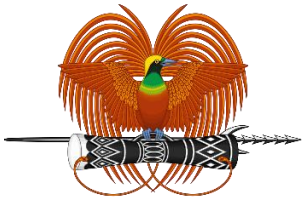


Papua New Guinea

Department of Information and Communication Technology (DICT)

Government Cloud Standards, Guidelines and Specifications 2025

Document Control:

Document Name	**PNG Government Cloud Standards, Guidelines and Specifications 2024**
Custodian	PNG Digital Government Services – Department of Information and Communications Technology
Edition	Draft 2
Approved by	National ICT Sector Coordination Committee
Date Approved	
Effective Date	
Next Review Date	

Papua New Guinea

Table of Contents

. 2

Government Cloud Standards 2024. 4

PART I. - PRELIMINARY. 4

1. NAME. 4

2. COMMENCEMENT. 4

3. AUTHORITY. 4

4. SIMPLIFIED OUTLINE. 4

5. DEFINITIONS. 4

6. OBJECTIVES OF STANDARDS AND GUIDELINES 5

7. SCOPE AND APPLICATION 5

8. E-GOVERNMENT CLOUD 6

PART II. – CLOUD STANDARDS 6

9. Overview. 6

Standard 1.3 Vendor Management 7

Standard 1.4 Data Management 7

Standard 1.5 Management and Ongoing enhancement. 7

Standard 1.6 Training and Change Management 8

Standard 1.7 Disaster Recovery and Business continuity. 8

Standard 1.8 Documentation and Reporting. 8

Standard 2.1 Data Formats and Protocols. 8

Standard 2.2 API Standards 9

Standard 2.3 Portability for Applications and Data 9

Standard 2.4 Data Migration. 9

Standard 4.1 Identity and Access Management (IAM) Standards 9

Standard 4.2 Data Encryption Standards 9

Standards 4.3 Compliance Regulations 9

Standard 4.4 Network Security and Firewall Standards 9

Standard 5.1 Resource Allocation and Monitoring Standards 10

Standard 5.2 Load Balancing and Auto-Scaling. 10

Standard 5.3 Performance Metrics and Monitoring Tools:. 10

Standard 6.1 Cloud Resource Management Standards 10
Standard 6.2 Change Management and Versioning Standards 10
Standard 6.3 Cost Management and Billing Standards: 10
Standard 7.1 Strategies to Avoid Vendor Lock-In 10
Standard 7.2 Open-Source Cloud Solutions and Standards: 11
Standard 7.3 Standardized Interfaces and APIs: 11
Standard 8.1 Cloud Service Level Agreements (SLAs) 11
Standard 8.2 Jurisdiction and Data Sovereignty Considerations: 11
Standard 8.3 Contractual and Legal Aspects of Cloud Services: 12
Standard 9.1 Data Backup and Recovery Standards: 12
Standard 9.2 Redundancy and Failover Strategies: 12
Standard 9.3 Disaster Recovery Planning in Cloud Environments: 12
Standard 10.1 Discussion of evolving technologies (edge computing, serverless, etc.): 12
Standard 10.2 Anticipating and preparing for future standards needs: 13
PART III. MISCELLANEOUS 13
14. Implementation schedule. 13
15. Compliance and monitoring. 13
16. Supplemental standards and guidelines. 13
APPENDIX. 14
APPENDICES 21
APPENDIX I: 21

Government Cloud Standards 2024.

PART I. - PRELIMINARY.

1. NAME.

This instrument is the PNG Government Cloud Standards 2024.

2. COMMENCEMENT.

This instrument commences on 1 July 2023.

3. AUTHORITY.

This instrument is made under Section 64 of the ***Digital Government Act* 2022**.

4. SIMPLIFIED OUTLINE.

(1) This instrument prescribes standards and guidelines for government cloud. All public bodies must comply with this instrument.

(2) This instrument has been developed by the Department of Information and Communication Technology.

(3) Part 1 sets out preliminary matters.

(4) Parts 2 sets out the different standards under Cloud.

(5) Part 3 contains CLoud Guidelines and best practices and Part 4 other relevant matters together with Appendix 1.

(6) Notes are included in this instrument to help understanding by drawing attention to other provisions information or explanations. The notes are in small type, so that they don't disrupt the text. They do not contain statements of law.

5. DEFINITIONS.

For the purposes of this PNG Digital Standard, the following definitions, abbreviations and symbols apply:

"Cloud computing" refers to the delivery of services, applications, and data storage over the internet through servers interconnected in a network.

"community cloud" means the cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations).

"Government Cloud" is like a specialized, ultra-secure version of popular services like Google Drive or Dropbox, but exclusively designed for government use.

“hybrid cloud” means the cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load-balancing between clouds).

“Infrastructure as a Service” or IaaS, means the capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications.

“Interoperability” typically refers to the ability to easily move workloads and data from one cloud provider to another or between private and public clouds

“Platform as a Service” or PaaS, means the capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider.

“Privacy” is the assured, proper, and consistent collection, processing, communication, use and disposition of personal information (PI) and personally-identifiable information (PII) throughout its life cycle.

“private cloud” means the cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise.

“public cloud” means the cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.

“public body” has the same meaning as the Digital Government Act 2022.

“Software as a Service” or SaaS, means the capability provided to the consumer is to use the providers applications running on a cloud infrastructure where applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email).

6. OBJECTIVES OF STANDARDS AND GUIDELINES

(1) The objectives of the cloud standards and guidelines are to encompass everything from service models and deployment strategies to security, performance, legal compliance, and forward-looking trends.

(2) By adhering to these standards, departments can ensure the reliability, interoperability, and security of their cloud environments.

7. SCOPE AND APPLICATION

(1) This standard shall provide guidelines on deployment of cloud-based computing products and services.

(2) This standard guides the Managed Cloud Applications as consumers of cloud services from vendors.

(3) This standard shall be applicable to the following
- All public bodies
- Other Stakeholders engaging with PNG Government

8. E-GOVERNMENT CLOUD

(1) The PNG Department of Information and Communications Technology (ICT) oversees the development and implementation of information technology and e-government initiatives in Papua New Guinea.

(2) By utilizing cloud computing technology, the e-Government Cloud seeks to modernize and optimize government processes, which in turns enhances service delivery, and revolutionize public administration.

PART II. – CLOUD STANDARDS

9. Overview

(1) This Part prescribes standards to support cloud computing.

(2) By adhering to these standards, public bodies may effectively manage their cloud computing environments, ensuring security, interoperability, and compliance while delivering high-quality services to their users.

Standard 1 Cloud Administrative Standards

Standard 1.1 Security

(1) Public bodies and stakeholders must standardize Identify and Access Management IAM protocols and enforce multi-factor authentication for all users. They must also regularly review, and update access privileges based on job roles and responsibilities.

(2) Public bodies must mandate the use of encryption for data both in transit and at rest.

(3) Public bodies must require regular security audits and monitoring to detect and respond to potential threats. By establishing protocols for real-time threat detection and incident response.

Standard 1.2 Compliance

(1) For regulatory alignment, public bodies in coordination with the Department of Information Communications and Technology （DICT） must ensure cloud services align with relevant government regulations and industry standards.

(2) For data classification and handling, public bodies must implement a standardized approach for classifying and handling data based on sensitivity according to the PNG Data Standards and Guidelines 2024.

(3) Public bodies must mandate regular reporting to DICT on cloud resource usage, security incidents, and compliance statutes, for reference refer to Government Cloud Policy. This includes establishing procedures for addressing and remedying compliance violations.

Standard 1.3 Vendor Management

(1) For Request of Proposal （RFP）, public bodies in coordination with DICT must develop a standardized RFP process for selecting cloud service providers. This includes criterion such as security, compliance, scalability, and cost in the evaluation process of implementation of cloud service.

(2) Public bodies must standardize Service Level Agreements （SLA） to ensure the availability, performance, and support levels meet agency requirements. This includes clearly defining penalties for SLA breaches and mechanisms for dispute resolution. If required, on behalf of the government DICT may review and negotiate SLA with CSPs.

(3) For legal and contractual considerations, public bodies must establish legal standards for reviewing contracts and agreements with CSPs. This includes ensuring contracts specify data ownerships rights, data portability, and exit strategies.

Standard 1.4 Data Management

(1) For migration planning, public bodies must consider standardizing an approach to data migration, including data classification and integrity checks. This includes developing a phased migration plan to minimize disruption.

Note: Refer to PNG Data Standards and Guidelines 2024 for data classification

(2) For integration, public bodies must implement standardized APIs and connectors for seamless integration with existing systems. This includes ensuring interoperability and data flow between on-premises and cloud environments.

(3) For backup and redundancy, public bodies must mandate regular data backups and redundancy across multiple regions or zones. This includes establishing procedures for quick data restoration in case of service disruptions.

Standard 1.5 Management and Ongoing enhancement

(1) For management framework, public bodies must consider standardizing roles and responsibilities for cloud management within a defined management framework. This includes establishing policies for resource provisioning, monitoring, and compliance.

(2) Public bodies must also consider implementing a standardized mechanism for users to provide feedback on cloud services. This includes using feedback to drive continuous improvement and optimization efforts.

(3) For performance optimization, public bodies must consider setting standards for regular reviews and optimization of cloud resources for cost-effectiveness and performance. This also requires keeping abreast of updates and new features from CSP.

Standard 1.6 Training and Change Management

(1) For employee training, public bodies must develop standardized training programs for employees or public servants on using cloud services securely. This includes communicating the benefits and changes resulting from cloud adoption.

(2) Public bodies must consider implementing standardized change management protocols to address cultural or organizational shifts. This includes fostering a positive attitude towards cloud adoption through consistent communication.

Standard 1.7 Disaster Recovery and Business continuity

(1) Public bodies must standardize the development and testing of disaster recovery plans. This includes ensuring plans encompass data recovery, system restoration, and service continuity.

(2) Public bodies must standardize backup procedures and redundancy measures to minimize downtown. This includes establishing protocols for quick restoration in case of service disruptions.

Standard 1.8 Documentation and Reporting

(1) Public bodies must ensure to set standards for maintaining detailed documentation for configurations, policies, and procedures. This includes maintaining an up-to-date inventory of cloud resources.

(2) Public bodies must also ensure to define standards for regular reporting on cloud resource usage, security incidents, and compliance status. This includes using standardized reports to identify areas for improvements.

Standard 2 Interoperability and Portability Standards

Standard 2.1 Data Formats and Protocols

(1) Public bodies must adhere to standardized data formats such as JSON and XML to ensure seamless data interchange.

(2) Industry-standard protocols must be utilized to facilitate effective communication between systems, promoting efficient data exchange.

Standard 2.2 API Standards

(1) Employ industry-standard practices for well-documented and consistent API design and documentation

(2) Consider using a query language for APIs that allows for flexible data retrieval can enhance user experience. By adopting industry-standard practices for query flexibility, developers can efficiently interact with APIs, retrieving data tailored to their specific needs.

Standard 2.3 Portability for Applications and Data

(1) Develop applications following microservices architecture to enhance portability.

(2) Encapsulate application dependencies for containerization using Docker standards.

(3) Employ container orchestration techniques to manage applications effectively. "This approach facilitates the deployment and scaling of applications across diverse environments without being specific to any tool, ensuring adaptability and consistency in different setups."

Standard 2.4 Data Migration

(1) Implement ETL processes to ensure efficient data migration, focusing on extraction, transformation, and loading tasks.

(2) Employ data synchronization tools such as Apache Kafka for real-time data migration.

4. Security and Privacy Standards

Standard 4.1 Identity and Access Management (IAM) Standards

(1) Adhere to widely accepted standards for secure user authentication and authorization, ensuring robust practices for user security and access control.

(2) Implement role-based access control (RBAC) following NIST guidelines for fine-grained access management.

Standard 4.2 Data Encryption Standards

(1) Employ recognized encryption standards, ensuring data security both at rest and during transmission, without specifying the encryption algorithm.

(2) Apply TLS/SSL protocols for secure communication between systems and services.

Standards 4.3 Compliance Regulations

(1) Adhere to GDPR standards for handling personal data and user privacy

(2) Follow HIPAA guidelines for secure handling of healthcare-related data.

Standard 4.4 Network Security and Firewall Standards

(1) Implement perimeter security using firewalls like Cisco ASA or pfSense, following best practices.

(2) Utilize intrusion detection and prevention systems (IDS/IPS) such as Snort for network security.

Standard 5 Performance and Scalability Standards

Standard 5.1 Resource Allocation and Monitoring Standards

(1) Implement dynamic resource allocation using tools like Kubernetes Horizontal Pod Autoscaling.

(2) Utilize cloud provider-native monitoring services such as Amazon CloudWatch for tracking resource utilization.

Standard 5.2 Load Balancing and Auto-Scaling

(1) Utilize load balancing techniques to distribute traffic and maintain high availability, optimizing system performance without specifying a particular load balancer.

(2) Implement auto-scaling policies based on metrics such as CPU utilization for optimal resource management.

Standard 5.3 Performance Metrics and Monitoring Tools:

(1) Track response time, latency, and throughput metrics to enhance system performance without specifying monitoring tools.

(2) Employ APM (Application Performance Monitoring) tools like New Relic to analyze application performance.

Standard 6 Cloud Governance and Management Standards

Standard 6.1 Cloud Resource Management Standards

(1) Establish a centralized cloud resource repository for managing configurations and templates to be used with tools like Terraform or AWS CloudFormation

(2) Implement tagging standards to categorize and manage resources efficiently.

Standard 6.2 Change Management and Versioning Standards

(1) Utilize version control systems like Git for managing infrastructure code changes.

(2) Implement CI/CD pipelines using tools such as Jenkins for automated deployment and versioning.

Standard 6.3 Cost Management and Billing Standards:

(1) Implement cost allocation tags for resources to track usage and allocate costs accurately.

(2) Utilize cloud provider billing and cost management tools, such as AWS Cost Explorer, to analyze spending patterns.

Standard 7 Vendor Lock-In and Openness Standards

Standard 7.1 Strategies to Avoid Vendor Lock-In

(1) Prioritize cloud-neutral solutions that adhere to widely accepted standards to ensure interoperability.

(2) Implement a multi-cloud strategy, distributing workloads across different providers to prevent dependency.

(3) Regularly assess migration readiness and plan for easy transitions between cloud vendors.

Standard 7.2 Open-Source Cloud Solutions and Standards:

(1) Embrace open-source cloud platforms like OpenStack to avoid proprietary constraints and vendor lock-in.

(2) Adopt open-source containerization tools like Kubernetes for portability across different environments.

(3) Consider open-source database solutions like MySQL to prevent reliance on proprietary database technologies.

(4) The table shows five top trusted open sources that can be utilized:

1. Open Stack
2. Kubernetes
3. Apache Cloud Stack
4. Cloud Foundry
5. Terraform

Standard 7.3 Standardized Interfaces and APIs:

(1) Adhere to RESTful API design principles to ensure consistent and standardized communication.

(2) Utilize well-established API standards like GraphQL to enable flexible and efficient data querying.

(3) Implement API versioning to maintain backward compatibility and support incremental updates.

Standard 8 Legal and Compliance Standards

Standard 8.1 Cloud Service Level Agreements (SLAs)

(1) Define SLAs that clearly state performance metrics, availability guarantees, and response times.

(2) Specify remedies and penalties for SLA breaches to ensure accountability and service quality.

(3) Regularly review and update SLAs to align with changing business needs and technology advancements.

Standard 8.2 Jurisdiction and Data Sovereignty Considerations:

(1) Adhere to data sovereignty regulations by hosting sensitive data within the country's borders.

(2) Clearly outline jurisdictional aspects in contracts to address legal concerns and ensure compliance.

(3) Establish data processing agreements that outline responsibilities for handling personal data in line with relevant regulations.

Standard 8.3 Contractual and Legal Aspects of Cloud Services:

(1) Clearly define data ownership rights and data usage terms in contracts to prevent disputes.
(2) Address liability clauses that outline responsibilities in case of data breaches or service interruptions.
(3) Include exit strategies in contracts that detail data extraction and transition processes when ending the cloud service.

Standard 9 Disaster Recovery and Business Continuity Standards

Standard 9.1 Data Backup and Recovery Standards:

(1) Implement automated data backups at regular intervals to minimize data loss in case of failures.
(2) Utilize incremental backups to reduce recovery time and bandwidth usage during restoration.
(3) Test backup restoration processes periodically to ensure data integrity and recovery efficiency.

Standard 9.2 Redundancy and Failover Strategies:

(1) Implement active-active configurations across multiple geographic regions for enhanced redundancy.
(2) Utilize load balancers with health checks to automatically route traffic to healthy instances during failures.
(3) Regularly conduct failover testing to validate the effectiveness of redundancy mechanisms and minimize downtime.

Standard 9.3 Disaster Recovery Planning in Cloud Environments:

(1) Develop comprehensive disaster recovery plans that outline roles, responsibilities, and procedures.
(2) Define recovery time objectives (RTO) and recovery point objectives (RPO) for critical applications.
(3) Conduct simulated disaster recovery drills to validate the readiness of the recovery processes and identify areas for improvement.
(4) Deployment of multi-site data centers to address data security and disaster recovery

Standard 10 Future Trends and Emerging Standards

Standard 10.1 Discussion of evolving technologies (edge computing, serverless, etc.):

(1) Explore the potential of edge computing for real-time data processing, enabling immediate decision-making in remote locations.
(2) Discuss the benefits of serverless computing in reducing operational overhead, enhancing scalability, and optimizing resource utilization.
(3) Examine the role of AI and machine learning in predictive analytics, enabling government departments to anticipate citizen needs more effectively.

Standard 10.2 Anticipating and preparing for future standards needs:

(1) Highlight the need for standards addressing the ethical considerations of AI and data privacy as technology evolves.

(2) Discuss the emerging challenges of managing decentralized data in a multi-cloud and edge computing landscape.

(3) Address the potential standardization requirements for ensuring interoperability among quantum computing resources and traditional cloud environments.

PART III. MISCELLANEOUS

14. Implementation schedule.

All public bodies must adopt the standards in Part 2 and 3 on or before [01.01. 2025].

15. Compliance and monitoring.

DICT may conduct an assessment and evaluation report of the compliance of public bodies with this instrument.

16. Supplemental standards and guidelines.

DICT may issue supplemental standards and guidelines to support this instrument.

<All appendixes will be update and align with Standards document>

APPENDIX.

Annexes 1

SUB DOMAINS

The following are the sub domains covered:

- Cloud service selection
- Cloud deployment model selection
- Service level agreements

REQUIREMENTS

Sub domain	Description	Requirements
Cloud Service selection (PaaS, SaaS, IaaS)	DICT shall select a cloud service based on an objective business case	Annex A.1
Cloud deployment model selection (public, private, hybrid, community cloud)	DICT shall select a cloud deployment model based on an objective business case	Annex A.2
Service level Agreements	DICT shall have an SLA covering cost, Liability, Information security, Inter operability and portability, availability, performance, Sustainability, Privacy, Vendor lockin, integration	Annex A.3

This section provides cloud standards needed to guide in selecting a cloud service and the model of deployment. The DICT shall develop operational manuals to institutionalize this standard.

ANNEXES 2

Subject		Requirements
1.SaaS	Business case	a. DICT shall not pursue a SaaS solution for an application if it requires specialized technical knowledge to operate and support, or requires customization that a SaaS vendor cannot offer, b. DICT shall determine what reporting services the provider offers, and whether they are compatible with the business reporting requirements. Because SaaS involves giving up direct control of some of DICT data, accurate and useful reporting is especially important. c. DICT shall consider the type and amount of data that will be transmitted to and from the application on a regular basis. Internet bandwidth pales in comparison to the gigabit Ethernet links commonly found in enterprise LANs, and data transmissions that take a few minutes to transfer between servers in the server room might take hours to transmit to and from a SaaS application located across the country. Because of this, DICT shall consider a solution that takes network latency into consideration. An appliance-based solution, for example, might cache or batch. d. DICT shall ensure the cloud service is accessible to persons with disability? e. Potential Saas include: ❖ Email ❖ office productivity suite ❖ collaboration including IP telephony ❖ customer relationship management

2. PaaS	Business case	a. DICT shall consider platform as a service - if they are carrying out collaborative software development project that involve multiple agencies - If they are deploying applications that are to be shared by multiple users simultaneously b. When evaluating and choosing a PaaS provider, DICT shall consider if the programming languages and server-side technologies offered by the provider match their needs. c. DICT shall ensure that providers meet the connectivity, storage and redundancy needs to ensure services availability.

Cloud Service Selection (PaaS, SaaS, Iaa

3. IaaS	Business case	a. DICT shall consider acquiring infrastructure as a service if they want a cloud-based data centre without requiring to install new equipment. b. DICT shall ensure that IaaS providers meet the commonly used standards for access. These include: Xtensible Markup Language (XML), Representative State Transfer (REST), Simple Object Access Protocol (SOAP), and File Transfer Protocol (FTP) c. DICT shall consider the burden to ICT staff for monitoring and managing applications in a cloud providers data centre in addition to those in the premises. This includes software patches, maintenance and upgrades. d. DICT shall ensure that providers meet the connectivity, storage and redundancy needs to ensure services availability. e. DICT shall take full advantage of pay-per-use pricing of the data centre for IaaS. f. DICT are discouraged from investment in private IaaS.

Annex : Cloud deployment model selection (public, private, hybrid, community cloud)

Subject		Requirements
1.Public Cloud	Business Case	DICT shall carry out a risk assessment based on Appendix 1 to determine the balance between cost and security of this model. This model has a variety of inherent security risks that need to be considered. It also has maximum potential cost efficiencies due to economies of scale.
2. Private Cloud	Business Case	DICT shall carry out a risk assessment based on Appendix 1 to determine the balance between cost and security of this model. This model has reduced potential cost efficiencies. However, it has reduced potential security concerns. It also enables easier contract negotiations between the provider and consumers.
3. Community Cloud	Business Case	DICT shall consider this model if they have other DICT with similar security requirements and in need of processing and storing data of similar requirements. This model attempts to obtain most of the security benefits of a private cloud, and most of the economic benefits of a public cloud.
4.Hybrid Cloud	Business case	DICT shall establish a business case for this model. It Involves a combination of cloud models. An example is using commodity resources from a public cloud such as web servers to display non- sensitive data, which interacts with sensitive data stored or processed in a private cloud.

Annex 3: Service level Agreement

Subject	Requirement
General requirements	a. The adoption of cloud services will require agencies to build new skills and capabilities into their workforce. In particular, agencies will require a high level of proficiency in procurement, contract negotiation and management, and supplier performance management to ensure value for money is realized. b. DICT shall look to first adopt cloud services for those areas where the market has already achieved an acceptable level of maturity. Mature areas typically have begun to extend their focus from delivery pure functionality to additional attributes like security, availability, performance and interoperability.
Liability	c. DICT shall ensure SLAs cover issues such as ending the arrangement, dispute resolution, early warning of bankruptcy (or similar), compensation for data loss/misuse, change of control and assignment/ novation, change of terms at the discretion of the provider.
Information security	a. DICT shall ensure that data is stored in agreed locations, and is retrievable inside agreed timeframes b. DICT shall retain control over any data or information that is placed in a cloud service and ensure it is adequately protected from loss c. DICT shall carry out a risk assessment to determine the information security viability of migrating to a cloud. The checklist in Appendix 1 shall serve as a guide. d. DICT shall ensure the provider is audited by a third party to determine their compliance with NCSC information security standards. e. privacy of any data stored f. on a cloud computing service must be maintained in accordance with statutory/regulatory obligations g. The chosen solution should not require significant firewall rule changes. For example, port 80 and port 443 should be sufficient for the solution to function (these ports are usually open already). h. DICT shall ensure data is permanently deleted from a provider's storage media when migrating i. DICT shall be aware of Kenya legislative and regulatory requirements when storing personal data (e.g. the Kenya Information Privacy laws and the Public laws). j. DICT shall ensure the location of the data is consistent with local legislation

	k. All stored and transmitted data must be encrypted l. Disaster Recovery expectations must be defined (e.g. worse case recovery commitment.

Inter-operability and portability	a. The following requirements should be carefully considered when identifying a suitable solution: • active directory integration • single sign on b. DICT shall ensure that the cloud provider supports open standards that guarantee: - - Workload migration where a workload that executes in one cloud provider can be uploaded in another cloud provider - Data migration: Data that resides in one cloud provider can be moved to another cloud provider - User authentication: User who has established an identity with a cloud provider can use the same identity with another cloud provider. - Workload management: Custom tools developed for cloud workload management can be used to manage multiple cloud resources from different vendors. c. DICT shall ensure that the cloud deployment model supports common standards on: i. application interfaces; ii. portability interfaces; iii. management interfaces; iv. file formats; and operation conventions
Availability	DICT shall ensure there is an SLA with the cloud provider for 99.99% during work days, 99.9% for nights/weekend
Performance	Service level agreements shall ensure maximum service response times

Cost	DICT shall consider the total cost of ownership (TCO) of a cloud service, compared to that of an equivalent on-premise service.
Sustainability	For DICT providing cloud services, the cost of deploying and maintaining cloud computing infrastructure is very huge and therefore there is need to be able to recover it back. DICT shall select a chargeback model that adequately fits the consumers' and Government needs i.e i. Pay - as -you- grow ii. Usage based pricing iii. Elasticity model
Privacy	DICT shall ensure the cloud providers adheres to regulatory law in relation to privacy and public record-keeping requirements. DICT shall consider any legal obligations they have towards customers or other parties, and whether cloud will allow them to continue to meet them.

Vendor lockin	a. DICT shall ensure that the cloud solution supports • quick entry • quick exit • low-cost solutions. b. DICT shall have an exit strategy in case they intend to change providers c. DICT shall not pursue a solution if: • A solution providers want months of preparation to assess agency needs or conduct training • the solution involves an extended lock-in period for the agency • the solution involves substantial financial investment • The cost of the solution should be such that if the solution fails to satisfy agency requirements, it is considered low risk to terminate the service or try another service. d. In addition, the costs should be simple and straight forward. A convoluted pricing model is uncommon for cloud services and should be carefully considered during evaluation.
Integration	DICT shall ensure that migrating to cloud will meet any functional and data-integration requirements the organization has in place.

APPENDICES

APPENDIX I: Risk assessment checklist

- ✓ Data or functionality to be moved to the cloud is not business critical
- ✓ The provider audited by a third party to determine their compliance with GoPNG information security standards?
- ✓ Reviewed the vendor's business continuity and disaster recovery plan
- ✓ Maintain an up-to-date backup copy of data
- ✓ Data or business functionality will be replicated with a second vendor
- ✓ The network connection between me and the vendor's network is adequate
- ✓ The Service Level Agreement (SLA) guarantees adequate system availability
- ✓ Scheduled outages are acceptable both in duration and time of day
- ✓ Scheduled outages affect the guaranteed percentage of system availability
- ✓ Receive adequate compensation for a breach of the SLA or contract
- ✓ Redundancy mechanisms and offsite backups prevent data corruption or loss
- ✓ If a file or other data is accidentally deleted, the vendor can quickly restore it
- ✓ Increase use of the vendor's computing resources at short notice
- ✓ Easily move data to another vendor or in-house
- ✓ Easily move standardised application to another vendor or in-house
- ✓ My choice of cloud-sharing model aligns with my risk tolerance
- ✓ My data is not too sensitive to store or process in the cloud
- ✓ Meet the legislative obligations to protect and manage my data
- ✓ Know and accept the privacy laws of countries that have access to my data
- ✓ The vendor suitably sanitises storage media storing my data at its end of life
- ✓ The vendor securely monitors the computers that store or process my data
- ✓ Use my existing tools to monitor my use of the vendor's services
- ✓ Retain legal ownership of my data
- ✓ The vendor has a secure gateway environment
- ✓ The vendor's gateway is certified by an authoritative third party
- ✓ The vendor provides a suitable email content filtering capability
- ✓ The vendor's security posture is supported by policies and processes
- ✓ The vendor's security posture is supported by direct technical controls
- ✓ Audit the vendor's security or access reputable third-party audit reports
- ✓ The vendor supports the identity and access management system that I use
- ✓ User's access and store sensitive data only via trusted operating environments

- ✓ The vendor uses endorsed physical security products and devices
- ✓ The vendor's procurement process for software and hardware is trustworthy
- ✓ The vendor adequately separates me and my data from other customers
- ✓ Using the vendor's cloud does not weaken my network security posture
- ✓ Have the option of using computers that are dedicated to my exclusive use
- ✓ When I delete my data, the storage media is sanitised before being reused
- ✓ The vendor does not know the password or key used to decrypt my data
- ✓ The vendor performs appropriate personnel vetting and employment checks
- ✓ Actions performed by the vendor's employees are logged and reviewed
- ✓ Visitors to the vendor's data centres are positively identified and escorted
- ✓ Vendor data centres have cable management practices to identify tampering
- ✓ Vendor security considerations apply equally to the vendor's subcontractors
- ✓ The vendor is contactable and provides timely responses and support
- ✓ reviewed the vendor's security incident response plan
- ✓ The vendor's employees are trained to detect and handle security incidents
- ✓ The vendor will notify me of security incidents
- ✓ The vendor will assist me with security investigations and legal discovery
- ✓ Access audit logs and other evidence to perform a forensic investigation
- ✓ Receive adequate compensation for a security breach caused by the vendor
- ✓ Storage media storing sensitive data can be adequately sanitised

Checklist for cloud service selection

	Compliance	Yes	No	Comment
	SaaS			
	Does the application require specialized technical knowledge or requires customization that a SaaS vendor cannot offer?			
	Does the application require large bandwidth on a regular basis?			
	Is the SaaS cheaper than on-premise application?			
	Does the SaaS provider adhere to regulatory law in relation to privacy and public record- keeping requirements?			
	Does the SaaS reports conform to MCA requirements?			
	PaaS			

	Is the project a collaborative software development project that involves multiple agencies?			
	Do the programming languages and server-side technologies offered by the provider match DICT needs?			
	Is it less costly to run the applications in PaaS than in-premise			
	IaaS			
	Does the DICT have enough staff capacity to manage the IaaS?			
	Does the provider meet the connectivity, storage and redundancy needs to ensure services availability?			
	Is it cheaper to acquire IaaS or in-premise hosting?			
	Does the provider meet the commonly used standards for access?			
	Does the DICT have an exit strategy from the provider and to take their existing data out of the solution and move it to another one?			
	Does the DICT capable of taking full advantage of pay-per-use pricing of the data center for IaaS			

APPENDIX III Checklist for selecting cloud deployment model

	Compliance	Yes	No	Comment
	Public Cloud			
	Has the DICT carried out a risk assessment based on Appendix 1 to determine the balance between cost and security of this model.			
	Private Cloud			
	Has the DICT carried out a risk assessment based on Appendix 1 to determine the balance between cost and security of this model?			
	Community Cloud			

	Does the GoPNG have other Agencies with similar security requirements and in need of processing and storing data of similar requirements?			
	Hybrid Cloud			
	Is there a justifiable business case for this model?			

APPENDIX III Checklist for SLA

Subject	Requirement	Yes	No	Comments
General requirements	The adoption of cloud services will require agencies to build new skills and capabilities into their workforce. In particular, agencies will require a high level of proficiency in procurement, contract negotiation and management, and supplier performance management to ensure value for money is realized.			
	DICT shall look to first adopt cloud services for those areas where the market has already achieved an acceptable level of maturity. Mature areas typically have begun to extend their focus from delivery pure functionality to additional attributes like security, availability, performance and interoperability.			

Liability	DICT shall ensure SLAs cover issues such as ending the arrangement, dispute resolution, early warning of bankruptcy (or similar), compensation for data loss/misuse, change of control and assignment/novation, change of terms at the discretion of the provider.			

Information security	DICT shall ensure that data is stored in agreed locations, and is retrievable inside agreed timeframes			
	DICT shall retain control over any data or information that is placed in a cloud service and ensure it is adequately protected from loss.			
	DICT shall carry out a risk assessment to determine the information security viability of migrating to a cloud. The checklist in Appendix 1 shall serve as a guide.			
	DICT shall ensure the provider is audited by a third party to determine their compliance with information security standards.			
	Privacy of any data stored on a cloud computing service must be maintained in accordance with statutory/regulatory obligations			
	The chosen solution should not require significant firewall rule changes. For example, port 80 and port 443 should be sufficient for the solution to function (these ports are usually open already).			
	DICT shall ensure data is permanently deleted from a provider's storage media when migrating			
	DICT shall be aware of Kenya legislative and regulatory requirements when storing personal data (e.g. the Kenya Information Privacy laws and the Public laws).			

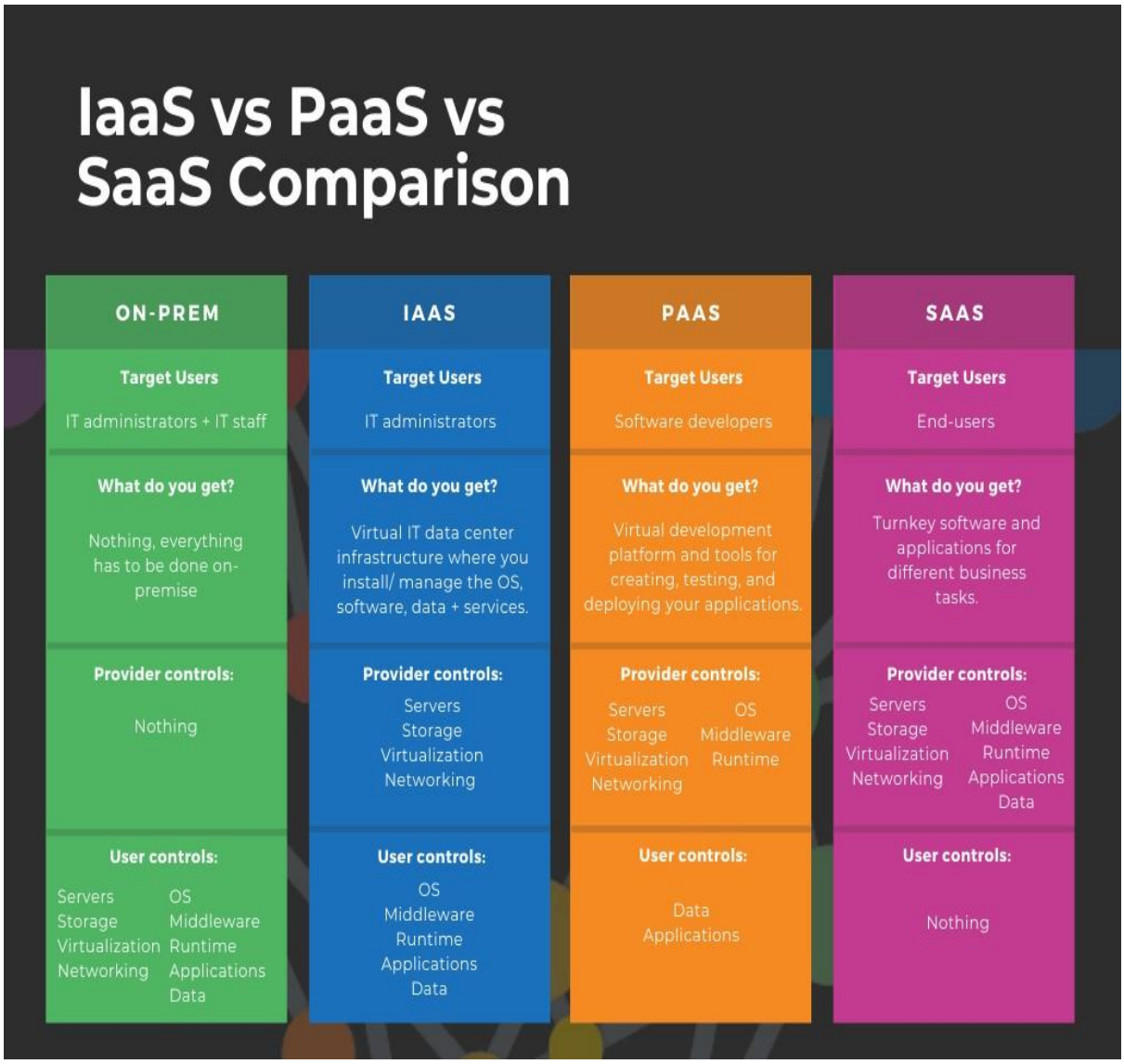
	DICT shall ensure the location of the data is consistent with local legislation			
	All stored and transmitted data must be encrypted			
	Disaster Recovery expectations must be defined (e.g. worse case recovery commitment			

Inter operability and portability	a. The following requirements should be carefully considered when identifying a suitable solution: • active directory integration • single sign on			
	b. DICT shall ensure that the cloud provider supports open standards that guarantee:- - Workload migration where a workload that executes in one cloud provider can be uploaded in another cloud provider - Data migration: Data that resides in one cloud provider can be moved to another cloud provider - User authentication: User who has established an identity with a cloud provider can use the same identity with another cloud provider. - Workload management: Custom tools developed for cloud workload management can be used to manage multiple cloud resources from different vendors.			

	c. DICT shall ensure that the cloud deployment model supports common standards on: I. application interfaces; II. portability interfaces; III. management interfaces; IV. file formats; and operation conventions			
Availability	DICT shall ensure there is an SLA with the cloud provider for 99.99% during work days, 99.9% for nights/weekend			
Performance	Service level agreements shall ensure maximum service response times			
Cost	DICT shall consider the total cost of ownership (TCO) of a cloud service, compared to that of an equivalent on-premise service.			
Sustainability	For DICT providing cloud services, the cost of deploying and maintaining cloud computing infrastructure is very huge and therefore there is need to be able to recover it back. DICT shall select a chargeback model that adequately fits the consumers' and Government needs i.e iv. Pay - as -you- grow v. Usage based pricing vi. Elasticity model			

Privacy	DICT shall ensure the cloud providers adhere to regulatory law in relation to privacy and public record-keeping requirements. DICT shall consider any legal obligations they have towards customers or other parties, and whether cloud will allow them to continue to meet them.			
Vendor lockin	DICT shall ensure that the cloud solution supports • quick entry • quick exit • low-cost solutions.			
	DICT shall have an exit strategy in case they intend to change providers			
	DICT shall not pursue a solution if: • A solution providers want months of preparation to assess agency needs or conduct training • the solution involves an extended lock-in period for the agency • the solution involves substantial financial investment • The cost of the solution should be such that if the solution fails to satisfy agency requirements, it is considered low risk to terminate the service or try another service.			

	In addition, the costs should be simple and straight forward. A convoluted pricing model is uncommon for cloud services and should be carefully considered during evaluation.			
Integration	DICT shall ensure that migrating to cloud will meet any functional and data-integration requirements the organization has in place.			



Papua New Guinea Government Cloud Standards **2024.**

ARRANGEMENT OF CLAUSES.

PART 1. - PRELIMINARY.

1. Name.
2. Commencement.
3. Authority.
4. Simplified outline.
5. Definitions.
6. Objects of standards and guidelines.
7. Scope and application.
8. E-government Cloud

PART II. – CLOUD STANDARDS

9. Overview.

PART III. – MISCELLANEOUS.

10. Implementation schedule.
11. Compliance and monitoring.
12. Supplemental standards and guidelines.

APPENDIX.