Paris Session 2022

Cybersecurity techniques, technologies and applications for securing critical utility assets

SC D2

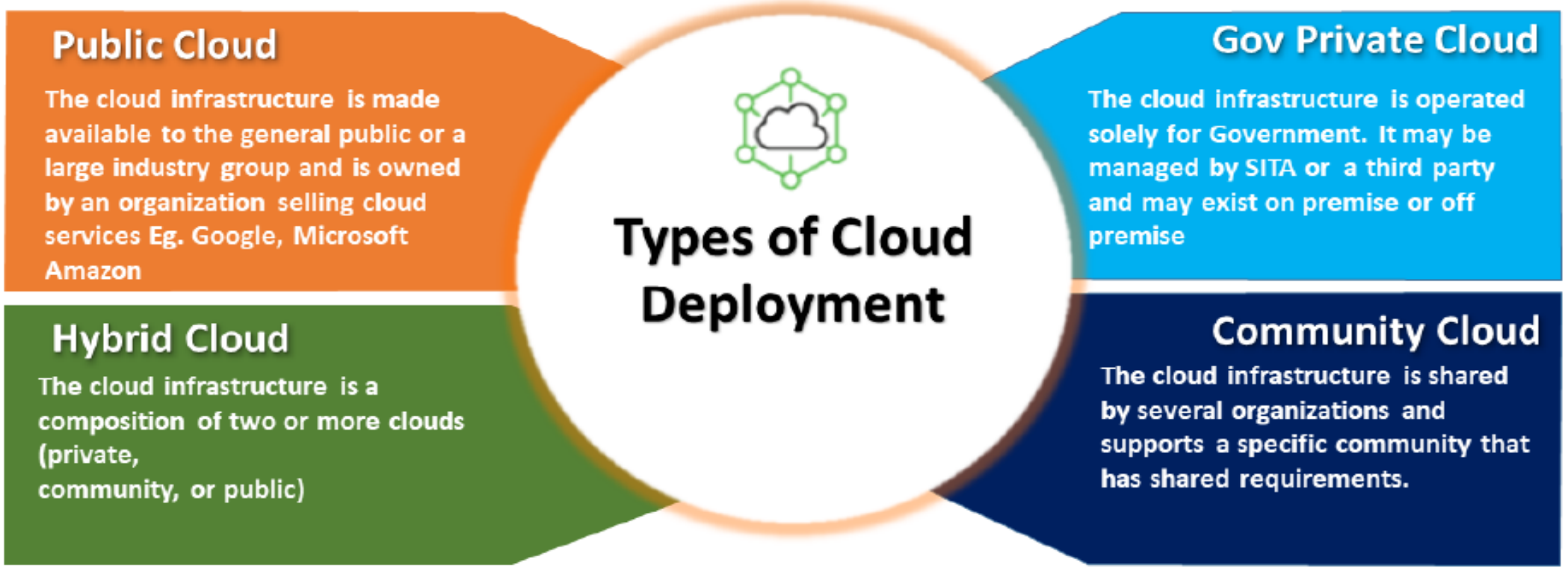
PS 2 : Q2.2 – What are the future needs of cyber security regulations, standards, protocols, or procedures for the power industry.

Sicelokuhle Oscar Ngwenya
(South Africa)
Presented by Thuthukani Nduduzo Biyela

Security in EPU OT Systems

- IEEE P1711 and OPSAID
- IEEEP171
  - SCM and MCM
  - Applied to legacy serial communications in SCADA systems
  - Secure remote engineering access to control equipment
- OPSAID
  - Encryption
  - Authentication and Access Control
  - Firewall
  - Intrusion Detection Systems (NIDS and HIDS)
  - Centralized logging

CLOUD Deployment Models from NIST



Cloud Services Deployments in EPUs

- The DPSA has specified that before acquiring and implementing cloud services the following, amongst other measures, must be in place:
  - The Head of Department (HOD) must ensure that all data is classified according to the classification system prescribed in the MISS.
  - The HOD must, as far as practically possible, avoid moving data classified as “Secret” or “Top Secret” to the Public, Hybrid or Community Clouds, in accordance to the definitions in Figure 1.
  - The HOD must ensure that data always resides within the borders of RSA. Where such is not practically possible, the HOD must ensure that provision of Section 72 of the POPIA are complied with.
  - The HOD must ensure that a comprehensive risk assessment is undertaken for each cloud service that the department intends to utilise.
  - The HOD must ensure that a Cloud Readiness Assessment is conducted before the decision is made to move to cloud-based computing services.