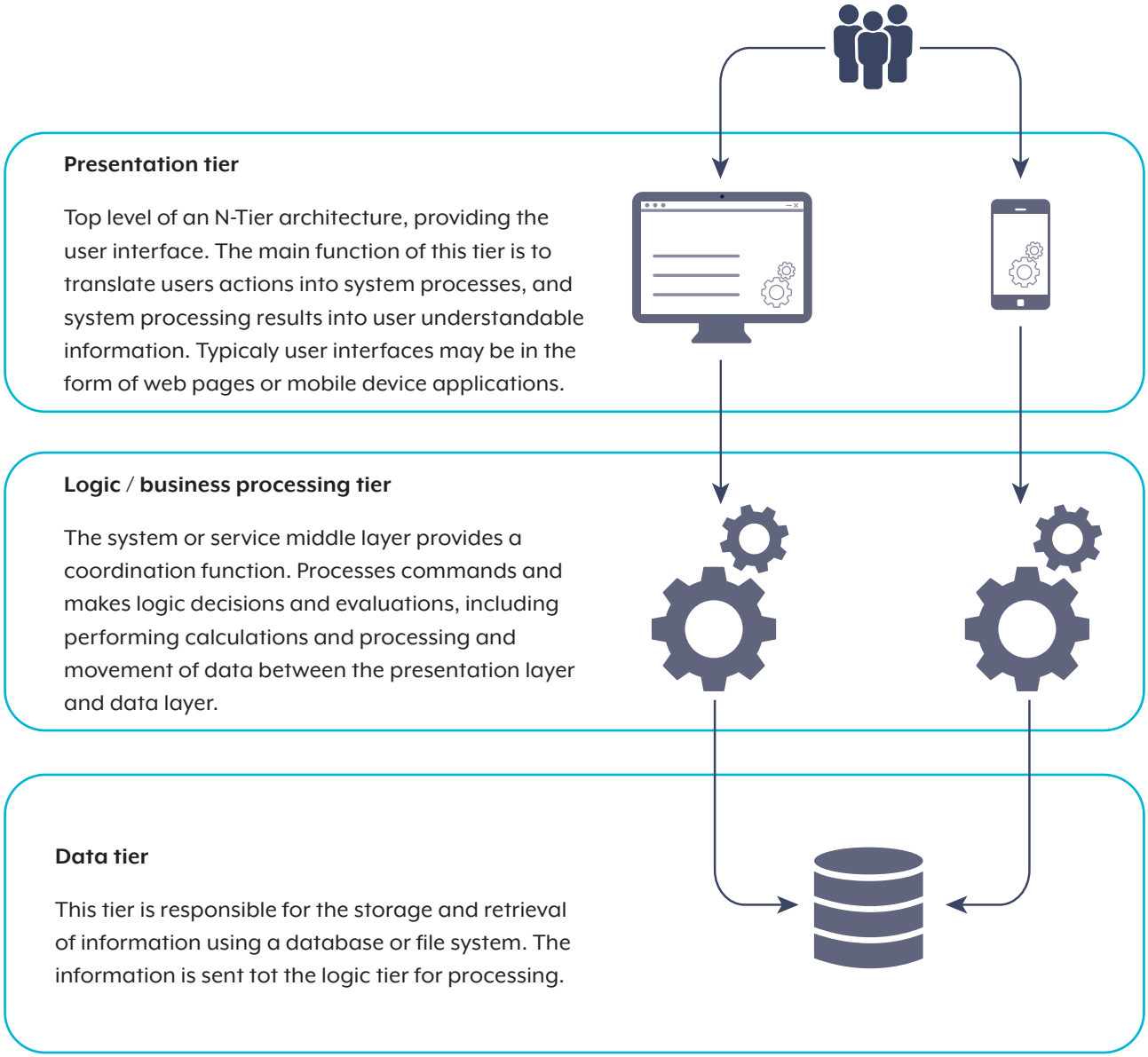

Figure 3 - N-tier system architecture

Example IaaS solutions

The following solution designs provide details of a system rehosted from an on-premises environment to Azure, AWS, and Google Cloud. The details within these examples provide information on the various technologies available within each platform.

Solution design example for Azure

Azure IaaS is a cloud computing service that offers essential computing, storage and networking resources on demand, through a pay-as-you-go service.

Migration of your organisation's infrastructure to an IaaS solution provides a reduction in maintenance of the on-premises data centre, savings on hardware costs, and gains real-time business insights. IaaS solutions allow the organisation to scale IT resources up and down with business demands. IaaS also helps the organisation to quickly provision new applications and increase the reliability of the underlying infrastructure.

Azure manages the infrastructure, while organisations purchase, install, configure and manage their software, including operating systems, middleware and applications. Tiers are a way to separate responsibilities and manage dependencies – each layer has a specific responsibility. A higher tier can use services in a lower tier, but not the other way around.

Tiers are physically separated, running on separate machines. A tier can call another tier directly or use asynchronous messaging (message queue). Although each layer might be hosted in its tier, it is not required. Several layers might be hosted on the same tier. Physically separating the tiers improves scalability and resilience but also adds latency from the additional network communication.

A traditional three-tier application has a presentation tier, a middle or application tier, and a database tier. The middle tier is optional. More complex applications can have more than three tiers. The diagram below shows a typical 3-tier IaaS, encapsulating different areas of functionality.

Each tier consists of two or more VMs, placed in an availability set or virtual machine scale set. Multiple VMs provide resiliency in case one VM fails. Load balancers are used to distribute requests across the VMs in a tier. A tier can be scaled horizontally by adding more VMs to the pool.

Each tier is also placed inside its own subnet, meaning its internal IP addresses fall within the same address range. That makes it easy to apply network security group rules and route tables to individual tiers.

The web and application tiers are stateless. Any VM can handle any request for that tier. The data tier should consist of a replicated database. For Windows, we recommend SQL Server, using Always On availability groups for high availability. For Linux, choose a database that supports replication, such as Apache Cassandra.

Network security groups restrict access to each tier. For example, the database tier only allows access from the application tier.

For secure administration of the system, it is recommended to deploy an Azure Bastion service. Bastion provides secure remote desktop protocol (RDP) and secure socket shell (SSH) connectivity to all the VMs in the virtual network in which it is provisioned. Azure Bastion protects your virtual machines from exposing RDP/SSH ports to the outside world while providing secure access using RDP/SSH.

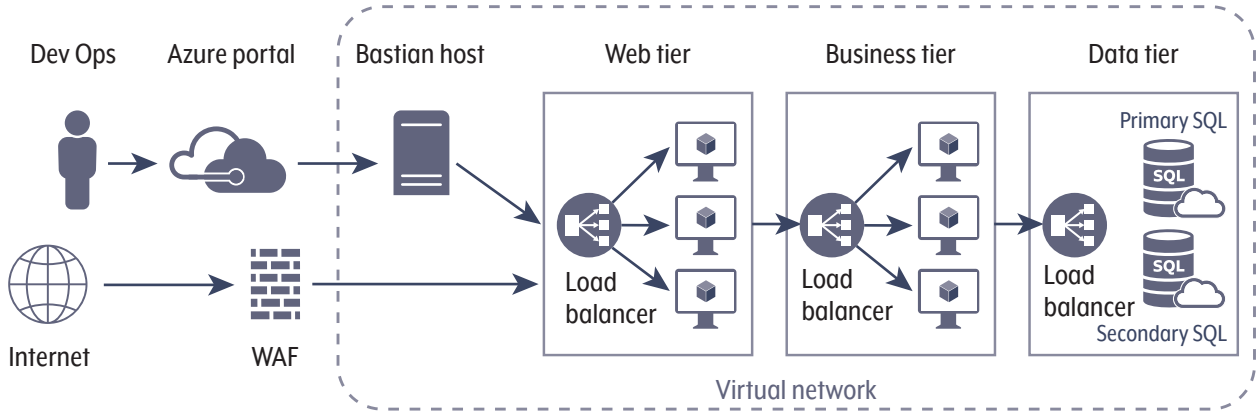

Figure 4 – typical Azure N-tier IaaS system architecture

Solution design example for AWS

Amazon Elastic Compute Cloud (Amazon EC2) provides scalable computing capacity in the AWS Cloud. Using Amazon EC2 eliminates the need for organisations to invest in hardware upfront to develop and deploy applications faster.

Amazon EC2 can be used to launch as many or as few virtual servers as required, configure security and networking, and manage storage. Amazon EC2 enables an organisation to scale up or down to handle changes in requirements or spikes in the required resources, reducing the need to forecast traffic.

Amazon EC2 provides a web-based user interface, the Amazon EC2 console. Administrators can access the privileged user interface after signing up for an AWS account, signing into the AWS Management Console, and selecting EC2 from the console home page.

Amazon EC2 supports creating resources using AWS CloudFormation. Developers can create a template in JSON or YAML that describes the organisation's AWS resources, AWS CloudFormation provisions, and configures those resources. Organisations can reuse the developed CloudFormation templates to provision the same resources multiple times, whether in the same region and account or multiple regions and accounts.

Amazon EC2 provides a Query API. These requests are HTTP or HTTPS requests that use the HTTP verbs GET or POST and a query parameter named Action. Developers may prefer to build applications using language-specific APIs instead of submitting a request over HTTP or HTTPS. AWS provides libraries, sample code, tutorials, and other resources for software developers.

When administering the EC2 platform, AWS strongly suggests using SSH access to further secure the services and their instances by implementing a Bastion host, also known as a 'Jump Box'.

A bastion host is a special-purpose machine utilised for privileged access that is configured and hardened to work against attacks. The machine contains a single application, which it hosts. Bastion hosts are accessed with the help of SSH or RDP protocols. After connectivity (remotely) is established with the bastion host, it allows using SSH or RDP to log in to other instances (thereby behaving like a 'jump server') that are present within the private network/subnet. The diagram below shows a typical AWS EC2 3-tier IaaS architecture.

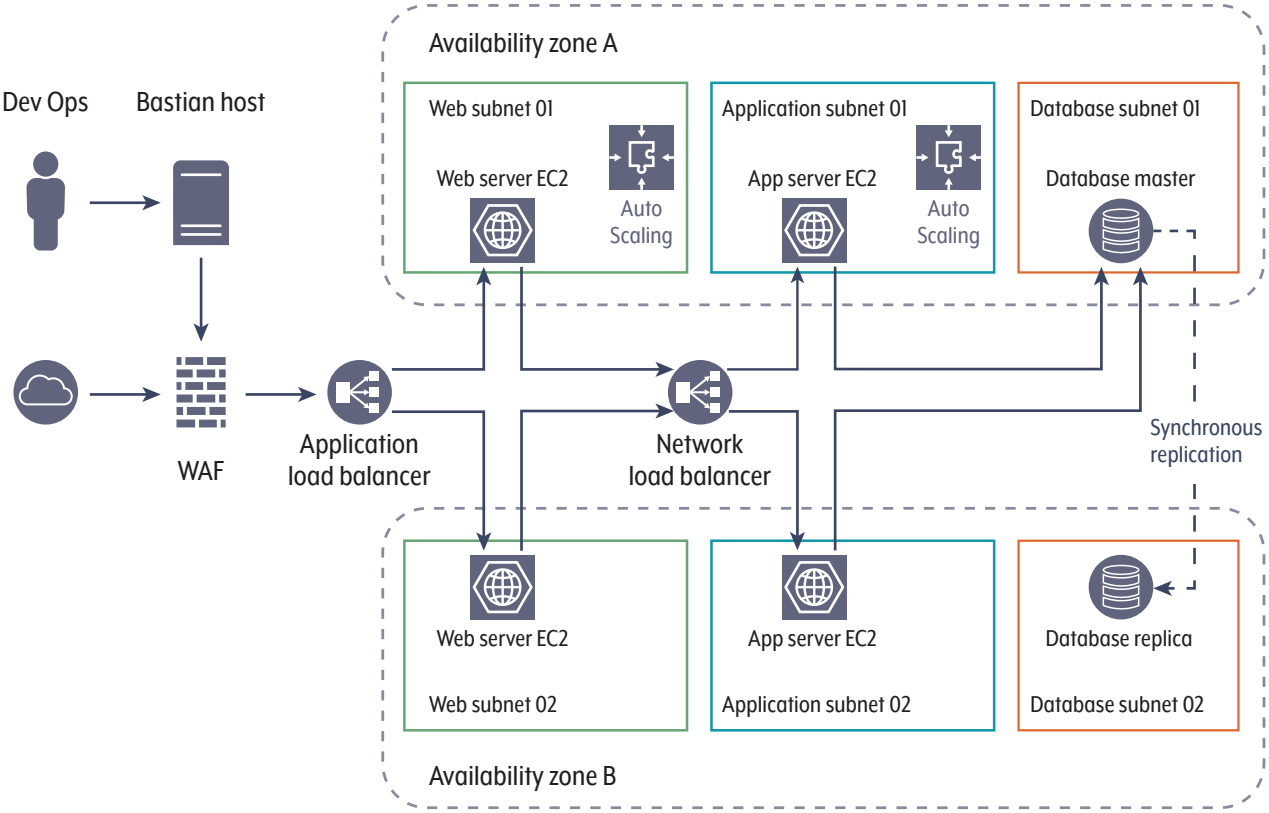

Figure 5 – typical Amazon Web Services N-Tier IaaS system architecture

Solution design example for Google Cloud Platform

Google Cloud Platform (GCP) is a suite of cloud computing resources for developing, deploying and operating applications on the web. GCP utilises the same infrastructure that Google uses internally for its end-user products. GCP IaaS provides a series of modular cloud services, including computing, data storage, data analytics and machine learning.

GCP provides whole infrastructure for business applications and assures security and reliability. GCP provides many APIs such as YouTube, Gmail, maps etc. It includes the options to create projects and work on specific projects, thus creating isolation. GCP is widely used in app development, as it provides several APIs.

When applications, websites or other cloud services are run on GCP, Google tracks the resources being used, such as processing power, storage and network connections. Unlike most conventional services that charge by the month, GCP charges by the minute to keep customer costs low. When using GCP to build and deliver your services, organisations can leverage the power of hyperscale in data centres or borrow sophisticated analytics and AI functions to reach users worldwide.

The GCP Virtual Private Cloud (VPC) network is a virtual version of a physical network implemented inside Google's production network using Andromeda. VPC networks, along with their associated routes and firewall rules, are global resources and are not associated with any distinct region or zone. A VPC network provides the following benefits:

- Connectivity to your Compute Engine VM instances, including Google Kubernetes Engine (GKE) clusters, App Engine flexible environment instances, and other GCP products built on Compute Engine VMs.
- Native Internal TCP/UDP Load Balancing and proxy systems for Internal HTTP(S) Load Balancing.
- Connection to on-premises networks using Cloud VPN tunnels and Cloud Interconnect attachments.
- Distributes traffic from Google Cloud external load balancers to back ends.

Google recommends that the management of the GCP be conducted by a bastion host, providing an external facing point of entry into a network containing private network instances. Bastion host offers a single point of fortification or audit and can be started and stopped to enable or disable inbound SSH. By using a bastion host, privileged users can connect to a VM that does not have an external IP address. This approach allows administrators to connect to a development environment or manage the database instance – at times without configuring additional firewall rules – for an external application. The below diagram represents typical GCP N-Tier architecture.

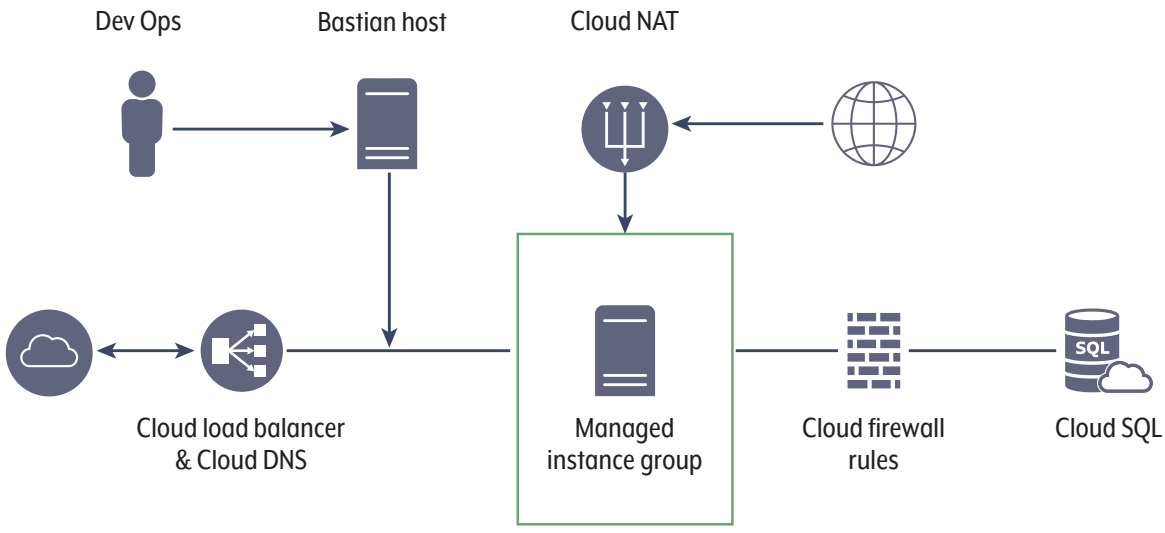

Figure 6 – typical Google Cloud Platform N-tier IaaS system architecture

Contact

For any enquiries concerning this guidance or to provide feedback, please navigate to cyber.gov.au/about-us/about-asd-acsc/contact-us. Select 'General enquiry or feedback', and choose 'Business Continuity in a Box' from the drop-down menu under 'Your enquiry/feedback type'.

If you or your organisation are victim of a data breach or cyber incident, follow relevant cyber incident response and communication plans, as appropriate.

Australian organisations impacted by, or requiring assistance relating to, a cyber incident can contact ASD's ACSC via 1300 CYBER1 (1300 292 371), or by using ReportCyber at cyber.gov.au/report-and-recover/report.

United States organisations may report cyber incidents to CISA's 24/7 Operations Center at report@cisa.dhs.gov, cisa.gov/report, or (888) 282-0870. When available, please include information regarding the incident: date, time and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organisation; and a designated point of contact.

Appendix A: acronyms, abbreviations and definitions

This document uses the following acronyms and abbreviations:

Acronym or Abbreviation	Definition
ACL	Access Control Lists
Amazon EC2	Amazon Elastic Compute Cloud
API	Application Programming Interface
AWS	Amazon Web Services
CSP	Cloud Service Provider
DLP	Data Loss Prevention
EFS	Elastic File System
GCP	Google Cloud Platform

GKE	Google Kubernetes Engine
HTTP(S)	Hyper Text Transfer Protocol (Secure)
IaaS	Infrastructure-as-a-Service
IDS/IPS	Intrusion Detection and Prevention Systems
IP	Internet Protocol
JSON	JavaScript Object Notation
MFA	Multifactor Authentication
PaaS	Platform-as-a-Service
RBAC	Role based Access Control
RDP	Remote Desktop Protocol
SaaS	Software-as-a-Service
SQL	Structured Query Language
SSH	Secure Socket Shell
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
VM	Virtual Machine
VPC	Virtual Private Cloud
VPN	Virtual Private Network
YAML	A Human-Readable Data Serialisation Language

For more information, or to report a cyber security incident, contact us:
cyber.gov.au | 1300 CYBER1 (1300 292 371)

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre