# VENDOR LOCK-IN & CLOUD SECURITY

DISCUSSION SUMMARY

BASED ON OPARA-MARTINS ET AL. (2014) & MORROW ET AL. (2021)

# VENDOR LOCK-IN: ISSUES

- • Proprietary APIs and data formats
- • Data and VM format incompatibility
- • Dependence on managed services
- • Migration cost and complexity
- • Lack of standardization
- • Limited awareness of lock-in risks

# MITIGATING VENDOR LOCK-IN

- • Use open standards & formats
- • Design cloud-agnostic architectures
- • Modular / loosely-coupled systems
- • Avoid deep reliance on proprietary services
- • Multi-cloud or hybrid strategies
- • Strong exit clauses in contracts
- • Governance & awareness programs

# MODERN CLOUD SECURITY CONCERNS

- • Reduced visibility & control
- • API/management interface compromise
- • Multi-tenancy & isolation risks
- • Misconfigurations & data exposure
- • Insider threats
- • Data loss & incomplete deletion
- • Shared responsibility confusion
- • Supply chain vulnerabilities

# MITIGATING CLOUD SECURITY RISKS

- • Strong IAM & MFA
- • Encrypt data at rest and in transit
- • Logging, monitoring, SIEM tools
- • Backup, redundancy, disaster recovery
- • Network segmentation, zero trust
- • Secure APIs & patch management
- • Governance, training & awareness
- • Contractual SLAs & due diligence