Challenge #	Describe the challenge with assumptions	Proposed Solution(s)
1	[A] Lacking in server-less development know-how and resources to convert the existing application sw. [B] Potential concern of application cold-start issue for the application payment process.	[A] Consider the insourcing of the serverless development resources to augment the existing application development resources. [B] Do not design for the payment process to be on serverless technology but just leveraging upon e-payments SaaS.
2	[A] Difficulty in re-migrating from X to Y due to proprietary technologies and services. [B] Increased switching costs of re-migrating, new/re-integrations including that of data transfers, potentially re-architecting of applications, and staffs re-training. [C] Dependency on the Cloud vendor roadmap and alignment to organization's evolving needs and priorities over time.	[A] Consider a hybrid or multi-cloud strategy which means the existing applications may need to be redesigned and refactored to support such a strategy. For example adopting a scalable and flexible, microservices architecture. Detailed evaluation will require to be made to assess which parts of the existing applications may be on-premise/private or public or which may be on Cloud X or Cloud Y. To adopt and adapt to cloud computing standard design patterns and best-practice migration strategies, eg. AWS Well-Architected Framework, that allows for incremental part-by-part implementation instead of a "big-bang" approach. [B,C] And to handle the cost of this addressing vendor lock-in challenge, may require additional investment (vis-a-vis the other benefits) but this can be capped by a capex/opex mix, and also spread over time rather than incurring a high upfront cost.
3	[A] Change management cost of redefining and converting the security policies from on-premise to the cloud migration. [B]	[A] Conduct a comprehensive IT security policy and SOP assessment with a gap analysis of the as-is and to-be to produce an incremental

	Additional IT op risk governance of the new cloud deployment process, with additional complexity depending on whether CI/CD may be required or not to meet not just the current but also future business needs. [C] Added cost of compliance with data sovereignty and data privacy protection laws that be differ country-to-country for a regional/global organization.	change management roadmap for implementation. [B] Adopt industry-standard, cloud deployment process and adapt it to best-fit the organization current-to-future needs. [C] Factor into this change management roadmap the organization’s legal compliance requirements of cross-border data laws, and ensuring that the infrastructure foundation design is flexible enough to cater for future extensions and changes.