Information required about the Cloud and Edge Computing technologies deployment and cybersecurity implementation approaches, strategies, and architectures, applicable to Eskom NTCSA Operational Technology (OT) environment

List of Abbreviations:

Abbreviation	Description
API	Application Programming Interface
CAPEX	Capital Expenditure
DER	Distributed Energy Resources
DMS	Distributed Management System
DNP3	Distributed Network Protocol 3
DR	Disaster Recovery
EPU	Electricity Power Utility
EMS	Energy Management System
IAM	Identity and Access Management
ICT	Information and Communications Technology
IT	Information Technology
KPI	Key Performance Indicator
LAN	Local Area Network
MISS	Minimum Information Security Standards
POPIA	Protection of Personal Information Act
OEM	Original Equipment Manufacturer
OPEX	Operation Expenditure

OT	Operational Technology
SCADA	Supervisory Control and Data Acquisition
SLA	Service Level Agreement
SOC	Security Operations Centre
TSO	Transmission System Operator
WAN	Wide Area Network

Definition List:

Definition	Description
Agility	The ability to rapidly deploy, modify, scale, and respond in real-time to operational or system changes.
Architecture	A high-level description that explains how system components (compute, storage, networking, security, OT devices, etc) are arranged, how they interact and where they are deployed across cloud, edge, and on-prem environments.
Cloud	A technology model for delivering centralized, virtualized computing resources (compute, storage, networking and applications) over a network on demand, with elastic scalability and managed infrastructure.
Cloud-Edge	A distributed architecture that combines centralized cloud resources with decentralised edge processing, where time critical functions are executed at the edge while large-scale analytics, storage and orchestration are handled in the cloud.
Deployment	Deployment is the implementation process through which cloud or edge technologies are installed, provisioned, configured, and made operational, covering physical hardware, installation, cloud resource provisioning,

	connectivity setup, data integration and readiness of the operational environment.
Edge	A model where data processing and compute resources are deployed close to the data source (e.g substations or field devices) to enable low-latency, real-time processing and reduced reliance on centralised systems.
Flexibility	The ability of cloud/edge systems to adapt to different deployment architectures, data locations, and OT requirements.
Impact	The measurable or observable effects, positive or negative, on operations, performance, compliance, finances, strategy, resilience and societal or national interests resulting from the adoption of cloud or edge technologies.
Implementation	The coordinated process of installing, provisioning, configuring, integrating, validating, and commissioning cloud and/or edge computing capabilities so they become operational within the OT environment.
Workload	A specific application, function, or set of computing tasks that executes on on-premises, edge or cloud infrastructure and consumes compute, storage and network resources to deliver an operational function.

1. Background

Eskom NTCSA is exploring the adoption of modern Cloud and Edge (Cloud-Edge) computing technologies as part of its strategic journey toward enhancing digital capability within the Operational Technology (OT) environment. Power utilities around the world are increasingly leveraging these technologies to improve system visibility, enable analytics, support digital substations and optimise grid operations. International Transmission System Operators (TSOs) and utilities are adopting hybrid

architectures where Edge platforms support time-critical functions, while Cloud environments enable scalable analytics, long-term data storage, machine learning, and fleet-wide optimisation.

As the electricity sector evolves due to greater grid complexity, renewable integration, and increased operational data volumes, NTCSA requires a deeper understanding of the applicability, benefits, limitations, and risks associated with Cloud and Edge computing within a South African critical infrastructure context. Key considerations include technology maturity, cybersecurity implications, architecture options, data sovereignty requirements, operational integration, skills demands and indicative cost models.

To support strategic planning, NTCSA is initiating this Request for Information (RFI) to gather insights from qualified vendors, Original Equipment Manufacturers (OEMs), cloud service providers, and system integrators with relevant experience in Cloud and Edge solutions for OT environments, particularly in the Electrical Power Utility (EPU) sector.

The RFI seeks market intelligence on:

- Maturity and readiness of Cloud and Edge solutions for OT,
- Typical deployment architectures and use cases in EPUs,
- Flexibility, scalability, and operational-agility capabilities,
- Required skills and organisational competencies,
- Cybersecurity challenges and mitigation approaches,
- Data governance, residency, and sovereignty considerations,
- Investment expectations, cost models, and implementation timelines,
- Practical examples (case studies) of successful application in comparable operating environments.

The information gathered will assist NTCSA in shaping future strategies, assessing technological suitability, and identifying potential pathways for adopting Cloud and Edge capabilities in a secure, compliant and operationally viable manner.

2. NTCSA User Requirements

NTCSA requires information from the market to better understand the capabilities, constraints, and applicability of Cloud and Edge technologies within the OT environment. The responses to this RFI should enable NTCSA to make informed decisions relating to future architectures, security, cost, and operational integration.

Tenderers are therefore requested to provide detailed information addressing the following requirements:

1) Technology Capability Requirements:

a) Description of Cloud and Edge Computing Platforms offered for OT environments, including:
- Architecture overview,
- Support deployment models (on-premises, hybrid, private cloud, public cloud, edge devices),
- Real-time performance capabilities (latency, deterministic behaviour),
- High-availability and redundancy options.

b) Supported OT protocols and standards include (but are not limited to):
- IEC 61850,
- IEC 60870-5-101/104,
- DNP3, Modbus.

c) Compatibility with digital substations, process bus, and virtualised OT protection/automation.

2) Use Case Requirements:

a) Example of EPU OT-specific use cases your solution supports, including:
- Grid Monitoring and situational awareness,
- Predictive maintenance analytics,
- Asset performance management,
- Virtualised protection and automation on Digital twins,
- SCADA or historian augmentation,
- Distributed energy resource (DER) coordination.

b) Evidence of successful implementation of Cloud/Edge solutions in EPU OT environments, including performance metrics or case studies.

3) Security and Compliance Requirements:

a) Description of the cybersecurity controls built into your Cloud/Edge solution, including
- Identity and access management (IAM),
- Network Segmentation,
- Encryption (in transit, in use, and at rest),
- Zero-Trust Architecture,
- Monitoring and threat detection,
- Patch and update mechanisms.

b) Ability to comply with South Africa data-sovereignty requirements, including:
- Data residency within SA,
- Secure handling of sensitive OT data,
- Support for localised cloud zones.

c) Alignment with relevant security and compliance frameworks such as:
- ISO 27001,
- NIST SP 800-82,
- POPIA,
- MISS,
- National Policy on Data and Cloud,
- IEC 62443,
- Critical infrastructure protection practices.

4) Integration Requirements

a) Ability to integrate with existing NTCSA OT systems, including:
- SCADA/EMS/DMS platforms,
- Substation automation systems,
- Operational historian systems,
- Legacy OT devices and proprietary vendor equipment.

b) Description of APIs, middleware, gateways, or integration tools available.

5) Operation and Support Requirements

a) Description of the skills, roles and competencies required to design, deploy, operate, and maintain Cloud and Edge solutions in an EPU OT context.
b) Overview of the support model, including:
- Response times,
- On-site support availability,
- Maintenance agreements,
- Firmware/software upgrade management.

c) User training, documentation, and change-management support provided.

6) Performance and Scalability Requirements

a) Capability of the solution to scale in response to:
- Increase in OT data,
- Growth of substations, renewables or DERs,
- Large analytics workloads.

b) Description of Edge resilience, including operation during:
- WAN outages,
- Network degradation,
- Loss of cloud connectivity.

7) Cost and Commercial Requirements

a) Indication of cost models, including:
- Licensing or subscription models,
- Consumption-based pricing,
- One-time capital costs vs OPEX expectations,
- Expected cost drivers for Cloud/Edge adoption.

b) Indicative implementation timelines, phases and required prerequisites.

8) Migration Considerations Requirements

a) Cloud provider partnerships and ecosystems, including:
- Details of strategic or operational partnerships with cloud service providers,
- Scope of services supported through these partnerships,
- Roles and responsibilities between supplier, cloud provider and customer.

b) Data and system migration approach, including:
- Migration of data and workloads from legacy/on-premises systems to cloud platforms,
- Migration or portability of data and workloads between cloud platforms,
- Tooling, methodologies and automation used to support migration.

c) Business continuity and availability considerations, including:
- Measures to ensure service continuity during migration activities,
- Strategies for coexistence, rollback and recovery in case of migration failure,
- Impact of migration on availability, performance and operational resilience.

d) Risk and dependency management, including:
- Identification and management of dependencies on cloud providers and network connectivity,
- Mitigation of vendor lock-in and long-term portability considerations.

9) Maturity Requirements

a) The proposed technologies shall be proven in production environments and not limited to laboratory, prototype or pilot implementations.
b) The proposed technologies shall demonstrate industry adoption, including:
    - Multiple operational deployments,
    - Use in critical infrastructure environments,
    - Availability of reference installations.
c) The proposed technologies shall be well understood from an operational perspective, with available documentation, support and established maintenance practices.
d) The proposed technologies shall support secure deployment in OT environments and align with recognized cybersecurity practices for critical infrastructure.
e) The proposed technologies shall comply with applicable IEC, IEEE, IETF, or equivalent industry standards relevant to power utility and OT environments.
f) The proposed technologies shall be practically deployed within power utility OT environments, considering latency, availability, reliability, and operational constraints.

Yours faithfully

Name: Oscar Ngwenya

Designation: Chief Engineer Prof Engin

Signature: 

Name: Njabulo Mazibuku

Designation: Learner Intern Grad Engin

Signature: