SERVICE DEFINITION DOCUMENT

AMZU INFORMATION TECHNOLOGY LTD
VERSION 1.1/2024

The service definitions in this document are generic; we are happy to create a custom service definition document based on your requirements.

ABOUT US

Amzu emerged from our extensive experience with cloud complexities, backed by over 20 years of expertise in insurance, banking, and financial services. Our founders, with their exceptional tech skills, prioritise robust processes and meticulous execution. We are dedicated to proactively identifying and solving our customers' challenges, ensuring a seamless experience across our diverse client base.

Table of Contents

1. Service Features

- **Cloud Strategy and Planning:**
    - Business analysis to understand client requirements.
    - Solution design tailored to business objectives.
    - Detailed cloud migration roadmap and implementation strategy
    - Robust security architecture design
- **Cloud Implementation and Migration:**
    - Initial assessment and strategy development
    - Customised migration plan
    - Technical execution and support throughout the migration process
    - Security and compliance adherence during migration
    - Optimisation and post-migration support
- **Cloud Security and Compliance:**
    - Security strategy development
    - Security design implementation
    - Cybersecurity consultancy
    - Security incident management
    - Security auditing services
- **Cloud Management and Optimization:**
    - Monitoring and management of cloud resources
    - Troubleshooting and technical support
    - Updates and maintenance
    - Cost optimisation
- **Cloud Support and Training:**
    - Vendor-neutral cloud hosting support (AWS, Azure, GCP)
    - Third-party cloud software support (Microsoft Office, Google Workspace, custom apps)
    - Tailored cloud training programs
- **Specialised Cloud Solutions:** Based on our Client’s unique requirements.

2. Service Benefits

Below are some of the benefits you could gain from our Cloud Consultancy Service.

- Reduces deployment times.
- Enhances security and mitigates risks.
- Lowers operational costs.
- Improves scalability.
- Increases organisational agility.
- Optimises performance.
- Facilitates better decision-making.
- Strengthens disaster recovery.
- Simplifies operations.
- Boosts productivity

All services are subject to mutual agreement and may incur additional costs, which can be agreed upon before any project initiation.

3. Service Planning

How it Works:

1. Initial Assessment Phase

- **Business Needs Analysis**: The service provider conducts interviews and surveys with the client's key stakeholders to understand their specific needs, challenges, and objectives. This includes assessing the current IT infrastructure to determine compatibility and readiness for cloud integration.
- **Requirement Gathering**: Specific requirements for the cloud software are identified, including performance, security, and scalability needs.
- **Risk Assessment**: Potential risks, including data migration risks, security vulnerabilities, and compliance issues, are identified and evaluated.

2. Service Design Phase

- **Solution Designing**: Based on the requirements and assessments, a design for the cloud solution is developed. This includes selecting the appropriate cloud platform (e.g., AWS, GCP, Azure), planning the architecture, and determining the necessary cloud services and resources.
- **Security Architecture**: A security plan is created to ensure the solution meets all required compliance and security standards.
- **Budgeting and Resource Allocation**: A budget and resources are formulated, ensuring that the project stays within financial limits while meeting all technical requirements.

3. Implementation Planning Phase

- **Project Timeline Creation**: A detailed project timeline is established, outlining all key milestones and deadlines.
- **Deployment Strategy**: The strategy for deploying the new cloud solution is formulated, including the phasing out of retiring systems, data migration plans, and integration with existing systems.
- **Testing Plans**: Plans for system testing, including performance and security testing, are developed to ensure the solution meets all specified requirements before going live.

4. Training and Change Management

- **Training Programs**: Custom training programs are developed for end-users and IT staff to ensure they can effectively use and manage the new system.
- **Change Management Strategy**: A change management plan is created to help employees transition to the new system, address potential resistance, and ensure smooth adoption.

5. Deployment and Go-Live

- **Final Testing and Adjustments**: Before going live, final testing is conducted and any necessary adjustments are made.
- **System Migration**: The cloud solution is deployed, and data migration is completed according to the plan.
- **Go-Live Support**: Intensive support is provided during and immediately after the go-live phase to address any immediate issues.

6. Post-Deployment Support and Evaluation

- **Ongoing Support**: Subject to mutual agreement, regular support and maintenance are provided to address any issues, update systems, and ensure continuous operation.
- **Performance Monitoring**: As part of the ongoing support, the system's performance is continuously monitored against established KPIs to ensure it meets business needs.
- **Feedback and Iteration**: On mutual agreement, feedback is gathered from users, and improvements are made over time based on this feedback.

Supported Cloud Services: Microsoft Azure, Amazon Web Service, Google Cloud Platform

4. Setup or Migration Service

How it Works:

1. Initial Consultation

- **Client Requirements:** Begin with a discussion to understand the client's specific needs, the scope of the migration, and the systems involved.
- **Technical Assessment:** Evaluate the current infrastructure to identify the technical requirements, dependencies, and potential challenges.

2. Planning

- **Migration Strategy:** Develop a comprehensive migration plan that includes the choice of technology, migration tools, and the sequence of migrating data and applications.
- Risk Management: Identify risks associated with the migration and establish protocols for risk mitigation.
- **Timeline and Milestones:** Set a realistic timeline with key milestones to guide the migration process.

3. Preparation

- **Infrastructure Setup:** If needed, set up new infrastructure that will support the applications and data being migrated.
- **Data Preparation:** Prepare the data for migration, which may involve data cleansing, data backup, and ensuring data integrity.

4. Migration Execution

- **Data Transfer:** Begin the actual migration of data using the chosen tools and methods. This may be done in stages to minimise operational disruption.
- **Application Migration:** Migrate applications, ensuring they are properly configured and integrated with the new environment.
- **Testing Phase:** Conduct thorough testing at each stage to ensure data and application integrity, functionality, and performance in the new environment.

5. Finalisation and Transition

- **System Integration:** Integrate migrated applications and data into the existing IT environment, ensuring seamless operation.
- **Final Testing and QA:** Perform final testing to ensure the entire system operates as expected without losing data or functionality.

6. Post-Migration Support

- **Monitoring:** Monitor the new system for issues arising following the migration.
- Optimisation: Optimize system performance based on operational feedback and performance metrics.
- **User Training:** Train users on the new systems to ensure smooth adoption.

7. Documentation

- **Migration Report:** Document the migration process, outcomes, and lessons learned.
- **Support and Maintenance Guidelines:** Provide detailed documentation on system support, potential troubleshooting steps, and maintenance schedules.

Supported Cloud Services: Microsoft Azure, Amazon Web Service, Google Cloud Platform

5. Security Services

How It Works:

1. Security Assessment

- **Risk Analysis**: Conduct a thorough risk analysis to identify potential vulnerabilities in the organisation's IT environment. This includes analysing current security measures, systems, networks, and data practices.
- **Threat Modelling**: Develop threat models based on potential attack vectors, considering external and internal threats.
- **Security Auditing**: Perform audits of existing security policies, practices, and controls to evaluate their effectiveness and compliance with regulatory requirements.

2. Security Design

- **Architecture Design**: Design a robust security architecture that integrates with the existing IT infrastructure. This may involve segmenting networks, designing secure communication channels, and implementing secure data storage solutions.
- **Policy Development**: Develop or update security policies and procedures to address identified risks and compliance requirements. This includes access control policies, incident response plans, and data protection policies.

3. Implementation

- **Security Solutions Deployment**: Install and configure security solutions such as firewalls, intrusion detection systems, encryption tools, and antivirus software.

- **Access Controls**: Implement strict access control measures, including role-based access controls, multi-factor authentication, and least privilege principles.
- **Security Training**: Provide comprehensive security training for all employees, focusing on best practices, threat awareness, and response procedures.

4. Monitoring and Response

- **Continuous Monitoring**: Implement tools and processes for continuous monitoring of the IT environment to detect and respond to security incidents in real time.
- **Incident Response**: Develop and regularly update an incident response plan that outlines procedures for responding to security breaches, including notification protocols and remediation steps.

5. Testing and Evaluation

- **Penetration Testing**: Based on the requirement, we can arrange penetration testing to identify vulnerabilities in the IT infrastructure that attackers could exploit.
- **Security Audits**: Based on the requirement, periodic security audits are performed to assess the effectiveness of implemented security measures and identify areas for improvement.
- **Compliance Checks**: Ensure that all security practices and controls comply with relevant laws, regulations, and industry standards.

6. Maintenance and Updates

- **Patch Management**: Establish a rigorous patch management process to ensure that all software and systems are updated with the latest security patches.
- **Technology Upgrades**: Regularly review and upgrade security technologies to address emerging threats and technological advancements.

7. Reporting and Documentation

- **Security Reporting**: Provide regular security reports to key stakeholders, detailing the current security posture, incident reports, and ongoing activities.
- **Documentation**: Maintain comprehensive documentation of all security policies, procedures, and configurations for audit trails and compliance purposes.

8. Continuous Improvement

- **Feedback Loops**: Implement feedback mechanisms to learn from security incidents and testing results.
- **Strategy Revisions**: Continuously update security strategies based on new threats, technological changes, and business needs.

Supported Cloud Services: Microsoft Azure, Amazon Web Service, Google Cloud Platform

CONTACT

Sales:
sales@amzuit.com

Support:
support@amzuit.com

Web:
https://www.amzuit.com

OFFICE

United Kingdom
Amzu Information Technology Ltd,
100, Space,
Avebury Boulevard,
Milton Keynes MK9 1FH