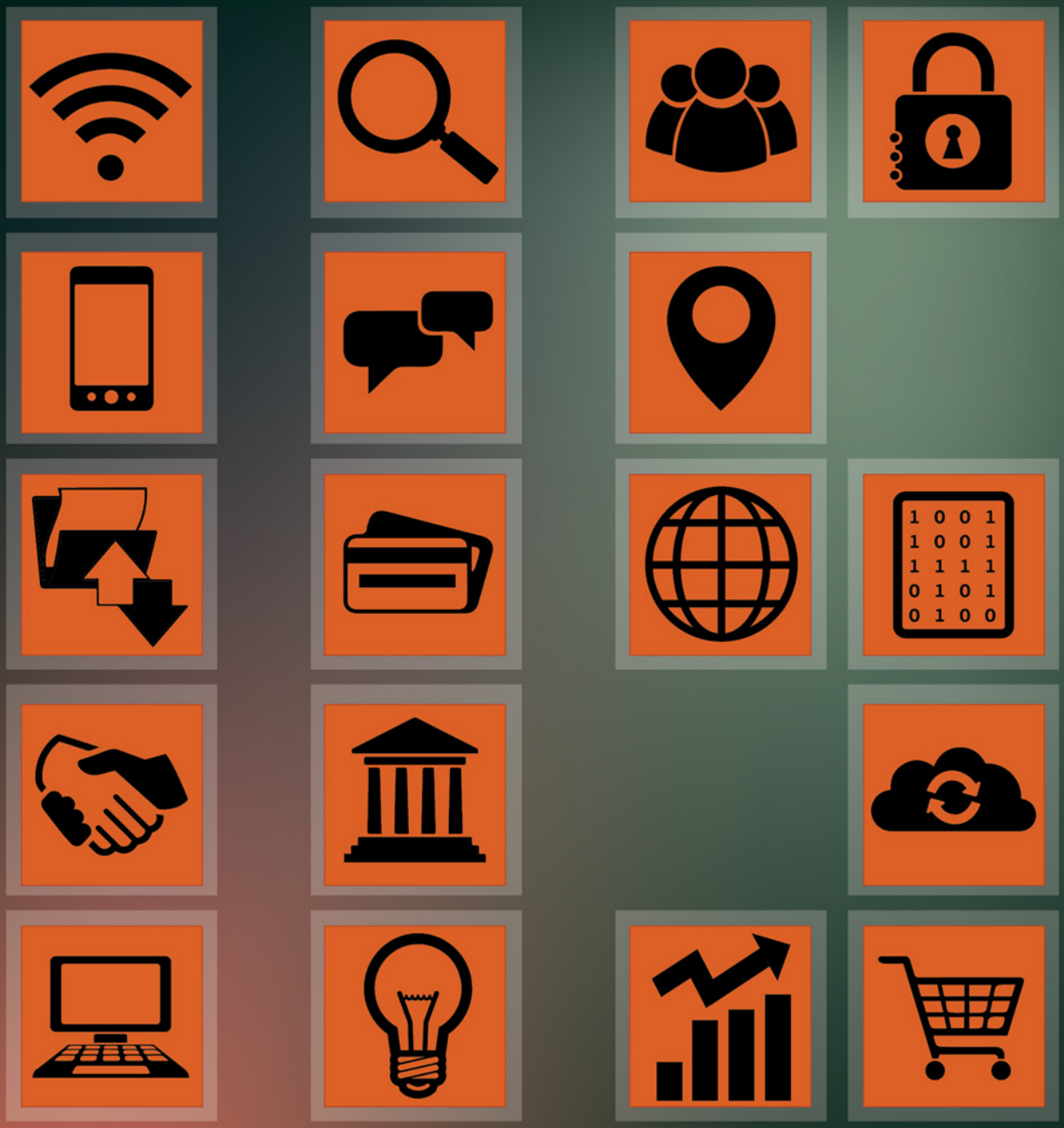

Safeguarding Privacy in the Cloud: Procurement Guide

May 2015

INFORMATION INTEGRITY SOLUTIONS

managing the **privacy** of **individuals** is **complex** and we can help you get it **right**

Acknowledgement

Information Integrity Solutions Pty Ltd (IIS) independently developed this Guide. IIS acknowledges Microsoft as a sponsor of the Guide.

Table of Contents

1. Purpose

This document aims to provide guidance for both public and private organisations on:

- How they should think about privacy in relation to the cloud
- How they should plan and take steps to safeguard privacy at all stages of the engagement with a cloud service provider.

The main body provides an overview and rationale of the guidance, while the appendix condenses the guidance into a step-by-step reference tool.

The intended audience for this document are procurement staff seeking to adopt a potential cloud solution, and more generally those who are responsible for privacy within their organisation.

2. Introduction

Over the past several years, cloud computing has transitioned from an industry buzzword to a mainstream business undertaking. The benefits of cloud computing have been well-documented. The market has expanded significantly as organisations of all sizes and from every sector have adopted cloud services to enhance or transform their operations.

Despite its many upsides, there are real issues associated with moving information to the cloud. Such issues can be conceptualised under the traditional rubric of 'information security':

- Confidentiality – Ensuring that information cannot be accessed by unauthorised parties
- Integrity – Ensuring that information is properly maintained, such as its accuracy and consistency
- Availability – Ensuring that information is protected from service interruptions and failures.

Additional issues arise when *personal* information[1] is stored or processed in the cloud – for example, the use of personal information for unrelated purposes. Thus, while aspects of privacy overlap with the three domains of information security, it is worth considering as a separate topic.

Trust, but verify

Cloud computing has different impacts on privacy risks compared to handling personal information within the organisation, potentially raising some and mitigating others. Furthermore, the timing and method for considering privacy issues may also differ. Because cloud service providers (CSPs) tend

[1] While definitions differ, generally 'personal information' means information relating to a person who is or can be reasonably identified. Organisations should consult the relevant laws and standards that apply to them.

to use standardised architecture and contractual provisions, due diligence on privacy and other matters must occur at the very beginning of the potential engagement.

In addition to implementing their own safeguards, organisations must rely on a set of claims made by the CSP with respect to safeguarding privacy in the cloud. Therefore it is important to carefully verify such claims before *and* during engagement, including adherence to relevant standards, compliance regimes and certification schemes. This document will help organisations think through:

- Utility – Do the claims meet its requirements and needs?
- Credibility – What is the evidence that supports the claims' legitimacy?
- Effectiveness – Is the CSP actually doing what it is claiming to do?

3. Privacy in the Cloud

Privacy matters

For the purposes of this document – and in line with privacy principles that exist in many legal regimes today – privacy is defined as the proper collection, use, disclosure, protection and disposal of personal information by organisations. Ultimately, the goals are to protect people from harm and to grant them appropriate control over information about them.

Privacy is an increasingly salient concern for organisations for a variety of reasons, including:

- The rapid adoption of technologies that facilitate, and business models that rely on, the collection, disclosure and use of personal information as a core organisational asset
- The significant consequences – for example, financial, reputational, regulatory – to organisations when personal information is misused, lost or stolen
- The increasing proliferation around the world of privacy and data protection laws (and their accompanying compliance obligations).

Thinking about privacy

What stays the same

At the outset it is important to emphasise that in practice, organisations remain accountable for the personal information they decide to place in the cloud. That is, they are responsible for ensuring its proper protection and are answerable when something goes wrong. In some jurisdictions, this is laid down in the law. However, even in the absence of legal compulsion, being accountable is in the organisation's interests – its customers and the wider public will not look kindly upon the shifting or disclaiming of responsibility, especially when their privacy has been breached.

While accountability cannot be outsourced, the level of responsibility an organisation has to implement privacy safeguards may vary depending on the cloud delivery model that is required.

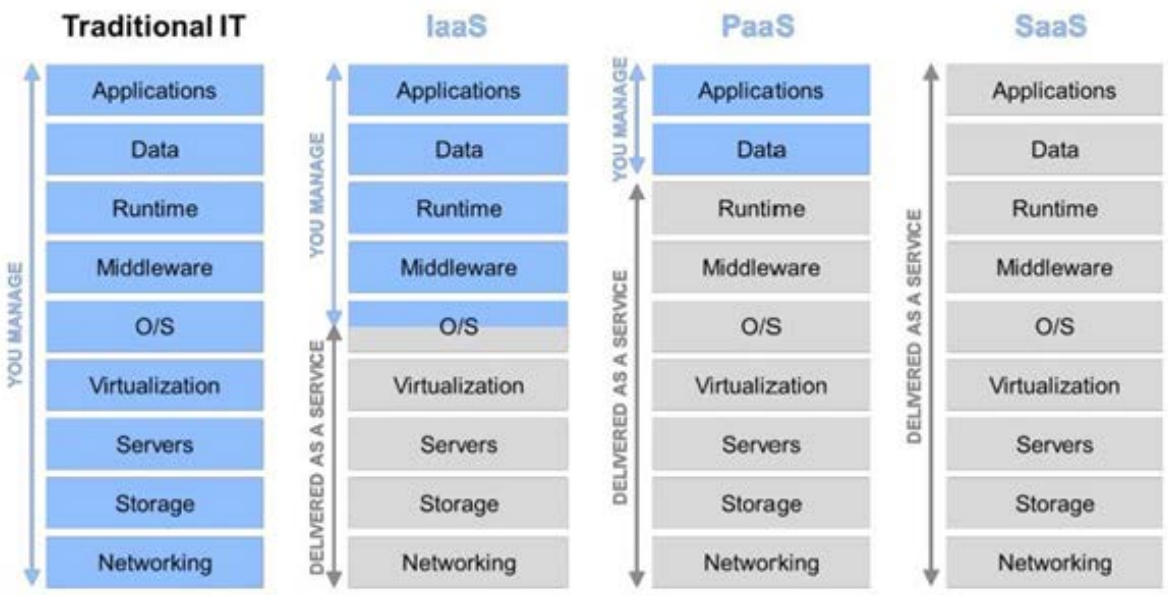

Figure 1: Cloud delivery models compared to an organisation's traditional IT arrangement. Source: Microsoft

Infrastructure-as-a-Service (IaaS)

The CSP provides the hardware and resources for the organisation to build its own solution. The organisation should assume full responsibility for implementing privacy safeguards with respect to the design, operation and governance of the solution.

Platform-as-a-Service (PaaS)

The CSP provides a development environment in addition to the cloud infrastructure. While the CSP may manage the identity and authentication elements of the solution, it is up to the organisation to develop and manage its own applications and data. The primary responsibility for safeguarding privacy remains with the organisation.

Software-as-a-Service (SaaS)

The CSP provides pre-built software that is hosted on a remote server and accessed over the Internet. Typically there is little or no customisation. With SaaS the organisation has much less scope to implement its own privacy safeguards – it is limited to assessing the suitability of the CSP and restricting the type and quantity of personal information that goes to the cloud.

What's different

Privacy in the cloud differs in certain respects to both within-organisation and traditional IT outsourcing arrangements. These differences manifest in both benefits and risks to the organisation.

Outsider control

Fundamentally, cloud computing involves an organisation providing information to someone else for a particular purpose(s). A key privacy consideration is the degree of discretion the CSP is afforded by the cloud customer in managing and using its personal information.

Sometimes the discretion can and should be minimised, if the CSP is providing a basic computing platform or storage service. At other times, the CSP requires some discretion in order to provide the necessary service. In all cases, the appropriate boundaries of that discretion should be clearly defined by contract and backed up by appropriate technical controls.

Security

Security is a necessary component of privacy, to the extent that personal information must be protected from unauthorised access, theft and loss. There are competing considerations with respect to security in the cloud.

On the one hand, CSPs are incentivised to invest in strong backup and security measures. Storing personal information with them may in fact be safer than storing it on-premises.

On the other hand, there is less scope for expressly accommodating an organisation's specific security requirements. While a service provider in a traditional outsourcing arrangement may agree to follow a customer's security policy, it is difficult or impossible for CSPs to do so, since multiple customers may share a standardised infrastructure.

Cross-border

Cloud computing often entails information travelling between the organisation and data servers in a different country, and possibly a different continent. There are two key privacy implications when personal information travels offshore, one jurisdiction independent and one jurisdiction dependent:

- **Ensuring personal information is appropriately protected (jurisdiction independent)**

  Organisations should ensure that the CSP apply at least the equivalent level of privacy protection, in terms of both its existing legal requirements and best practice, regardless of where the personal information is sent.

- **Third party access to personal information (jurisdiction dependent)**

  Increasingly in the mind of organisations is the potential for access to personal information held offshore by foreign parties for investigatory or surveillance purposes. Organisations should include possible data destinations as part of their risk analysis.

4. Safeguarding Privacy

Given that organisations remain accountable for personal information they place in the cloud, it is important to consider how privacy will be safeguarded through steps taken by both the CSP and the organisation itself. Chronologically speaking, there are three stages in which privacy should be considered when engaging a CSP:

1. Before engagement
2. During engagement
3. After engagement.

This document is designed to help organisations achieve both privacy compliance (if that is sufficient for their goals) as well as privacy best practice (if they wish to aspire to a higher standard).

Before engagement

The critical period for an organisation to consider how to safeguard privacy in the cloud is at the very beginning, *before* it enters into an arrangement with the CSP. In addition to assessing the resilience, adaptability and overall suitability of the cloud solution, the organisation needs to assure itself that its privacy needs will be met from a compliance and risk perspective.

To help organisations with assuring privacy, this document adapts and applies to the privacy domain the Security Assurance Framework for Evaluation (SAFE)[2] – a structured, lightweight methodology for assessing compliance and risk in the cloud.

SAFE sets out a five-step process, which is expanded upon below:

1. Understand strategic intent
2. Define requirements
3. Verify claims
4. Assess risks
5. Decide and plan.

[2] Microsoft, *Assuring the Security of Cloud Services* (March 2014), available at: <http://www.microsoft.com/enterprise/en-au/it-trends/cloud-computing/articles/is-the-cloud-safe-and-secure-for-your-organisation.aspx>. The following discussion refers to and expands on the handbook's treatment of privacy.

1. Understand strategic intent

Strategic intent and benefits case

The evaluation begins with consideration of the problem to be solved or opportunity to be harnessed. For example, a government agency may wish to modernise its service delivery over the cloud to mobile devices, or an enterprise may see cloud infrastructure as a way to reduce costs and gain flexibility.

From this, the organisation should develop a clear and succinct statement of strategic intent, and an agreed-upon set of expected benefits. This is important since decisions about risk, level of compliance and privacy controls are necessarily made in the context of how they relate to the strategic intent and realisation of benefits.

Context

Understanding the organisation's context is crucial to specifying privacy requirements and all aspects of risk management.

From a privacy and best practice perspective, the external context includes not only regulatory requirements, but also community and customer expectations around the use, disclosure and protection of personal information. In many cases, privacy failures result from initiatives that are unexpected or perceived to be 'creepy', even though the project technically abides by privacy law. Given the added complexities of cloud computing, community and customer expectations should be carefully considered and managed.

Internal context includes consideration of the organisation's objectives, ongoing programs, culture and attitude towards risk, constraints, existing privacy practices and perceived vulnerabilities. A key aspect of internal context is the organisation's data holdings.

Internal context – inventory of data holdings

Personal information that may be stored or processed in the cloud should be identified and classified. This will help in defining requirements and determining what controls to put in place.

In particular, the organisation should flag information that may be more sensitive from an operational or legal perspective – for example, employee records, health and financial information.

For the purpose of this exercise, data holdings should not be considered as separate silos but rather as a whole, in light of how various datasets may become connected via the cloud or stored together in the cloud (including with third party datasets). This is important because certain datasets that do not contain personal information may fall within the regulatory scope of data privacy laws when it becomes linked with other datasets that do contain personal information. Furthermore, the linking of datasets may introduce or exacerbate privacy risks that will need to be addressed as part of the privacy assurance process.

2. Define requirements

The survey of the organisation's internal and external context leads to enumeration of the specific privacy compliance obligations of the organisation. These obligations can arise from:

- External legislation – for example, privacy and data protection law; consideration of data holdings is relevant here, including their level of sensitivity and potential for linkage with other datasets
- Government policies – for example, guide to adopting cloud services for the public sector
- Industry codes and standards – for example, Payment Card Industry Data Security Standard (PCI DSS)
- Contracts – for example, outsourcing restrictions with existing business partners.

As highlighted above, while the nature of the cloud delivery model (as well as specific contractual provisions) may affect the allocation of responsibility, generally speaking the organisation is accountable for meeting its compliance requirements.

SAFE proposes a streamlined approach to identifying and documenting compliance requirements, by answering the following questions:

1. **What are the source and specifics of the compliance requirement?**

   Focus should be on the actual external source, rather than the current practice or policy within the organisation.

2. **How does the organisation currently satisfy the compliance requirement?**

   Understanding how requirements are currently satisfied can guide the organisation in defining appropriate requirements for the new solution or identify gaps in current practice.

3. **Who is the appropriate authority for compliance?**

   Typically there is a person accountable for privacy within the organisation, such as the Chief Privacy Officer or Head of Legal/Compliance.

4. **How is the compliance requirement verified?**

   This could be, for example, an annual review to confirm that the requirement has been implemented and is working as planned.

3. Verify claims

Once the organisation understands its privacy requirements, the next step is to ascertain whether the CSP can meet (or even exceed) them. This involves verifying the claims of the CSP. The assurance process involves mapping the organisation's privacy requirements to the claims made by the CSP. Ideally there will be a one-to-one relationship. Often the mapping is incomplete or even absent. In such cases, the organisation may still wish to proceed with the engagement, treating them as risks to be managed.

Additionally, some claims may exceed the organisation's strict requirements and thus engender further confidence by representing best practice. However, other claims (or lack thereof) may be unsuitable for the organisation, leading to termination of the potential engagement.

The CSP's claims can be found in three primary places:

- Its internal documentation
- External standards to which it adheres
- Contractual terms and conditions.

The verification of claims before engagement of the CSP should feed into a process of ongoing verification during engagement. This can be confirmed, for example, in the contract.

Internal documentation

Where possible, the organisation should request documentation from the CSP to help assess whether its privacy requirements can be met. These include, for example:

- Technical descriptions
- Security and privacy control frameworks
- Policies and procedures relating to privacy practice such as access controls, employee training and discipline, auditing, access and correction procedures, etc.

If the organisation's requirements are particularly high – and subject to the cooperation of the CSP – it may seek a precontractual audit of the documented measures, or at least the outcome of past audits (both internal and external).

External standards

As the cloud computing market matures, external standards are playing an increasingly important role in setting clear benchmarks for cloud customers to seek assurance and for CSPs to deliver against. They come from a variety of sources, including government, industry groups and international standards bodies. A CSP may adopt certain standards because they are prerequisites to operating within particular industries. It may adopt other standards voluntarily to build trust and increase its appeal with prospective customers.

Most standards address security practices that, while relevant to privacy, do not address the full spectrum of potential requirements. The publication of ISO/IEC 27018 has changed the landscape – it

is the first international standard that addresses the protection of personal information in the public cloud.[3]

When assessing a CSP's assurance claims in relation to standards, the organisation should consider:

- Scope – The scope of the claim may be limited to certain facilities, locations, functions, business units or other criteria
- Type – Some claims relate only to the management of security; others have only a financial or operational focus
- Authority – Adherence to standards can be verified through self-audit or by an independent party; generally, the latter provides a higher level of assurance
- Validity – Some verifications are only valid for a defined period of time or for a particular configuration.

Contractual terms and conditions

The standard contracts commonly used by CSPs can be a source of both assurance and peril for prospective customers. In the current market, negotiations are highly unlikely. It is therefore incumbent on organisations to review the terms carefully and determine their suitability before committing to the contract. The following are terms that organisations should especially watch out for:

- Restrictions on CSP's use and disclosure of personal information – for example, for marketing or other internal purposes (including access by support staff)
- Disclosure of personal information upon court order or law enforcement request – including whether the organisation can be notified or have the request passed on to it
- Security requirements and incident response – including data breach notification
- Location of data centres – for example, ability to specify preferred location(s)
- Use of subcontractors – including whether the organisation can have a say in the CSP's future engagements
- Exclusion of liability for outages and data loss – this is particularly problematic, and may call for termination of the engagement
- Unilateral variation of terms – this is another problematic provision; if possible, the organisation should negotiate for its written approval, or at least prior notification whereupon it can terminate if it deems the change(s) to be unacceptable
- Ongoing audit rights – and/or tools to increase transparency such as providing the organisation with real-time monitoring of accesses to its data
- Post-termination procedures – including data retention, deletion and portability.

[3] See Appendix II for a primer on ISO/IEC 27018.

4. Assess risk

Inevitably, gaps exist between the organisation's requirements and the CSP's assurance claims. Furthermore, analysis of the organisation's customer expectations as part of the external context as well as the cloud arrangement itself may raise privacy risks that go beyond strict compliance issues. It is therefore highly advisable for the organisation to conduct a risk assessment before engaging a CSP. In some jurisdictions and sectors, this may even be a requirement.

The Privacy Impact Assessment (PIA) is widely acknowledged by regulators and enterprises as a valuable tool to identify, assess and manage the privacy risks of a project or business function. Having identified the need for a PIA, the process consists of the following steps:[4]

1. **Describe information flows**

   For example, how does the personal information flow from the individual, how does it flow between the organisation and the CSP, what is it used for, who will have access, etc.

2. **Identify the privacy risks**

   Privacy risks should be identified *both* from the perspective of the organisation (for example, events that may lead to non-compliance, reputation damage, etc) *and* from the perspective of its customer (for example, events that may lead to financial loss, embarrassment, etc). The nature of the personal information will be a key consideration in identifying risk.

3. **Evaluate the privacy risks**

   A common approach is to evaluate risks along the dimensions of likelihood and impact. The product of the two is the risk exposure (or rating). This evaluation helps the organisation to prioritise its resources and efforts to manage identified risks, starting from the highest rating.

4. **Formulate risk management strategies**

   Strategies to manage risk should be formulated in light of the risk exposures and the organisation's risk tolerance level (which involves consideration of the strategic intent and benefits). These steps may include mitigation, avoidance and acceptance of risk.

5. **Integrate PIA outcomes back into the project plan**

   It may be necessary to return to the PIA at various stages of the project's development and implementation. The PIA may also generate actions which continue after the assessment has finished, leading to monitoring and re-evaluation down the line.

---

[4] For current information on how to conduct a PIA, see, e.g., Office of the Australian Information Commissioner, *Guide to undertaking privacy impact assessments* (May 2014) <http://www.oaic.gov.au/privacy/privacy-resources/privacy-guides/guide-to-undertaking-privacy-impact-assessments>; Information Commissioner's Office (UK), *Conducting privacy impact assessments code of practice* (February 2014) <https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf>.

5. Decide and plan

The outcomes of the compliance and risk assessments with respect to privacy should feed into the broader assessment of the security and suitability of the cloud solution. From this, the organisation can make a decision about the best course of action, keeping in mind the original strategic intent.

As outlined above, the organisation is also responsible for taking appropriate steps to build privacy into the design of its own solution when using a IaaS or PaaS cloud delivery model.

During engagement

While conducting assurance before engaging a CSP is critical for safeguarding privacy in the cloud, equally important are steps to be taken during the engagement. Organisations should bear in mind the following during their engagement with the CSP.

Ongoing verification

Ongoing verification is necessary to ensure that the CSP has done, is doing and will continue to do what it claimed at the beginning of the engagement. Typically this involves regular audits of the CSP's operations, with accompanying privacy criteria.

Depending on the arrangement, the CSP may allow the organisation (or a third party on its behalf) to conduct the audit, or otherwise provide the results of its own internal audit. The CSP may also provide the organisation with monitoring capabilities that it should make use of.

In relation to external standards, the organisation should ensure that any third-party verifications for privacy and security are up-to-date and continue to cover the relevant scope.

Ongoing appraisal

Today's environment is highly dynamic:

- In the cloud – services are constantly changing as new functionality and capabilities are released
- Organisationally – business requirements may lead to new and/or changing initiatives that leverage the cloud
- Externally – new threats emerge as technology evolves; the compliance landscape shifts as governments and regulators become more active in addressing the cloud; consumer expectations can also be volatile and may impact on the requirements that need to be placed on the CSP.

In light of this, it is unwise for the organisation to 'set and forget' its privacy requirements after the initial assurance process. The organisation should be constantly monitoring its external environment and that of its CSP. It should have a clearly-defined process for triggering an appraisal of any new project or change to existing operations that may involve personal information in the cloud.

The organisation should also keep track of its CSP's activities that may impact on its privacy obligations. These include, for example:

- Changes to controls around privileges and credentials for operator personnel
- New functionality that uses personal information in an unexpected way
- Engagement of a subcontractor that will handle the personal information
- Alteration to the location(s) where the personal information will be held.

Incident response

Incident response refers broadly to the mechanisms the organisation puts in place to handle failure – that is, adverse events that occur in spite of risk mitigation and avoidance strategies. In the privacy context this means any event that involves the misuse, loss or theft of personal information.

From the perspective of individuals it is immaterial whether an incident is the fault of the organisation or the CSP – they are interested in recovery or, failing that, appropriate redress for any inconvenience or harm caused. Given that the organisation is likely to have the most proximate ties to its customers, it should take primary responsibility for the management of failure. This may call for co-ordination with the CSP in relation to incidents in the cloud.

After engagement

The relevant considerations after engagement with the CSP relate to what is done with personal information in terms of its retention, deletion and portability (the post-termination procedures). While chronologically this is the last phase, appropriate steps should be considered and confirmed prior to engagement.

These post-termination procedures constitute not only a potential legal requirement, but also more broadly sound business practice. Information shouldn't be kept if the CSP no longer needs it; keeping it for longer than necessary only increases the likelihood of misuse, loss or theft. Data portability allows the organisation to increase flexibility and avoid vendor lock-in. Since CSPs rarely if ever implement their cloud solutions in the same way, it is very important that the organisation is able to obtain the data held with one CSP in a usable format and easily switch to another CSP.

Generally, post-termination procedures are contained in the CSP's standard contract. The organisation should carefully consider the provisions – and negotiate if possible – to ensure that its privacy requirements are met. Things to watch out for include:

- Whether data will be retained at all following termination – It may be preferable for data to be retained for a limited period (rather than deleted immediately) in order for the organisation to take appropriate steps to retrieve and export the data
- If so, the length of time that data will be retained – Common periods include 30 and 60 days; be alert if it is unspecified or vague (for example, 'commercially reasonable')

- Information on how the CSP destroys the data – This may be relevant if the organisation has specific technical requirements with respect to deletion; CSPs vary in the method and thoroughness of their ‘deletion’
- Whether and in what format the CSP allows for the export of data, so that it can be deployed in another environment.

Appendix I – Reference Tool

Below is a reference tool that summarises the process for safeguarding privacy before, during and after engagement with the CSP for a particular project or business function. Some illustrative examples are provided within.

Before engagement

1. Understand strategic intent

Strategic Intent Statement
For example, consider an organisation in a highly competitive market that is exploring a cloud platform to offer differentiated customer services while improving the ability of their workforce to work from anywhere. The strategic intent statement could be: "To establish a cost-effective technology platform for providing dynamic, customer-centric services while allowing employees to be highly productive anywhere."

Simple benefits table.

Business Area	Efficiency Benefit	Effectiveness Benefit	Performance Benefit
Customer Service	• Reduced time on administrative tasks • Improved service scheduling	• Mobile access to customer information • More rapid time-to-market with new services	• Customer satisfaction improvement • Increased revenue through profitable new services
Information Technology	• Infrastructure cost reduction • Ability to scale up and down on demand	• More rapid deployment of capabilities • Improved mobile security	• Greater agility to align and support the business
Human Resources	• ICT staff re-directed to higher vale work	• Better planning for human resource needs	• Increased staff morale by enabling work-at-home
...	...	...	...

Consideration of external context.

Context area	Considerations
Regulatory	*Relevant legislation – e.g., privacy and data protection law* *Relevant regulatory guidelines and codes* *Laws, regulations or requirements in other countries*
Social	*Community and customer expectations – e.g., sending personal information offshore, data mining, etc.*
Market and competition	*Relevant industry practices and codes*
External stakeholders	*Key external stakeholders – e.g., regulators, civil society groups, cloud and technology industry bodies* *Relevant views, positions or considerations of these stakeholders*
...	*...*

Consideration of internal context.

Context area	Considerations
Structure	*Business unit(s) affected by proposed cloud solution*
Culture	*Workforce awareness of risk and privacy processes* *Privacy governance at the management and board level*
Technology	*Technology platforms deployed within the organisation*
Risk management	*Organisation's current approach around privacy risk management*
Data holdings	*Personal information, categorised into, for example:* • *Name and contact details* • *Demographic information* • *Employee information* • *Health information* • *Financial information* • *Other sensitive information* *De-identified or non-personal information – including the method of de-identification, and how it might be linked with other datasets.*
...	*...*

2. Define requirements

Source	Specifics	Current Practice	Verification
Data Protection Act of Country X/Y/Z	Organisation must ensure that: • The CSP must hold and process personal information consistent with the instructions of the organisation, and may not use the data for its own purposes • Data security and safeguards against misuse, loss, unauthorised access or alteration must be in place • The organisation and the data subject must be able to have ongoing access to the personal information. Access for the data subject will typically be via the organisation • Personal information must be disposed of when there is no longer a legitimate reason to hold it.	Although the organisation does not currently use cloud services, it does have processes in place to manage compliance with privacy requirements when dealing with third party contracted suppliers and service providers.	No formal verification requirement
Government-issued cloud standard on incident response	• The organisation should be able to configure and view reports of system access, malware detections or other security event • The organisation should be alerted to suspicious activity or attacks against its applications.	Currently, access to all external resources is monitored through a gateway. All malware incidents are reported through a security management application.	None
Contract with credit card company	Organisation must comply with the Level 1 Payment Card Industry Data Security Standard requirements.	Currently the organisation is fully compliant.	Annual attestation, quarterly network scans
...	...	...	...

3. Verify claims

Legend	
	Fully conforms to requirement
	Partial conformance to requirement
	Non-conformance to requirement

Mapping requirements to claims.

	Requirement	Claim	Source of Claim
	Personal information must be held and processed only according to the instructions of the organisation.	CSP will hold and process personal information solely for the provision of the cloud services.	Contract, internal policy
	All shared service providers must attain and maintain third party accreditation to ISO 27001.	The hosted service data centre is certified to ISO 27001, but the application or collaboration and communications is not.	Compliance documentation
	The organisation should be alerted to suspicious activity or attacks against its applications.	N/A	N/A
	...	...	...

Catalogue of best practice claims.

Claim	Source of claim
Based on its adherence to ISO/IEC 27018 the CSP will inform the organisation as soon as possible if the CSP determines that its personal information has been breached.	Contract, third party verification
...	...

Catalogue of problematic claims.

Claim	Source of Claim	Further Steps
The CSP may change the terms of the agreement or any services description by posting a new version on its website ... The organisation accepts any modified terms by continuing to use the affected services.	Contract	Negotiate for prior notice before changes to terms or services. If this is not possible, terminate engagement with the CSP
...	...	...

4. Assess risk

Description of Information Flows
Description of how personal information flows from the individual, to the organisation, to the CSP and any other third parties. Note any conditions, safeguards or other relevant information attached to particular pathways. *Ideally accompanied by diagram(s).*

Identify privacy risks – events and corresponding harms.

Risk Event	Potential Harm
Personal information inappropriately used by the CSP, e.g., for marketing purposes	For organisation: non-compliance, reputation damage For individual: embarrassment, anxiety
Data theft by external attacker	For organisation: non-compliance, reputation damage For individual: anxiety, financial damage
Data subject not able to exercise access and correction requests	For organisation: non-compliance For individual: tangible loss or inconvenience due to decision made on the basis of inaccurate information
...	...

Evaluate privacy risks.

Probability	Criteria
1. Rare	• Maybe in extreme circumstances, or • A 100 year event
2. Unlikely	• Never yet happened but might, or • Could occur in 10 years or so
3. Possible	• Could happen, maybe has before, or • Could occur in a year or so
4. Likely	• Could easily happen, or • Could occur in weeks or months
5.Almost certain	• Happens often, or • Could occur within days or weeks

Impact	Criteria
1. Minimal	• Isolated, brief impact • Slight inefficiencies
2. Minor	• Minor, transient impact • Inefficiencies somewhat recoverable
3. Moderate	• Negative impact for a few days • Significant inefficiencies and loss
4. Major	• Persistent negative impact • Unable to achieve a core objective
5. Catastrophic	• Extremely negative impact • Unable to satisfy critical objectives

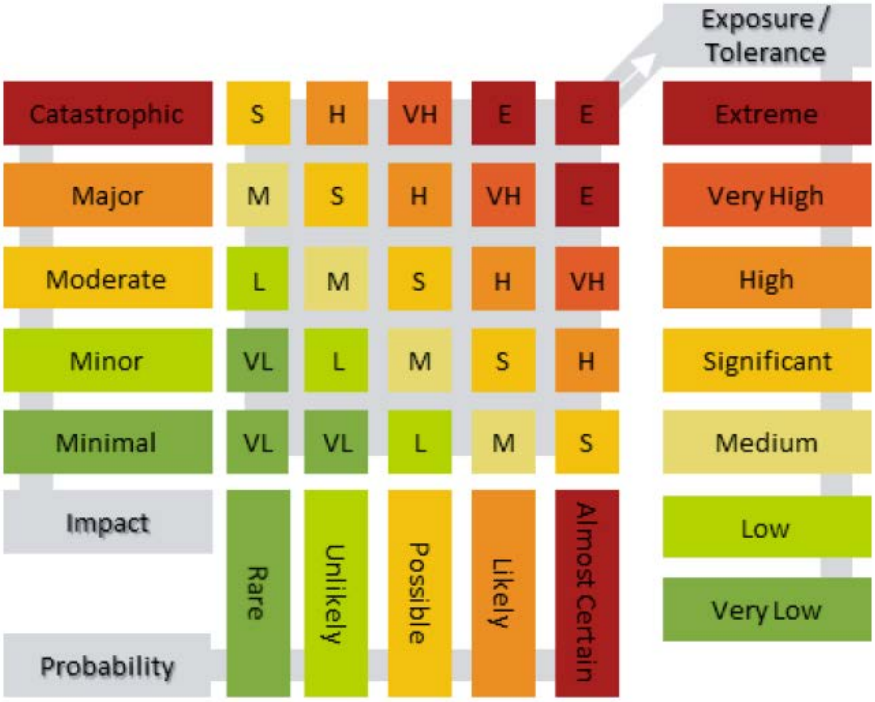

Figure 2: Calculation of risk exposure. Source: Microsoft.

Risk Event	Tolerance	Probability	Impact	Exposure
Inappropriate use of personal information	**M**	**2**	**3**	**M**
Data theft by external attacker	**M**	**2**	**4**	**S**
Unable to exercise access and correction	**M**	**1**	**2**	**VL**
....	...	...	...	...

Risk management strategies.

Risk Event	Strategy
Data theft by external attacker (*prioritise*)	*Avoidance – Refrain from putting certain types of personal information in the cloud* *Mitigation – Implement incident detection and response strategies; purchase cyber insurance*
Inappropriate use of personal information	*Mitigation – Contractual penalties*
Unable to exercise access and correction	*Accept risk – Re-evaluate if risk event occurs*
...	...

5. Decide and plan

Decide and Plan
Combine the privacy compliance and risk assessment with analysis of security, resilience, adaptability and overall suitability of the cloud solution. Make decision on engagement with the CSP in light of the strategic intent. *In the case of a IaaS or PaaS service delivery model, outline how the organisation will build privacy into the design, operation and governance of its own solution.*

During engagement

Ongoing Verification
Describe process(es) for ongoing verification.

Ongoing Appraisal
Describe process(es) for monitoring, appraising and responding to privacy-related events in: • *The external environment* • *The actions of the CSP* • *Internal business developments.*

Incident Response
Describe process(es) – including co-ordination with the CSP – for responding to the misuse, loss and theft of personal information. *Describe the policy for dealing with individuals, including communications, complaints handling, and the provision of recovery and/or redress.*

After engagement

Post-Termination Procedures
Describe how long the personal information will be retained by the CSP. *Describe how the personal information will be deleted by the CSP.* *Describe the format in which the personal information will be exported by the CSP.*

Appendix II – Primer on ISO/IEC 27018

Introduced in July 2014, ISO/IEC 27018 is the newest member of the ISO/IEC 27000 family, which includes the well-accepted ISO/IEC 27001 standard on information security management. Below is a primer that IIS has prepared on the standard.

What is ISO/IEC 27018?

ISO/IEC 27018 is the first international standard comprising a set of privacy and security controls and guidelines for cloud vendors that process and store personal information on behalf of cloud customers in the public cloud.

Why is ISO/IEC 27018 useful?

ISO/IEC 27018 serves as a helpful reference point for cloud customers seeking a trustworthy cloud solution. For cloud vendors, the standard presents a way to differentiate themselves by adopting a set of credible, controls for the protection of their customers' personal information, which can be verified through independent audits.

How does ISO/IEC 27018 work?

ISO/IEC 27018 references existing controls in the ISO/IEC 27002 code of practice for information security management and introduces new controls and guidelines specifically for protecting personal information in the public cloud. The controls are suggestive, rather than prescriptive.

What are the key elements?

- Support cloud customers' privacy obligations, such as enabling access, correction and erasure by individuals
- Process personal information only in accordance with the cloud customer's instructions
- Notify the cloud customer of law enforcement disclosure requests, where legally permissible
- Reject non-legally binding requests to disclose personal information and consult with the cloud customer first where possible before disclosing personal information
- Seek consent from the cloud customer and ensure proper controls are in place when engaging sub-contractors
- Refrain from using personal information for marketing without express consent of the cloud customer
- Promptly notify the cloud customer of unauthorised access to personal information, or an event that results in its loss, disclosure or alteration
- Develop a policy for the return, transfer, retention and disposal of personal information
- Encrypt data when using portable devices and transmitting over public networks
- Specify and document the countries in which personal information may be stored, including by sub-contractors
- Refrain from unilaterally varying the contract to reduce technical and organisational measures for privacy and security protection.

Appendix III – Relevant information for Australia

Privacy Law	
The Privacy Act 1988 (Cth) is Australia's general privacy law. It applies to all Australian Government agencies and also private organisations with an annual turnover of more than $3 million.[5] Major amendments to the Act were made in 2012 and took effect on 12 March 2014.	**Applicable legislation**
The Privacy Act regulates the handling of personal information, which is defined as: "information or an opinion, whether true or not, and whether recorded in a material form or not, about an identified individual, or an individual who is reasonably identifiable." The handling of personal information is subject to 13 Australian Privacy Principles (APPs).	**Definition of personal information**
The APPs accord with the foundational OECD Privacy Principles, and include principles dealing with collection, use and disclosure, data quality, data security and deletion, and access and correction rights. Notably, APP 1 obliges entities to implement practices, procedures and systems that will ensure compliance with the APPs. This calls for a proactive, rather than reactive, approach to privacy.	**Privacy requirements and other notable elements**
The Privacy Act allows personal information to be disclosed and held overseas. To do so, an entity must satisfy APP 8.1 – which requires them to take reasonable steps (usually contractual provisions) to ensure that the recipient does not breach the APPs – or otherwise rely on an exception outlined in APP 8.2. Under section 16C, any breach by the recipient under APP 8.1 is taken to be a breach by the entity. The Privacy Act has not attained adequacy recognition under the EU's framework for allowing personal data of Europeans to be sent to third countries.	**Cross-border requirements**
The Privacy Commissioner's functions include raising awareness, providing guidance, investigating and conciliating complaints, conducting assessments and enforcing breaches of the Privacy Act. The Privacy Commissioner can also develop further sources of compliance, such as privacy codes and determinations. After an investigation, the Privacy Commissioner may determine that affected individuals are entitled to compensation for any loss or damage suffered as a result of a privacy breach. Serious or repeated interferences with privacy may lead to a civil penalty of up to AU$1.7 million.	**Regulator powers**

[5] Subject to some exceptions. For a full list, see: <http://www.oaic.gov.au/privacy/who-is-covered-by-privacy>.

Other requirements
Regulatory actions: <http://www.oaic.gov.au/privacy/privacy-act/applying-privacy-law>
Sectoral legislation: <http://www.oaic.gov.au/privacy/privacy-act/other-legislation>
Australian Signals Directorate, Information Security Manual: <http://www.asd.gov.au/publications/Information_Security_Manual_2014_Controls.pdf>
State and territory privacy laws: <http://www.oaic.gov.au/privacy/other-privacy-jurisdictions/state-and-territory-privacy-law>

The following resources include guidance on good privacy practice in general and cloud computing in particular.

Guidance
OAIC: • APP Guidelines: <http://www.oaic.gov.au/privacy/applying-privacy-law/app-guidelines/> • Guide to Securing Personal Information: <http://www.oaic.gov.au/privacy/privacy-resources/privacy-guides/guide-to-securing-personal-information> • Data Breach Notification Guide: <http://www.oaic.gov.au/privacy/privacy-resources/privacy-guides/data-breach-notification-a-guide-to-handling-personal-information-security-breaches> • Developing an APP Privacy Policy: <http://www.oaic.gov.au/privacy/privacy-resources/privacy-guides/guide-to-developing-an-app-privacy-policy> • Guide to Undertaking PIAs: <http://www.oaic.gov.au/privacy/privacy-resources/privacy-guides/guide-to-undertaking-privacy-impact-assessments>
Department of Finance, Cloud Computing Policies and Guidelines: <http://www.finance.gov.au/cloud/>
Department of Defence, Cloud Computing Security: <http://www.asd.gov.au/infosec/cloudsecurity.htm>
Attorney-General's Department, Protective Security Policy Framework: <http://www.protectivesecurity.gov.au/informationsecurity/Pages/RiskManagementOfOutsourcedICTArrangements-IncludingCloud.aspx>

Appendix IV – Relevant information for New Zealand

Privacy Law	
The Privacy Act 1993 is New Zealand's general privacy law. It applies to all New Zealand public and private organisations that hold personal information, referred to collectively as "agencies".[6] The New Zealand Government is currently conducting a major review of the Privacy Act.	**Applicable legislation**
Personal information means "information about an identifiable individual." The handling of personal information is subject to 12 Information Privacy Principles (IPPs).	**Definition of personal information**
The IPPs accord with the foundational OECD Privacy Principles, and include principles dealing with collection, use and disclosure, data quality, data security and deletion, and access and correction rights. Notably, the Privacy Act requires that agencies nominate at least one individual to be a "privacy officer", who is responsible for encouraging privacy compliance, dealing with privacy requests and working with the Privacy Commissioner in relation to investigations.	**Privacy requirements and other notable elements**
The Privacy Act allows personal information to be disclosed and held overseas. The IPPs do not place conditions on cross-border disclosure. Rather, agencies that store or process personal information overseas (including by a third party acting on their behalf) must comply with the relevant IPPs. In the case of overseas recipients not acting on behalf of an agency, once the IPP 11 disclosure principle is satisfied the personal information will be held subject to the laws of the recipient country. The Privacy Act has achieved recognition under the EU's framework for allowing personal information of Europeans to be sent to third countries. The Privacy Commissioner may prohibit an onward transfer of personal information from one country through New Zealand to another country, if the recipient country does not have comparable safeguards to the Privacy Act and there is likely to be a contravention of the OECD Privacy Principles.	**Cross-border requirements**
The Privacy Commissioner's functions include raising awareness, investigating and conciliating complaints, monitoring technological developments, and examining new legislation. Serious interferences with privacy may lead to commencement of proceedings in the Human Rights Review Tribunal, which can award damages of up to NZ$200,000.	**Regulator powers**

[6] Subject to minor exceptions, see: <https://privacy.org.nz/the-privacy-act-and-codes/privacy-act-and-codes-introduction/>.

Further potential sources of compliance include privacy codes and policies that apply to specific sectors.

Other requirements
Privacy Commissioner, Codes of Practice: <https://www.privacy.org.nz/the-privacy-act-and-codes/codes-of-practice/>
Government Chief Information Officer, Cloud Computing – Information Security and Privacy Considerations: <http://www.ict.govt.nz/assets/ICT-System-Assurance/Cloud-Computing-Information-Security-and-Privacy-Considerations-FINAL2.pdf>

The following resources include guidance on good privacy practice in general and cloud computing in particular.

Guidance
Privacy Commissioner: • Data Safety Toolkit: <https://privacy.org.nz/news-and-publications/guidance-resources/data-safety-toolkit/> • Cloud computing – A Guide to Making the Right Choices: <https://privacy.org.nz/assets/Files/Brochures-and-pamphlets-and-pubs/OPC-Cloud-Computing-guidance-February-2013.pdf> • Privacy Impact Assessment Handbook: <https://privacy.org.nz/news-and-publications/guidance-resources/privacy-impact-assessment-handbook/>
State Services Commission, Government Use of Offshore Information and Communication Technologies (ICT) Service Providers – Advice on Risk Management: <https://ict.govt.nz/assets/Uploads/Drupal/offshore-ICT-service-providers-april-2007.pdf>
Government Chief Information Officer, Guidance and Resources on Privacy and Security: <https://ict.govt.nz/guidance-and-resources/information-management/privacy-and-security/>
Institute of IT Professionals New Zealand, New Zealand Cloud Computing Code of Practice: <http://www.nzcloudcode.org.nz/>

Appendix V – Relevant information for Hong Kong

Privacy Law	
The Personal Data (Privacy) Ordinance ("PDPO") is Hong Kong's general privacy law. It applies to all Hong Kong public and private organisations that control the handling of personal data ("data users").[7] It does not apply to organisations that handle personal data solely on behalf of another party ("data processors").	**Applicable legislation**
Personal data means any information relating to a living individual that can be used to identify that person, in a form that is able to be accessed or processed. The handling of personal information is subject to 6 Data Protection Principles (DPPs).	**Definition of personal data**
The DPPs accord with the foundational OECD Privacy Principles, and include principles dealing with collection, use and disclosure, data quality, data security and deletion, and access and correction rights. The PDPO was amended in 2012 to include strict provisions on direct marketing and the unauthorised disclosure of personal data, with maximum penalties of HK$1 million and five years' imprisonment.	**Privacy requirements and other notable elements**
The PDPO allows personal data to be disclosed and held overseas. A provision that would place conditions on the transfer of personal data outside Hong Kong is not yet in operation.[8] The existing DPPs have a cross-border element. When the data user engages a data processor to handle personal data on its behalf – whether within or outside Hong Kong – it must adopt contractual or other means: • To ensure that the personal data is being kept no longer than necessary • To prevent unauthorised or accidental access, processing, loss or use. The PDPO has not attained adequacy recognition under the EU's framework for allowing personal data of Europeans to be sent to third countries.	**Cross-border requirements**
The Privacy Commissioner's functions include raising awareness, providing guidance, investigating complaints, enforcing the PDPO, and assisting individuals seeking compensation for damage suffered from a privacy breach. Upon discovery of a contravention of the PDPO, the Privacy Commissioner may issue an enforcement notice specifying steps that must be taken to rectify the issue. Non-compliance with the enforcement notice leads to a penalty of HK$50,000 and two years' imprisonment on a first conviction, with higher penalties for second and subsequent convictions.	**Regulator powers**

[7] Subject to minor exceptions, see: <http://www.pcpd.org.hk/english/data_privacy_law/ordinance_at_a_Glance/ordinance.html>.

[8] Section 33 of the Ordinance. Note, however, that the Privacy Commissioner has released guidance that encourages organisations to adopt practices that are broadly in line with the requirements of section 33.

The following resources include guidance on good privacy practice in general and cloud computing in particular.

Guidance

Privacy Commissioner:

- Privacy Management Programme – A Best Practice Guide: <http://www.pcpd.org.hk/english/resources_centre/publications/guidance/files/PMP_guide_e.pdf>
- Guidance on Data Breach Handling and the Giving of Breach Notifications: <http://www.pcpd.org.hk/english/resources_centre/publications/guidance/files/DataBreachHandling_e.pdf>
- Cloud Computing – Information Leaflet: <http://www.pcpd.org.hk/english/resources_centre/publications/information_leaflet/files/cloud_computing_e.pdf>
- Guidance on Personal Data Protection in Cross-Border Data Transfer: <http://www.pcpd.org.hk/english/resources_centre/publications/guidance/files/GN_crossborder_e.pdf>
- Outsourcing the Processing of Personal Data to Data Processors – Information Leaflet: <http://www.pcpd.org.hk/english/resources_centre/publications/information_leaflet/files/dataprocessors_e.pdf>

Hong Kong Computer Society, A Practical Guide for IT Managers and Professionals on the Personal Data (Privacy) Ordinance: <http://www.hkcs.org.hk/en_hk/home/publication/PDPO/files/assets/downloads/publication.pdf>

Office of the Government Chief Information Officer, Practice Guide for Procuring Cloud Services: <http://www.infocloud.gov.hk/themes/ogcio/media/practiceguideindividual/Practice_Guide(2013-11)_EN_new.pdf>

Appendix VI – Relevant information for Singapore

Privacy Law	
The Personal Data Protection Act 2012 ("PDPA") is Singapore's general privacy law. It applies to all private sector organisations that handle personal data.[9]	**Applicable legislation**
Personal data means data about an individual, whether true or not, who can be identified from that data alone or in combination with other information that the organisation has or is likely to have access. The handling of personal data is addressed by key provisions in the PDPA (sections 11 to 26).	**Definition of personal information**
Sections 11 to 26 of the PDPA impose obligations that accord with the foundational OECD Privacy Principles, and include provisions on collection, use and disclosure, data quality, data security and deletion, and access and correction rights. Organisations that process personal data on behalf of others ("data intermediaries") are subject only to the data security and deletion obligations. Notably, the PDPA has two additional requirements for organisations. Firstly, organisations must develop and implement policies and practices that enable them to meet the obligations of the PDPA, including a process for responding to complaints. This calls for a proactive, rather than reactive, approach to privacy. Secondly, organisations must designate at least one individual (the "data protection officer") to oversee their data protection responsibilities.	**Privacy requirements and other notable elements**
The PDPA allows personal data to be transferred overseas, subject to requirements set out in the Personal Data Protection Regulations 2014. Generally, this entails taking reasonable steps to ensure that the recipient is bound by legally enforceable obligations that protect the personal data to a comparable standard to the PDPA, for example by law or contract. Otherwise, organisations must satisfy one of several exceptions, including obtaining consent from the individual. The PDPA has not attained adequacy recognition under the EU's framework for allowing personal data of Europeans to be sent to third countries.	**Cross-border requirements**
The Personal Data Protection Commission is Singapore's regulator. Its functions include raising awareness, investigating and conciliating complaints, conducting research and holding workshops relating to data protection, and enforcing the PDPA. To ensure compliance with the data handling provisions, the Commission has the power to issue financial penalties of up to SG$1 million.	**Regulator powers**

[9] Subject to minor exceptions, see: <https://www.pdpc.gov.sg/legislation-and-guidelines/overview>. The public sector is bound by internal data protection rules as well as other legislation that address secrecy and disclosure.

The following resources include guidance on good privacy practice and IT risk management.

Guidance
Personal Data Protection Commission • Advisory Guidelines on Key Concepts in the Personal Data Protection Act (see especially the protection and transfer limitation obligations): <https://www.pdpc.gov.sg/docs/default-source/annual-seminar-2014-pr/key-concepts.pdf> • Sector Specific Advisory Guidelines: <https://www.pdpc.gov.sg/legislation-and-guidelines/advisory-guidelines/sector-specific-advisory-guidelines>
Monetary Authority of Singapore, Technology Risk Management Guidelines (for financial institutions): <http://www.mas.gov.sg/~/media/MAS/Regulations%20and%20Financial%20Stability/Regulatory%20and%20Supervisory%20Framework/Risk%20Management/TRM%20Guidelines%20%2021%20June%202013.pdf>

INFORMATION
INTEGRITY
SOLUTIONS

Information Integrity Solutions Pty Ltd

Level 3, 53 Balfour Street, Chippendale, Sydney NSW 2008 Australia
PO Box 978, Strawberry Hills NSW 2012, Australia

P: +61 2 8303 2438
F: +61 2 9319 5754
E: inquiries@iispartners.com
www.iispartners.com

ABN 78 107 611 898
ACN107 611 898