Part 3

Country selection
When selecting a hosting country, it is essential to assess how well the country's legal and security frameworks align with international standards and existing frameworks in other countries, including New Zealand. International standards create a baseline for data security and privacy practices, ensuring that sensitive customer information is consistently protected, regardless of whether the data is processed or stored. The alignment between local frameworks, the Philippines, and global standards ensures that:

1. Best practices are followed to mitigate risks like data breaches of cyber-attacks,
2. The chosen cloud provider meets international obligations required by New Zealand, as well as other international countries, where it can provide safe cross-border data transfers and
3. Such alignment reduces operational risks and ensures business continuity without compromising data integrity.

Compliance
Compliance with New Zealand's Privacy Act 2020[1] ensures that personal data of New Zealand residents is managed according to strict privacy requirements. Data sovereignty and privacy obligations mean that offshore data storage (like in the Philippines) must meet the same standards as in New Zealand, ensuring sensitive data remains protected. The goal is to maintain data integrity and availability by ensuring the chosen cloud provider supports both local regulations and global frameworks, such as ISO standards[2] and GDPR[3] principles.

GDPR
The General Data Protection Regulation (GDPR) has been implemented in services across the Philippines for data privacy. This benefitted most organizations in the Philippines, as it enhanced their transactions and dealing with European Union businesses [4] because of the data privacy and transparency measures that are in place. GDPR has been pushing countries including the Philippines to improve their respective data privacy regulations, making it a widely-used security regulation across the globe[4]. GDPR is regarded as the most significant change in data-privacy regulation in 20 years[4], which has been changing the way businesses perform data-privacy worldwide. The regulation draws transparency from organizations that process personal information as well as granting consumers more control over their data.

GDPR does not apply inside New Zealand but may be of interest if you are sending information outside New Zealand[5]. While GDPR imposes additional obligations on agencies, and provides additional privacy rights to EU residents, agencies in New Zealand are likely to comply with most of its obligations under the GDPR if it complies with the New Zealand Privacy Act [6]. This ensures that

organizations handling data both domestically and internationally can maintain consistent privacy standards, enhancing trust and security.

When selecting a cloud provider in the Philippines, ensuring that they align with GDPR principles demonstrates their commitment to international best practices in data privacy and security. Even though GDPR does not directly apply to New Zealand businesses, GDPR-aligned providers offer reassurance that the data will be protected according to high international standards. The Philippines adoption and compliance of GDPR principles in their DPA highlights the growing global recognition of data privacy standards[7], making GDPR compliance an important factor when choosing a hosting country. This alignment helps maintain data integrity and supports safe cross-border data transfers, critical for organizations that need to store or process New Zealand data abroad.

ISO/IEC

As data has gained more importance in business, security of information has become even more crucial. The ISO/IEC frameworks provide structured and internationally recognized guidelines for cloud providers to manage security risks, protect sensitive information, and comply with legal obligations[8]. Implementing these standards ensures that cloud services align with global best practices, offering a competitive edge by safeguarding confidentiality, integrity, and availability of data[8].

ISO/IEC 27001: Information Security Management: Focuses on establishing, implementing, and continuously improving an information security management system (ISMS)[9]. It ensures that data confidentiality, integrity, and availability are maintained through robust security policies, processes, and controls. 27001 reduces risks of data breaches and financial losses, provides assurance to clients and business partners regarding data security and meets regulatory and contractual requirements for managing sensitive data. Cloud providers compliant with ISO 27001 demonstrate that they have structured processes in place to secure information, minimizing security risks and offering reliable service to customers[9].

ISO/IEC 27017: Security Controls for Cloud Services: 27017 builds on ISO 27001 by providing cloud-specific security controls[10]. It offers additional guidance to cloud service providers and customers on mitigating risks unique to cloud environments, such as multi-tenancy and remote access. 27017 enhances data security controls that consist in cloud infrastructure, provide guidance on shared responsibility between cloud providers and customers and protection against unauthorized access and data leakage in cloud settings[10].

ISO/IEC 27018: Protection of Personally Identifiable Information in the Cloud
ISO 27018 focuses on ensuring privacy and security of personally identifiable information (PII) processed in cloud environments[10]. Compliance with this standard shows that the cloud provider has implemented measures to protect personal data in accordance with privacy regulations and frameworks. 27018

strengthens customer trust by ensuring data privacy, demonstrates the provider's ability to handle personal data securely and helps providers align with privacy regulations such as GPR, New Zealand's Privacy Act and Philippines Privacy Act[10].

ISO/IEC 27701: Privacy Information Management System (PIMS)
27701 builds upon ISO/IEC 27001 and 27018 to address privacy management and regulatory compliance [11]. This framework provides privacy-related controls to help organizations manage personal data risks and ensure compliance with privacy laws like New Zealand Privacy Act and Philippines Privacy Act. 27701 establishes a structured approach to managing privacy risks, supports compliance with privacy regulations[11] through defined outputs and provides a systematic way to demonstrate accountability for personal data protection.

These standards ensure that cloud providers manage information security and privacy risks effectively. Selecting a cloud provider that is compliant with these ISO standards, provides trust to organizations that their sensitive data is being handled in accordance with global best practices.

SOC
The SOC certification provides internationally recognized auditing guidelines that assess the controls, processes, and systems of service organizations, including cloud providers. These reports offer assurance to clients, vendors, and regulations that a provider operates securely and in compliance with relevant standards. The primary SOC certification that relates to security and privacy controls is SOC 2.

SOC 2 focuses on controls related to security, availability, processing integrity, confidentiality and privacy of data[12]. It is particularly relevant to technology service providers and SaaS companies that handle or store customer data[12]. In terms of security, it ensures protection against unauthorized access. In terms of availability[13], it verifies that systems are reliable and accessible when needed. In terms of integrity, it confirms that data is processed accurately and as intended. In terms of confidentiality and privacy, it ensures sensitive information is kept private and protected[13]. Choosing a cloud provider that is SOC 2 compliant, demonstrates trustworthiness of the service to customers, vendors and stakeholders, provides assurance that data is handled securely throughout the service lifecycle and supports regulatory compliance by ensuring cloud services maintain high levels of data integrity and security.

CSA STAR
Another important international certification is CSA STAR; Security, Trust, Assurance, and Risk[14]. It is designed specifically for cloud service providers (CSPs). The certification builds on ISO/IEC 27001[15] but focuses on cloud-specific risks. It ensure that cloud providers maintain transparent, reliable, and secure practices through two levels; Level 1 (which involves self-assessment by

the provider, giving insight into their cloud security policies[15]) and Level 2 (which is a third-party audit that verifies whether the provider meets both ISO standards and cloud-specific security controls from the Cloud Controls Matrix (CCM)[15]). By selecting cloud providers certified with CSA STAR, organizations can trust that their data is securely managed in compliance with global security standards, reducing risks associated with cloud storage. This framework ensures alignment with New Zealand's privacy requirements and reinforces confidence in cross-border data management.