**Question 1: What are the main vendor lock-in issues the authors identify and how would you mitigate them?**

According to the paper, providers create lock-in through "proprietary or non-standard APIs and data storage methods" (p. 93). The authors specifically identify how cloud software vendors lock in customers: "by designing a system incompatible with software developed by other vendors; by using proprietary standards or closed architectures that lack interoperability with other applications; by licensing the software under exclusive conditions" (p. 92).

Integration presents another major challenge, with the authors noting that "companies have abandoned the use of roughly one departmental cloud application a year due to integration problems" (p. 95). They emphasize that "the cost and complexity of developing and maintaining integrations between heterogeneous platforms with disparate interfaces and protocols can quickly erase the economic and efficiency gains the cloud delivers" (p. 95).

To mitigate these issues, the paper recommends ensuring data portability, which they define as "the ability to migrate a cloud-deployed asset to a different provider" (p. 94). The authors stress that "portability should therefore be a key criterion of any organizations strategy to move into cloud services, allowing for a viable exit strategy to be developed" (p. 94). They specifically recommend that "cloud service should at least provide tools to ensure the consumer can extract, access and interchange data if such a need arises" (p. 95).

**Question 2: What are the security concerns with the modern cloud and how can these be mitigated?**

The paper identifies that "data maintained in a cloud environment may contain personal, private or confidential information such as intellectual property (IP) etc. that requires proper safeguards to prevent disclosure, compromise or misuse" (p. 96). A key security challenge emerges from data jurisdiction, as "an enterprise or SME organization using cloud based IT services is likely to have processing performed in, and data moved between, different jurisdictions" (p. 96).

The authors note that "existing laws and governance are insufficient to keep pace with cloud computing service development" (p. 96). This creates significant legal exposure, as they explain that "many jurisdictions will have specific requirements and regulations regarding the location of data" (p. 96).

For mitigation, the authors recommend that "policies need to be crafted around data interoperability related issues to ensure that data interchanged between cloud services is un-hindered" (p. 96). They emphasize that providers must "put mechanisms in place to ensure that whatever enterprise data they put in the cloud service can be easily and securely taken out" (p. 96). The paper also calls for "lawmakers to come up with useful multi-jurisdictional regulations that will help in determining the applicable legislation in cases where data is located in different jurisdictions" (p. 96).

**References**

Opara-Martins, J., Sahandi, R., & Tian, F. (2014). Critical Review of Vendor Lock-in and Its Impact on Adoption of Cloud Computing. International Conference on Information Society (i-Society 2014), 92-97. IEEE.