Oifig um Sholáthar Rialtais
Office of Government Procurement

Cloud Services Procurement Guidance Note

February 2021

Rialtas na hÉireann
Government of Ireland

Contents

This document is provided for guidance and information purposes only. The document will be subject to amendment and review periodically and the most up to date version will be published on the OGP website www.ogp.gov.ie. The document is not intended as legal advice or a legal interpretation of Irish or EU law on public procurement.

1. Glossary of Terms Used

Term	Acronym	Explanation of Term
Application Programming Interface	API	A software mechanism that allows applications interact with and obtain data from each other.
Cloud Service Provider	CSP	Any supplier of "Cloud" based computer services where "Cloud" based means a system hosted in a data centre owned or leased by the supplier and not by the customer.
CSP Agreement		The standard form of CSP contract.
Data Protection Impact Assessment	DPIA	An assessment of the impact of potential issues from a data protection perspective.
Hyperscalers		The largest Tier 1 CSPs with a global presence and the ability to scale their services and capabilities indefinitely.
Information and Communications Technology	ICT	The general term for the grouping of information technology (IT) and communications technology.
Infrastructure as a Service[1]	IaaS	The capability provided to the customer by the CSP is to provision processing, storage, networks and other fundamental computing resources where the customer is able to deploy and run software, which can include operating systems and applications. The customer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications and, possibly, limited control of networking components (for example, host firewalls).
Intellectual Property Rights	IPR	This generally covers such intangible assets as patents, industrial designs, trademarks, service marks, trade or business names, domain names and copyrights, including copyright in computer programs.
IT Infrastructure Library	ITIL	A framework of best practices for delivering IT services.
Key Performance Indicator	KPI	A performance metric associated with a service or service element.
Multi-tenant[1]	Multi-tenant	An architecture in which a single computing resource is shared but logically isolated to serve multiple consumers.
Platform as a Service[1]	PaaS	The capability provided to the customer by the CSP is the ability to deploy onto the cloud infrastructure customer applications created using programming languages, libraries, services and tools supported by the CSP. The customer does not manage or control the underlying cloud infrastructure, including network, servers, operating systems or storage, but has control over the deployed applications and, possibly, configuration settings for the application hosting environment.
PSB Services Contract		The form of contract included by the PSB in their tender documentation which sets out the terms and conditions for the cloud services to be provided by the CSP to the PSB.
Recovery Point Objective	RPO	The maximum period of time in which an organisation's data might be lost following a major incident.
Recovery Time Objective	RTO	The time to restore data and operations following a major incident.
Request for Information	RFI	Generally used as a mechanism for conducting a pre-market assessment of market and supplier capabilities.
Request for Tender	RFT	Used to solicit tenders from the market in line with Public Procurement Regulations and guidelines.
Reseller		An organisation that re-sells CSP services.

[1] NIST: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.500-322.pdf

Service Level Agreement	SLA	The agreed set of measures, which define the level of service to be provided by the CSP. This can include details such as availability, permitted outages in a given period of time, issue response and resolution timelines and associated service descriptors.
Software as a Service[1]	SaaS	The capability provided to the customer is the ability to use the CSP's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The customer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.
Sub-contractor		An organisation contracted by the CSP to provide services which may augment or be ancillary to the services provided by the CSP. The PSB will not normally have a direct contractual relationship with Sub-contractors.
Sub-processor		This term is used in this guidance note exclusively in the context of data processing and GDPR and relates to a Sub-contractor who processes the PSB's personal data as part of the delivery of the CSP services.
Systems Integrator	SI	An organisation that builds and implements ICT solutions for its customers, often on platforms that are provided by CSPs.
Tier n cloud service provider	"Tier n" CSP	A cloud services provider that is categorised according to its brand, size and capabilities.
Tier 1 cloud service provider	Tier 1 CSP	A global CSP which owns the network in which it is the sole operator and has a direct connection to the internet and networks it uses to deliver voice and data services.
Tier 2 cloud service provider	Tier 2 CSP	A regional CSP which may get a portion of its network from a Tier 1 CSP.
Tier 3 cloud service provider	Tier 3 CSP	A CSP which gets 100% of its network from Tier 1 or Tier 2 CSPs, with no direct access of its own.
User Acceptance Testing	UAT	Final testing by the PSB prior to acceptance of the service.

2. Introduction

2.1. Background to the Guidance Note

The Office of the Government Chief Information Officer (OGCIO) published its Cloud Computing Advice Note in October 2019[2]. The advice note clearly sets out the approach to be taken by Public Sector Bodies (PSBs) to the adoption of cloud services. The advice note also outlines the many advantages and benefits associated with the use of cloud services and provides guidance in relation to the definition, business context, vision and principles associated with cloud computing.

This guidance note augments the OGCIO Cloud Computing Advice Note[2] to the extent that it provides information with regard to the contractual and commercial considerations to be taken into account when preparing to procure cloud services.

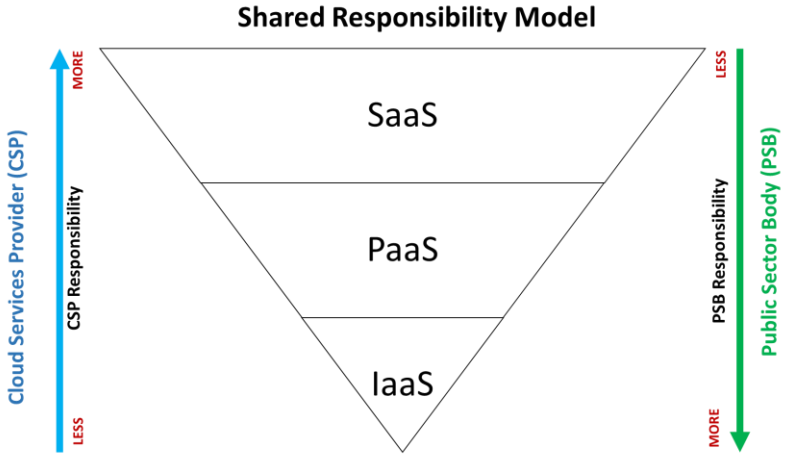
This guidance note should be read in conjunction with the OGCIO Cloud Computing Advice Note[2], referenced above.

The Office of Government Procurement (OGP) recognises that Public Sector Bodies (PSBs) have a need to procure cloud services. OGP has, therefore, produced this guidance note to provide high-level information and guidance to PSBs when considering the procurement of these services. The information provided is not intended to be exhaustive and, if required, PSBs should seek further advice from experts with recognised relevant experience.

To comply with the Public Procurement Regulations[3], PSBs who wish to tender for cloud services are obliged to provide contract terms and conditions as part of the tender documentation. However, this can pose a challenge when tendering for cloud services for a number of reasons, including:

- cloud service providers (CSPs) may offer differentiated services and their terms and conditions may vary, depending on the specific nature and attributes of their services;
- as shown in the following diagram, cloud services may span a spectrum from, at the lowest level, infrastructure as a service (IaaS), to platform as a service (PaaS), to software as a service (SaaS). The breadth of CSP obligations and responsibilities will vary significantly across the different layers of the cloud services spectrum. This will result in a significant variation in terms and conditions across the IaaS/PaaS/SaaS cloud services model.

[2] https://www.gov.ie/en/publication/078d54-cloud-computing-advice-note-october-2019/
[3] http://www.irishstatutebook.ie/eli/2016/si/284/made/en/pdf



This guidance note provides information and guidance with regard to the contractual and commercial considerations to be taken into account when procuring cloud services, generally described within this guidance note under the following headings:

- Software as a Service (SaaS);
- Platform as a Service (PaaS); and
- Infrastructure as a Service (IaaS);

collectively referred to as "XaaS"[4].

In summary, cloud computing consists of a set of technologies and service models that focus on network-based, on-demand use and delivery of IT applications, processing capability, storage and memory space. The cloud services utilising these technologies and service models can be provided by an external service provider or can be delivered in-house, or a combination of both. They can be provided on a private or shared basis. It should be noted that, while PSBs may outsource delivery of a service to a cloud service provider, they remain accountable for the service. It is important, therefore, that PSBs understand the risks, as well as the benefits, associated with the use of cloud services.

In addition to the technical factors related to cloud computing and the provision of cloud services by cloud service providers, PSBs need to understand the nature of the contractual and commercial arrangements that apply when contracting for these services. This applies in particular for PSBs who are coming from a background of self-hosted, on-premises technology environments and may be approaching the cloud services market for the first time.

The benefits associated with cloud services are clearly set out in the OGCIO Advice Note referred to above and at a summary level include:

- enhanced application functionality may only be available online to cloud customers;
- ease of upgrades (particularly for SaaS solutions) and continued support of the service;
- attractive upfront costs;

[4] note that other "as a service" cloud services – such as Desktop as a Service (DaaS) - are not covered in this guidance note

- an alternative option for the replacement of on-premises applications which may be reaching their end of life;
- limited or no in-house IT support or managed service (although in-house IT services are still required, for example, configuration);
- cloud services may be cheaper when workloads are steady;
- cloud may be useful as a cost effective Geo-resilient secondary location (PaaS, IaaS) rather than a secondary on-premises datacentre.

This guidance note addresses the key considerations for the acquisition of cloud services from a commercial and contractual perspective. In all cases, PSBs (contracting authorities) must ensure that they procure cloud services using public procurement competitive processes in accordance with Public Procurement Regulations and national public procurement guidelines, thereby ensuring open, transparent and non-discriminatory processes.

2.2. Guidance Note Context

The general context of this guidance note is to provide information and guidance to PSBs with regard to:

- procuring cloud services in an informed and legally compliant manner which enables PSBs to avail of the value inherent in cloud services while also achieving an equitable balancing of risk with CSPs;
- the general complexity associated with contracting for cloud services; and
- the general differences, from a commercial and contractual perspective, between traditional (legacy) ICT contracts and cloud contracts.

As this note is for guidance only, PSBs should consult with the relevant cloud services market and subject matter or other relevant experts in order to gather the information necessary to enable them to develop their tender documentation, including contractual terms and conditions. Cloud services - and the contexts in which PSBs may wish to use them – can be complex; therefore, the knowledge gleaned from a pre-market engagement will provide for a more informed, efficient and effective procurement process. Pre-market engagement, including where advice is sought from independent experts or market providers, must not confer any unfair advantage on any supplier in any subsequent tender process. The principles of equal treatment and transparency apply.

When considering a contract with a CSP there are a significant number of provisions which differ from more traditional ICT contracts for “on premises” solutions. These differences arise, in the main, as the CSP is likely to be delivering a consolidated set of services to a diverse group of customers. The CSP will, accordingly, endeavour to minimise variations to key contract terms in order to reduce their exposure to risk and to simplify contract administration and management across their customer base.

This guidance note refers to differences, where relevant, between a “cloud” contract and a legacy ICT contract. The aim is to provide PSBs with information to help to ensure that their tender documents contain contractual terms and conditions which are informed and balanced in terms of the risks which may arise under such contracts. PSBs should seek their own legal advice when constructing cloud PSB Services Contracts.

The commentary on the contractual terms and conditions which are in scope for this guidance note is grouped based on the degree of commonality generally seen in the market. Similarly, the commentary on commercial considerations reflects cloud services pricing models commonly seen in the market.

2.3. Overview of Cloud Contracts

Market analysis indicates that CSPs generally insist that their terms and conditions (for example, security, data protection, term, termination and exit provisions) take precedence over any client terms and conditions. This is usually implemented through "click-through" hyperlinks to the CSP's terms and conditions.

This may be challenging for PSBs insofar as it may have the effect of conflicting with the terms and conditions published in the PSB's tender documentation. In compliance with Public Procurement Regulations and guidelines, PSBs must publish the terms and conditions which will apply in respect of a contract awarded under a public procurement competition. Contractual terms and conditions cannot be subject to substantial modification thereafter. Accordingly, the PSB terms must take precedence over any conflicting terms put forward by CSPs and this should be specifically set out in the PSB Services Contract. It is important to note that not all CSPs are amenable to modifications to their terms and conditions. PSBs should always seek legal advice in relation to any conflicts between their published terms and conditions and those of the CSP.

In some instances, cloud services may be supplied indirectly through resellers, cloud services brokers or Systems Integrators. These entities act as an intermediary between the cloud services customer and the CSP and, in this role, may be willing to accept risk in their contracts which would otherwise be borne by the CSP's customer (in this case the PSB) in a direct sale transaction with the CSP.

2.4. Pre-Market Engagement

PSBs are encouraged to engage with the market prior to drafting their tender documentation. The most transparent mechanism by which PSBs can conduct market soundings is by publishing a Request for Information (RFI). During this pre-market engagement phase of the public procurement process, PSBs should consider the following:

– **solution assessment:** the output from an RFI process can be used to inform the solution assessment and in determining the right type of solution to meet the requirements. The solution could be IaaS (with the applications hosted in the cloud but under the ownership and control of the PSB), PaaS (with the development and test environment and operational infrastructure hosted in the cloud) or SaaS (with the full solution – hardware, software, network and security – provided in the cloud and accessed by the PSB users through their mobile or PC/laptop devices).

– **Data Protection Impact Assessment:** the solution assessment should also include completion of a data protection impact assessment (DPIA) and classification of the data which will be migrated to the cloud in terms of its sensitivity, including the impact of a data breach.

– **risk and benefit analysis:** pre-market engagement can provide useful information

to be used in assessing the risks and benefits that the proposed solution will deliver from the perspectives of implementation, control, ease of deployment, accessibility, lifetime costs and overall business case.

– **contractual and commercial terms:** engagement with the market will assist PSBs in drafting the terms and conditions to be published as part of their tender documentation.

Key contractual and commercial factors to be considered are addressed at a more detailed level in the checklists in Appendix 1. PSBs are advised to seek expert legal advice when drafting the PSB Services Contract which is to be included in the tender documentation.

3. Cloud Services Contract Considerations

Cloud services can be complex and the contractual provisions in cloud services contracts define what services are to be provided, how they are to be provided and what the pricing arrangements are for the differing types of cloud services. This section sets the context for the general factors to be taken into account when entering into contracts with CSPs for the provision of cloud services.

3.1. Overview of CSP Contractual and Commercial Provisions

PSBs need to have a reasonable understanding of the types of provisions that apply to cloud services contracts and how they differ between IaaS, PaaS and SaaS contracts.

This section provides an overview of some key contractual and commercial provisions generally seen in CSP standard agreements. The overview will help to inform PSBs regarding the provisions of a typical CSP Agreement, which CSPs will expect to have incorporated into any contract they enter into with a PSB. PSBs should satisfy themselves that they are familiar with the content of CSP Agreements in the context of the contractual terms and conditions they are publishing in the tender documentation and should conduct their own analysis, as required, in order to ensure that they are so informed.

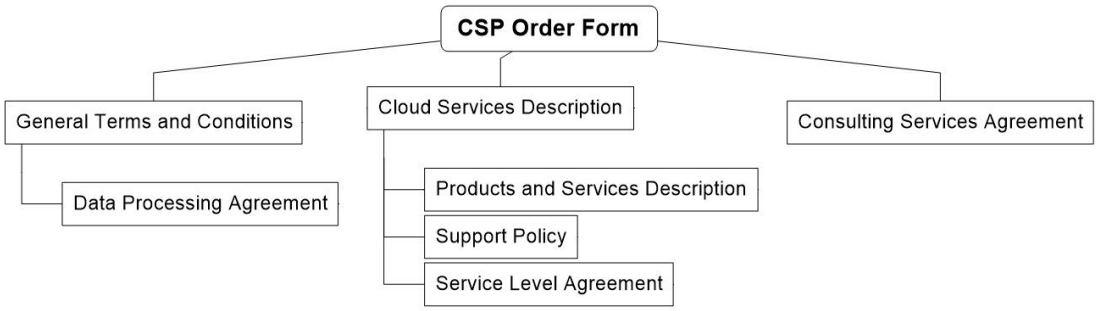
For cloud services contracts, the contractual and commercial considerations are of fundamental importance to the apportionment and equalisation of risk and delivery of value across the lifetime of the contract. Some provisions are more important than others and it is incumbent on PSBs who are entering into contracts with CSPs to understand the context in which any particular provision within those contracts may apply and its relevance to: the services, the anticipated value being delivered through those services and the apportionment of risk between the contracting parties under the contract.

Key contractual and commercial provisions are described in outline here. More detailed guidance is provided through the checklists in Appendix 1 and it is recommended that the checklists are used by PSBs to inform the construction of PSB Services Contracts for the provision of cloud services. CSPs may often be supported by an ecosystem of Sub-contractor partners for the delivery and ongoing support of the services. These Sub-contractors may have their own agreements which may be visible to the PSB or, on the other hand, may not be readily visible but are instead contained in downstream agreements referenced through URL links contained in the CSP Agreement.

Great care must be taken to understand the structure of the cloud services agreements and the rights and obligations of all parties in the delivery of the services. An example of the standard agreements structure provided by a CSP for an enterprise SaaS solution is shown in figure 1. In some instances, the solution may be delivered by a third party service provider (for example, a Systems Integrator) which may take on a prime contracting role for the implementation of the solution.

It should be noted that the assessment of CSP terms and conditions should be undertaken in the pre-market assessment phase and the PSB Services Contract should be constructed bearing in mind what is acceptable to the market while also maximising protection for the PSB (particularly in relation to data protection and security) and ensuring a reasonable balance of risk.

Figure 1: Example CSP Enterprise SaaS Agreements Structure



In the example 'CSP Enterprise SaaS Agreements Structure' above:

- the CSP Order Form is the controlling agreement and it takes precedence over the other agreements. There can be multiple Order Forms under a single Enterprise SaaS Agreement;
- the Cloud Services Description describes the cloud services to be provided;
- the Product and Services Supplement, Support Policy and Service Level Agreement describe, respectively, the specific products and services to be provided, the support provisions and the service level agreement for the services being delivered (containing such metrics as availability, incident response times, service credits for service failures);
- the General Terms and Conditions contain the main body of general legal provisions (term, termination, warranties, liabilities, indemnities);
- the Data Processing Agreement may specify the CSP's general obligations in terms of conformance with data processing laws and regulations (for example, GDPR); and
- the Consulting Services Agreement will cover the provision of professional services/consulting services for initial implementation of the services and subsequent use of CSP professional services on a project by project basis. These services will generally be drawn down under specific Statements of Work (SOWs), each of which will have its own provisions to reflect the deliverables, delivery and payment milestones, acceptance processes, personnel/resource allocations, rate cards for the resource types to be deployed under the SOW and any specific qualification or augmentation of terms that may be set out in the "umbrella" Consulting Services Agreement or the General Terms and Conditions.

Therefore, in addition to the specific provisions that apply in cloud services agreements, PSBs also need to understand the structure of cloud services agreements including:

- how component sub-agreements are constructed;
- their relevance to each other; and

- the precedence of common or conflicting provisions between the "master" services agreement and any component agreements or schedules. This need for understanding applies in particular in relation to the role of Sub-contractors in the implementation, delivery and support of the services.

PSBs have an obligation to comply with Public Procurement Regulations when tendering for products and services. This includes providing a PSB Services Contract which ensures compliance with the Public Procurement Regulations but which will also elicit bids from the market; this can be a difficult balance to achieve. With an understanding of CSPs' general contractual provisions, PSBs can ensure that the PSB Services Contract published with the tender documentation will be compliant with the Public Procurement Regulations and have a likelihood of eliciting supplier responses accordingly. As recommended elsewhere in this guidance note, legal advice should be sought when preparing contract documentation for cloud services tenders.

3.2. An Introduction to Key Contractual and Commercial Terms

Contract Term or Duration

The contract term is a key consideration for both parties to the agreement:

- For the CSP, a long contract term results in guaranteed revenues over the customer lifetime. This helps CSPs maintain and grow revenue while mitigating the negative revenue impacts of customer "churn" - the loss of customers over time due to non-renewal of CSP service agreements. Therefore, CSPs will generally have a strong interest in a long, rather than short, contract term and may provide incentives to customers to commit to longer term contracts.
- For the PSB, a long contract term generally results in guaranteed service provision at a defined price (subject to variations related to usage, etc.). A longer-term commitment may result in such incentives as improved pricing and lower total cost of ownership (TCO) over the contract term. However, ICT market analysts also indicate that the price of CSP services may increase following the initial contract term. PSBs always need to consider whether a long contract term may have the effect of restricting competition.
- PSBs should consider the "what-if" factors relating to potential early termination of the contract and how flexible or inflexible CSPs may be in such an event; this will be dictated by how the term and termination provisions have been defined.
- PSBs should also consider the potential effect of "lock-in" to a specific CSP and resulting loss of leverage that may ensue at the end of the contract term if the PSB wishes to extend the service beyond the initial term i.e. avail of any permitted extensions to the contract.

Contract Termination

Contract termination is a key consideration for both parties. As cloud services contracts are limited term contracts which will (unless terminated early, renewed or extended) come to an end at the conclusion of the contract term, a number of key factors need to be considered. These include:

- the factors which may result in termination of the contract (for example, normal

termination at the end of the contract term, early termination due to default or unremedied material breach);
- the likely consequences of such termination; and
- the management of any risks associated with contract termination, including transfer/transition of data and services from the CSP back to the PSB or to another replacement CSP.

These topics are addressed in further detail in Appendix 1.

Exit Management

Cloud-based services create a higher dependency on CSPs than equivalent services deployed on-premises. On-premises deployments of hardware, software and communications capabilities are largely under the control of the PSB. In the cloud environment, some or all of these capabilities are under the control of the CSP. The extent of this control depends on whether the services provided are IaaS, PaaS or SaaS, with the level of CSP dependency generally increasing as the services move from IaaS to PaaS and on to SaaS.

It is important to fully consider how the transition from a cloud service provided by an incumbent CSP to another CSP, or back on-premises, is managed on expiry or termination of the cloud services contract. This is addressed through the exit management provisions and associated processes specified in the contract. An exit management plan should be agreed and reviewed regularly with the CSP to ensure that it remains relevant and up-to-date over the full term of the contract.

Security

Key elements of the security considerations for the provision of cloud services include:

- data encryption: this must cover, at a minimum, data at rest and data in transit and the required standard must be set out by the PSB;
- data location: in general, personal data must not be transferred outside the EEA or, if it is to be transferred outside the EEA, the transfer must be in compliance with the provisions of Chapter V of the GDPR;
- under the terms of many standard CSP Agreements the responsibility for data protection and security remains with the PSB, particularly for IaaS agreements. PaaS and SaaS contracts will likely provide security, backup and recovery as part of the CSP services, but some service elements may incur an additional charge;
- private versus public access (VPN versus public network access); and
- physical versus virtual tenancy in the cloud.

When considering the security requirements as set out in their RFTs and contracts, PSBs should always refer to the EDPS guidance on XaaS security.[5]

[5] https://edps.europa.eu/sites/edp/files/publication/18-03-16_cloud_computing_guidelines_en.pdf

Data Protection

Compliance with data protection obligations is a fundamental requirement for CSP Agreements. Since the CJEU "Schrems II" judgment on 16th July 2020, Privacy Shield certification is no longer a valid compliance regime for US CSPs. Therefore, great care must be taken in specifying the data protection provisions in the PSB Services Contract, particularly where CSP organisations are likely to process data outside the EEA. If PSB data is to be transferred outside the EEA, it must be done in compliance with the provisions of Chapter V of the GDPR. PSBs should note that they cannot outsource their accountability in relation to data protection and security and therefore remain fully responsible and accountable in regard to these obligations.

Suspension of Services by the CSP

PSBs should be aware that CSP Agreements may contain provisions that allow them to suspend services (for example, non-payment of fees or degradation of service for other customers resulting from the PSB's use of the services).

This "suspension of services" factor has more significance in cloud services agreements than PSBs may have been familiar with previously under non-cloud agreements and therefore needs to be considered carefully when drafting cloud PSB Services Contracts. The provisions for suspension of services should be limited to the greatest extent possible.

Pricing Models

The pricing models applying to cloud services can be complex and can vary significantly according to the type of cloud service being procured (IaaS, PaaS or SaaS). PSBs need to understand the pricing models that apply to the different types of cloud services and their component elements (for example, physical or virtual servers, storage and compute capacity, operating system, middleware and applications software, network bandwidth, security services and other services that may be included as part of an overall managed service). Each of these elements may have a different pricing model; some may be fixed and others may be variable and it is important for PSBs to understand fully the likely total cost of ownership (TCO) for the services under consideration for the envisaged term of the contract.

In-Life Service and Relationship Management

During the contract term, the services being delivered will require to be carefully managed. This will require the implementation and enablement of adequate service delivery management processes (for example, in line with ITIL processes) on the CSP's side and supplier performance and service management on the PSB's side. These are often supported by mutual governance and relationship management processes which, in addition to supporting the ongoing management of PSB demand and CSP operational delivery, also provide forums for strategic planning, CSP technology roadmap discussions and general service and relationship optimisation planning.

4. Introduction to the Cloud Services Contractual and Commercial Checklist

The checklist in Appendix 1 of this note provides guidance to PSBs on the key differences between procuring and contracting for cloud services compared to PSB-controlled, on-premises ICT solutions, and the key contractual and commercial considerations regarding those differences. The checklist also serves as a toolkit to assist in drafting tender documentation for cloud services procurements. As previously stated, PSBs should also glean an understanding of the cloud services market through their pre-market engagement and solution assessment.

PSBs are reminded that they should seek expert support and legal advice to assist in developing tender documentation and PSB Services Contracts when procuring cloud services.

Appendix 1: Cloud Services Contractual and Commercial Checklist

Contractual and Commercial Considerations – Section 1

Topic	Checklist Item	PSB Considerations	Reasons for PSB Considerations
Agreement Termination	a. Termination Notice Period	1. When considering the duration of the termination period, PSBs should consider fully the impact and consequences of termination, both at the end of the contract term and, in the event of early termination, before the termination date. 2. Conduct a risk assessment as part of the business impact analysis. 3. Carefully consider the actions which will be required to migrate the service in the event of termination. These are often addressed as part of business continuity planning and related exit management processes. 4. The PSB should consider the time taken to procure a replacement CSP, if required, and should specify, where relevant, a longer termination notice period above that which may be set out in the standard CSP Agreement. 5. The PSB should endeavour to have a provision in the PSB Services Contract to rescind notice of termination by the PSB, if necessary, provided that it is issued within a defined period before the termination date.	1. This is a key consideration. The termination notice period will determine how much time will be available to the PSB to effect a migration from the CSP, either back in-house or to a replacement CSP. 2. A business impact analysis to address all risks relating to contract termination should be undertaken so that any risks may be foreseen and managed effectively if/when they arise. 3. Exit management, data transfer/migration and CSP commitment to support the exit process are key factors in mitigating any risk resulting from the contract exit. Any prospect of termination should be considered carefully in terms of the potential impact of a failed transition and reliance on the incumbent CSP for migration and termination support and related activities. 4. The PSB will need to ensure that the termination notice allows sufficient time to transition off the service; ideally, the termination notice period should be up to one year to allow a successful transition of services from the CSP. 5. It may be necessary to rescind notice of termination. Some CSPs will allow for notice of termination to be rescinded if received within a defined period before the contract termination date.

Topic	Checklist Item	PSB Considerations	Reasons for PSB Considerations
		6. PSBs should consider all potential termination contexts when planning for termination and exit management and seek legal advice in relation to termination provisions.	6. The PSB needs to be clear on all circumstances in which the contract may be terminated (natural end of term, termination for breach by either party, termination for convenience and termination resulting from the occurrence of specific events).
	b. Termination Costs	1. The PSB Services Contract should specify what services associated with termination and exit are provided free-of-charge by the CSP and what services will be chargeable. Where additional professional services may be required of the CSP for data downloads, assistance with data migration and any other related services, the costs and the charging mechanism for additional data downloads and professional services should be clearly defined in the PSB Services Contract.	1. The rationale and basis for any costs associated with termination must be defined up-front. For example, PSB data must be returned free of charge and in a format that will be usable by the PSB or an incoming CSP. Any in-life data downloads that may be required for the purpose of migration contingency tests should be defined in terms of the number of downloads and the costs of any downloads over and above a minimum number. It is not unusual for free-of-charge downloads to be limited to one download for test purposes to ensure that the data is correct and a second download for live migration.
	c. Bandwidth Restrictions	1. The PSB Services Contract should specify any minimum bandwidth requirements.	1. To prevent bandwidth “throttling”, any minimum bandwidth requirements should be specified for data downloads.
	d. Data Format and Deletion of Data	1. The PSB Services Contract should specify the data format for data downloads (for example, CSV, XML, Excel). 2. Depending on the nature of the XaaS Service, PSBs should specify a) the conditions under which their data is deleted from the CSP environment and b) the method of verifying that the deletion of data has been successfully completed following termination of the service.	1. The PSB should ensure that the data format for the migrated data is called out in the PSB Services Contract to avoid potential issues at time of termination and to enable the PSB/incoming CSP to ensure the appropriate data formats and related migration tools are available prior to the data migration. 2. Where applicable, all PSB data must be deleted by the CSP from the CSP environment after confirmation by the PSB that it approves the deletion. A certificate of deletion must be provided by the CSP.
	e. Transition Assistance Services	1. The PSB Services Contract should specify that PSB access to the CSP’s data download tool will be	1. The PSB Services Contract should specify that access to the CSP’s data download tool will be provided, free of charge, to enable “self-service” data download.

Topic	Checklist Item	PSB Considerations	Reasons for PSB Considerations
		available, free of charge, for data downloads as required. 2. The PSB Services Contract should: – state that the CSP will not unreasonably withhold paid-for professional services that may be required to undertake the data downloads and support the data migration activity; – contain a professional services rate card addendum that sets out the daily/hourly rates by resource type; – specify the method of calculating and paying for the professional services that may be required.	2. The PSB Services Contract should state that the CSP will not unreasonably withhold professional services that may be required to perform the data downloads and support the data migration activity. The professional services day rates for this service should be defined in a rate card and the overall fee for the services should ideally be fixed or capped.
	f. Termination by CSP and Deletion of Data.	1. The PSB Services Contract should clearly define the respective termination rights of the parties. 2. The PSB Services Contract should address termination for convenience which, ideally, should be at the PSBs discretion. The termination notice period should be at least one year to allow the PSB to plan and undertake the contract exit with minimal risk of disruption to services. The PSB should ensure that its exit management plans and processes reflect the impact of normal termination at the end of the contract term as well as early termination (whether due to either termination for convenience or termination for cause). 3. The PSB should specify the termination notice period in the tender documentation.	1. The general circumstances in which a CSP will have the right to terminate the contract would be as a result of an unremedied breach by the PSB, breach of confidentiality etc. Any termination rights by the CSP beyond these should be carefully assessed and understood. Termination for convenience should be at the PSB's discretion. 2. Any termination by the CSP should allow a sufficient amount of time for the PSB to migrate data and transition off the terminating service. In addition, any termination by the CSP should provide clarity with regard to the PSB's obligations to pay any sums that would otherwise be due for subsequent periods if the contract were not terminated. There should also be clarity with regard to refunds that may be due to the PSB for any cloud services that have been prepaid and would have been scheduled for delivery after the termination date. 3. The period of termination will be decided by the PSB when drafting the tender documents.

Topic	Checklist Item	PSB Considerations	Reasons for PSB Considerations
		4. The PSB Services Contract should clearly state that data may not be deleted by the CSP until it has been downloaded by the PSB.	4. It is critical that PSB data must not be deleted by the CSP until it has been returned to, validated and verified by the PSB. As noted under item e. (Transition Assistance Services) above, great care must be taken to ensure that the PSB data is downloaded in a format which will enable it to be migrated to another CSP.
		5. The PSB Services Contract should allow for the PSB to audit the CSP environment to ensure that data has been deleted from the CSP environment; failing this, the CSP should be obliged to certify that the data has been deleted from primary and backup data locations.	5. The PSB's right to audit the CSP environment must survive termination in order to validate that data has been deleted. If this is not achievable, certification of data deletion must be provided by the CSP. It should be noted that market analysts indicate that a global standard of certification of data deletion is not available and certification is generally a written statement signed by the CSP.
		6. The PSB Services Contract should specify any applicable standards or, in the absence of standards certification, equivalent assurances that the CSP's internal controls conform to good industry practice.	6. Ideally, the PSB Services Contract will include SSAE 18[6] or SOC [7] provisions which will provide some assurances regarding the CSP's internal controls.
	g. Risk of Suspension of Service	1. The PSB should satisfy itself that the circumstances in which the CSP may suspend services are limited as far as possible.	1. PSBs should be aware that CSP Agreements may contain provisions that allow them to suspend services (for example, non-payment of fees or degradation of service for other customers resulting from the PSB's use of the services).
		2. The PSB Services Contract should have well-defined and clear resolution processes for any disputes that may arise.	2. Because the CSP holds significant power as a result of being the controller of the PSB's use of its services, the conditions under which CSPs may suspend services should be limited (for example, in the event of a legitimate dispute that has not been resolved through normal governance, escalation or dispute resolution processes).

[6] SSAE 18 – https://www.aicpa.org/content/dam/aicpa/research/standards/auditattest/downloadabledocuments/ssae-no-18.pdf
[7] SOC – System and Organisation Controls (SOC) reports

Topic	Checklist Item	PSB Considerations	Reasons for PSB Considerations
Contract Term	Contract Term	1. As CSP Agreements are term-limited, the contract term is a key consideration. The PSB should ensure that the PSB Services Contract does not allow for any "auto-renew" provision.	1. PSBs need to ensure that the contract term is carefully considered and clearly set out in the contract and/or Order Form. PSBs need to be aware of "auto renew" provisions (which may only appear in the Order Form, for example) which would result in the contract being renewed at the end of the initial term unless a termination notice is received by the CSP in accordance with the contract termination notice provisions (which can, for example, be up to six months before the end of the initial term).
		2. The contract term, including any option to extend the contract, for any short term pilot should be explicitly called out in the PSB Services Contract, with adequate notice periods allowing for consideration by the PSB of all relevant contract extension or contract exit factors.	2. PSBs should exercise care when undertaking short-term pilot projects as any "auto-start" language may result in the contract extending into a longer term commitment once the trial period has ended (unless it is explicitly cancelled).
		3. PSBs should ensure that, following the initial term, pricing does not automatically revert to CSP "list price" and should include provisions in their PSB Services Contract for price increases to be limited to consumer price index (CPI) or a fixed percentage increase.	3. Where the PSB wishes to extend the initial contract term (either explicitly or via an auto-renewal), by availing of any extension(s) permitted under the terms of the contract, the PSB Services Contract should state that any renewal will be based on the terms and conditions and pricing applicable during the initial term, subject to a CPI or fixed uplift.
Security	a. Data Encryption – Data at Rest / Data in Transit	1. The PSB Services Contract should specify the encryption processes that will apply to, at a minimum, data at rest (that is, data stored on primary and secondary storage devices and locations) and data in transit (that is, data that is being transmitted across networks). If data encryption is not provided by the CSP as standard, PSBs should stipulate that data encryption is provided. However, PSBs need to be aware that certain types of encryption may slow down performance (therefore, a technical assessment by	1. All data, whether personal data or otherwise, must be encrypted wherever it is and whether it is in transit or at rest. Please refer to GDPR guidance [8] on allowed location of personal data for the Irish public sector - that is: a) in the Republic of Ireland; b) in the EEA, including Norway, Switzerland and Lichtenstein; c) in other jurisdictions where GDPR-like arrangements and reciprocity with EU exist (see note regarding Privacy Shield below).

[8] https://www.dataprotection.ie/sites/default/files/uploads/2019-10/Guidance%20for%20Engaging%20Cloud%20Service%20Providers_Oct19.pdf

Topic	Checklist Item	PSB Considerations	Reasons for PSB Considerations
		the PSB of the CSP's data encryption capabilities is required which includes consideration of all facets of the encryption regime). PSBs should consult with their legal advisers in relation to data transfer provisions in their PSB Services Contracts.	
	b. Data Backup & Recovery and Disaster Recovery (DR)	1. PSBs should ensure that they fully understand the differing contexts in which data backup, recovery and disaster recovery apply and who is responsible for what. 2. The PSB Services Contract should clearly set out the roles and responsibilities of the parties in relation to data backup and recovery. 3. Where applicable, the service level agreement set out in the PSB Services Contract should define any metrics relating to data backup and recovery (for example, target RPO and RTO metrics). 4. PSBs should use market research to understand the range of BCM/DR policies and practices before constructing the PSB Services Contract and any related service level agreements. **NOTE:** PSBs need to be aware of any potential additional costs that may be associated with the backup/recovery and disaster recovery services or any client-specific KPIs relating to them.	1. Depending on the type of cloud services being procured, data backup and recovery and disaster recovery services may be the responsibility of the PSB or the CSP: – for PaaS and SaaS, these are generally the responsibility of the CSP, but may incur additional charges; – for IaaS, they may be the responsibility of the CSP or the PSB. 2. PSBs should ensure that the roles and responsibilities of the CSP and the PSB in relation to backup and recovery are clearly defined. 3. Where the CSP is responsible, then the PSB should ensure that there are clear and comprehensive RPO and RTO metrics in the service level agreement. 4. In addition, PSBs should ensure that the CSP's business continuity management and disaster recovery (BCM/DR) policies and practices meet the PSB's requirements.
	c. CSP Responsibility for Security	1. PSBs should understand and define clearly in the PSB Services Contract where the responsibility for security lies. PSBs should note their obligations	1. Some standard cloud contract terms and conditions place the responsibility for data protection and security with the PSB, particularly for IaaS contracts. PaaS and SaaS contracts may

Topic	Checklist Item	PSB Considerations	Reasons for PSB Considerations
		under Article 28 of the GDPR as to what is required when engaging with a Data Processor. 2. A DPIA should be undertaken by the PSB prior to publication of tender documents and CSP capabilities should be considered in this context. 3. The PSB Services Contract should specify the CSP's responsibility in relation to such topics as: – compliance with security standards (for example, ISO 27001, ISO27017 or equivalent); – logical and physical security; – DDOS attacks; – penetration testing. 4. The PSB Services Contract should specify the CSP's security compliance obligations. These should be defined by or agreed with the PSB's internal information security personnel and form part of the contract. CSPs may employ Sub-contractors across their partner ecosystems in order to deliver and implement their services with speed and to scale. The PSB Services Contract must specify that the CSP will agree to enforce the same security obligations on the Sub-contractors as the CSP agrees with the PSB. The PSB Services Contract should comprehensively address all relevant security obligations to be covered by the CSP.	provide security, backup and recovery as part of the cloud service, although this may incur an additional charge. 2. CSPs have clearly defined responsibility for access and physical security (data centre premises etc.). Depending on the type of service being provided (IaaS, PaaS or SaaS), responsibility for all other security requirements must be clearly set out (for example, Security Incident and Event Management and protection against malware). 3. The CSP must have processes in place to ensure compliance with the PSB's security requirements, relevant legislation and their contractual obligations, including compliance with GDPR. Appropriate technical and organisational processes and procedures should be in place to secure the PSB data that is being processed and call out the standards and certifications they have received and are operating under (for example, ISO27001 for Information Security Management). Refer to the OGCIO Guidance note[9] for further information relating to certification. 4. Article 28.4 of the GDPR states that the CSP must commit to enforcing at least the same security obligations on Sub-contractors as the CSP itself is agreeing with the PSB. **NOTE:** If the PSB is regulated as an "Operator of Essential Services" under the Network and Information Systems Directive[10], it must ensure that the security provisions in the PSB Services Contract allow it to meet its obligations under the Directive.

[9] https://www.gov.ie/en/publication/078d54-cloud-computing-advice-note-october-2019/
[10] https://www.gov.ie/en/publication/313e9-nis-compliance-guidelines-for-operators-of-essential-service-oes/

Topic	Checklist Item	PSB Considerations	Reasons for PSB Considerations
	d. Data Integrity	1. The PSB Services Contract should specify the CSP's obligations in relation to ensuring the integrity of PSB data and should reflect the context in which data is stored, for example: – data residing on the PSB's dedicated infrastructure within the CSP's environment; – data residing on shared infrastructure (PSB's dedicated virtual machines or shared virtual machines); – data residing in shared data stores (databases).	1. When selecting a cloud services solution, careful consideration must be given to the assessment of data separation (ensuring that another consumer of the CSP's cloud service cannot interrupt or compromise the service or data of another). This is also a key consideration when deciding on whether to opt for a multi-tenancy implementation (where customers may share infrastructure or, in the case of a SaaS solution, share the application code base) or to use dedicated resources. In some instances, the PSB may not have a choice; for example, a SaaS solution provider may only provide a single instance, multi-tenant option in order to streamline their solution delivery, software updates and version management processes. Whichever option is selected, the PSB must have confidence in the CSP's ability to ensure the integrity of the PSB's data.
Data Protection	a. GDPR Compliance – Audits / Access to Data	1. The PSB Services Contract should stipulate that the PSB has access to all third party independent audits. 2. The PSB Services Contract should specify what data processing activities will be carried out and how the PSB's data will be protected. 3. The PSB Services Contract should be explicit in terms of what is allowed and disallowed with regard to the use of the PSB's data.	1. In general, CSPs use third party independent auditors to assess their cloud services (including their data centres, networks, logical and physical security facilities etc.). PSBs should request access to this information. 2. CSP obligations in terms of data processing and protection of PSB data should be clear and comprehensive to include: pseudonymisation and encryption of personal data, isolation and separation of personal data from other PSBs' data, availability and resilience of data processing systems and services, procedures to deal with a data breach (including incident response processes, notification timelines and incident resolution plans). 3. PSBs should clearly set out in the PSB Services Contract what is explicitly allowed and what is explicitly disallowed in relation to the processing of their data (for example, use of data for marketing purposes).

Topic	Checklist Item	PSB Considerations	Reasons for PSB Considerations
		4. The PSB Services Contract should set out clear obligations in relation to the processing of data by the CSP's Sub-processors. The PSB should be satisfied that the CSP will only process personal data in accordance with the specific instructions of the PSB. The PSB Services Contract should take into account the potential impact arising from loss, destruction, alteration, unauthorised disclosure of or access to personal data stored by the CSP, whether accidental, unlawful or otherwise.	4. CSPs are responsible for data processing by their Sub-processors including ensuring that there are no international data transfers that are not compliant with GDPR (and this now includes no data transfers to countries that were previously covered by the Privacy Shield framework which has been invalidated by the CJEU Schrems II judgment[11]). The Irish Data Protection Commissioner states that, with reference to security, Data Controllers must be satisfied that the CSP will only process personal data in accordance with its instructions. Further data protection guidance on engaging with CSPs is available through the data protection website.[12]
	b. Role of CSP as Data Processor / Data Controller	1. Where procurement of cloud services is being considered, the PSB should consult with its Data Protection Officer and legal advisors in relation to the most appropriate provisions covering the CSP's Data Controller activities.	1. CSPs should only be Data Processors, although, in some more complex scenarios, CSPs may also be Data Controllers or joint Data Controllers. PSBs should always refer to legal advisors and their Data Protection Officer in relation to the Data Processing activities which will be allowed by CSPs and the obligations that CSPs will be required to meet in this respect.
	c. Data Subject Access Rights	1. The PSB Services Contract should ensure that the PSB, as Data Controller, should either have access to the CSP environment to perform processing operations that are necessary to implement Data Subject rights or the CSP should react without delay to any PSB instruction relating to a Data Subject request.	1. The PSB, as Data Controller, should ensure that they can comply with the GDPR requirement to implement Data Subject rights (to access, rectify, block or erase personal data).
	d. Derived Data	1. The PSB Services Contract should specify what types of derived data, if any, may be generated (including "metadata") and clearly identify the owner of that data.	1. It is not entirely clear who is responsible for data emanating from relationships between CSPs and the PSB in cloud services; for example, as a result of activities between the PSB and CSP, information of various types such as usage and traffic patterns can be generated, as well as information relating to security information and events. This is sometimes

[11] https://www.dataprotection.ie/en/news-media/press-releases/dpc-statement-cjeu-decision
[12] https://www.dataprotection.ie/sites/default/files/uploads/2019-10/Guidance%20for%20Engaging%20Cloud%20Service%20Providers_Oct19.pdf

Topic	Checklist Item	PSB Considerations	Reasons for PSB Considerations
			provided by the CSP as part of the service dash-boarding and performance reporting under their service level agreements (SLAs) but ownership of the data may reside with either the CSP or the PSB. The nature and type of data which may be generated should be made known by the CSP.
	e. Data and Software Access In the Event that the CSP Ceases Trading	1. The PSB Services Contract should specify the CSP's obligations in relation to data backup and providing the PSB or its agents' access to data for the purposes of downloading and migrating the data to another CSP. Where the data is under the CSP's control, the PSB could consider using a trusted third party as a recipient of CSP data backup copies in order to mitigate the risk of being unable to access data in the event of the collapse of the CSP or other catastrophe which would render the CSP unable to continue to provide the services. The PSB should consider any cost implications related to this approach. 2. The PSB should consider the context in which the software and data are to be provided and whether software escrow would be a viable option: – for SaaS, it is unlikely that SaaS escrow will be a viable option; – for PaaS services, the responsibility for applications may be shared, in which case escrow for the software which is installed on the platform may be a viable option; – for IaaS, software escrow for the software which is installed on the infrastructure is a definite option as the CSP will be providing infrastructure and the software applications will be under the control of the PSB. The PSB's escrow contract would be made directly with the third party software provider (generally, using a trusted escrow agent).	1. In the event of a CSP, or one of its Sub-contractors, ceasing to trade due to examinership, receivership or liquidation, the PSB will require access to its data to enable migration of the service to a replacement CSP or back on-premises. This should be provided for in the PSB's disaster recovery and business continuity planning and should align with the CSP's data backup and restore processes. If using IAAS or PaaS cloud services, the PSB may have some control over data backups. Where the CSP is providing SaaS cloud services, the PSB will have much less control over data backups. Specific arrangements may require to be implemented to enable data backups to a third party, agreed between the parties, so that data access will be affirmed in the event of the CSP ceasing to trade. 2. When compared to on-premises software agreements, SaaS software escrow is generally not a practical option due to the complexity of SaaS cloud software environments and the co-existence of the software and data. Market analysts indicate SaaS escrow is not a common practice and is cost prohibitive. SaaS providers are generally reluctant to provide software escrow. From a practical point of view, SaaS software applications are complex and may be built with third party or open source software components, are updated on a continuous basis and would create significant implementation and ongoing maintenance challenges for a PSB.

Topic	Checklist Item	PSB Considerations	Reasons for PSB Considerations
	f. Other CSP Data Protection Obligations	1. The PSB Services Contract should specify the services and support required to enable the PSB to fulfil its obligations in relation to data access requests. Data migration/portability requirements in order to facilitate the migration of data to another CSP, if required, should also be defined. 2. The CSP's incident management processes should be clearly defined in the PSB Services Contract and be compliant with relevant EU regulations and directives, including notification of incidents or security breaches to the PSB (for example, ENISA Cloud Security Incident Reporting framework[13]). 3. The PSB Services Contract should specify that PSB consent is required regarding the use of data Sub-processors by the CSP.	1. The CSP should provide support for data subject access requests in a shared responsibility scenario; for example, fulfilment of data subject access requests would be the PSB's responsibility and CSPs would be required to provide capabilities and tools to facilitate the fulfilment of access requests to the PSB. These capabilities should include data portability between CSPs for customer data only, data deletion and provisioning of support. 2. Definition of security incident or breach should be based on EU regulations and directives such as GDPR and NIS. Requirements for notification by the CSP to the PSB of incidents or breaches should be compliant with Data Protection obligations (including GDPR). 3. The use of data Sub-processors by the CSP should be carefully reviewed and express consent required from the PSB for their use.

[13] https://www.enisa.europa.eu/publications/incident-reporting-for-cloud-computing

Contractual and Commercial Considerations – Section 2

Topic	Checklist Item/Question	PSB Considerations	Reasons for PSB Considerations
Warranties	Types of Warranties	1. The PSB should consider the rationale for and the relevance of each warranty it requires the CSP to provide. In general, the PSB Services Contract should specify the warranties that are required and remedies that will apply in the event that such warranties are breached. The PSB Services Contract should specify the CSP's obligations to comply with any warranties required, as well as any specific warranties related to the quality and performance of the services which are to be provided (for example, system availability and performance). 2. When drafting the tender documents, the PSB should specify that the CSP will be required to warrant that fault tolerance, resilience and redundancy will be in place for the cloud service provided by the CSP. 3. The PSB should carefully consider the nature and form of warranty provisions in its cloud PSB Services Contract and any proposed warranty exclusions; these may vary depending on whether the cloud services required are IaaS, PaaS or SaaS. The PSB's legal advisors may need to be consulted in this regard.	1. The general warranties provided by CSPs under cloud services agreements include: – compliance with all applicable laws and regulations in relation to the operation of the CSP's business insofar as it relates to the cloud services being provided, the PSB's data and PSB's use of the cloud services; – provision of the cloud services in accordance with good industry practice (for example, in substantial conformance with the services documentation and in accordance with the levels of skill and care expected of an organisation providing similar services); – system availability in accordance with the availability metric in the SLA. 2. It would be unlikely, for example, for a CSP to warrant that a SaaS software solution will be defect free; however, it is normal for a warranty for software to state that the software will operate in accordance with the user documentation. Some CSPs may limit the duration of this warranty while others may provide this as an unlimited duration warranty (or unlimited for the duration of the contract term). 3. CSPs will generally include a warranty disclaimer which will exclude all warranties or representations other than those expressly included in the contract.
Interoperability and Cooperation	Interoperability with PSB network and pre-existing infrastructure	1. The PSB should make provisions in the tender documents and the PSB Services Contract to ensure that the CSP warrants that the XaaS solution will function as specified with the existing PSB	1. This warranty is required to ensure that the cloud service will operate in conjunction with the PSB's existing network and any hardware or other infrastructure which is in place. Failure to address this could result in interoperability issues down the line which the CSP may rightfully claim do not form part of the

Topic	Checklist Item/Question	PSB Considerations	Reasons for PSB Considerations
		network and any pre-existing infrastructure which is not in the scope of the procurement project.	CSP's service obligations. This, in turn, could lead to unforeseen service outage or performance issues and/or the incurring of additional costs or charges to resolve them.
	Cooperation with Third Party Suppliers	2. The PSB should explicitly call out in the tender documents and in the PSB Services Contract any PSB third party suppliers to be considered when procuring the XaaS solution and the nature of the cooperation required with them. For example, the PSB may have ICT support arrangements in place with a third party or may have elements of its business outsourced to a third party who require access to the XaaS solution.	2. This provision would place an obligation on the CSP to engage with relevant third parties in order to ensure that the end-to-end service delivery chain is clearly defined. Where cooperation with third parties is needed to ensure the service operates as intended, the CSP will be obliged to cooperate with them as required. The nature and scope of the specific cooperation requirements should be clearly set out in the relevant tender documents and the PSB Services Contract.
Indemnification	Indemnities and Links to Insurance Levels	1. Legal advice and/or the advice of the State Claims Agency should be sought when setting out the indemnities and associated insurance levels in the PSB Services Contract. 2. The tender documentation should clearly set out the indemnities, insurance types and insurance levels required.	1. The indemnities provided by CSPs will vary. Some CSPs will link indemnities to insurance levels[14]. 2. The nature of the indemnities to be provided by the CSP and associated liability limits should be clearly set out in the PSB Services Contract. Cyber insurance is a key consideration for cloud services contracts. The cyber insurance may cover the gap between the liability limits set out in the RFT and the costs resulting from a data loss. **NOTE:** It is important to note that not all CSPs are in a position to modify their terms and conditions. PSBs should always seek the advice of their legal advisors in relation to any conflicts between their published terms and conditions and those of the CSP.
Liabilities	Limits of Liability	1. For all questions and advice relating the topic of indemnities and liabilities, PSBs should conduct appropriate risk assessments and seek the advice	1. Limitations on liability can be contentious if they extend beyond the CSP's normal limits. The types of indemnities and associated liabilities will generally be set out in the CSP's standard terms and conditions and the CSP may or may not

[14] PSBs should consult with the State Claims Agency regarding insurance levels; for information regarding insurance levels, refer to https://stateclaims.ie/news/state-claims-agency-general-indemnity-scheme-launches-new-guidance-document-for-insurance-and-contractors

Topic	Checklist Item/Question	PSB Considerations	Reasons for PSB Considerations
		of the State Claims Agency and/or their legal advisors, as required.	be agreeable to change these. PSBs should note the following: – general liability caps will normally be based on the value of fees paid for the services in a period, or a multiple thereof; – in certain instances, CSPs may agree to "carve-outs" to cover specific events or liabilities. **NOTE:** As noted above, not all CSPs are in a position to modify their terms and conditions. PSBs should always seek the advice of their legal advisors in relation to any conflicts between their published terms and conditions and those of the CSP.
Use of Contractors	Prime/Sub-contractors	1. The PSB Services Contract should specify the CSP's obligations in relation to the use of Sub-contractors and should, ideally, list all Sub-contractors. 2. The PSB Services Contract should set out clearly that the obligations for the Sub-contractors in relation to key obligations such as security and data protection compliance will be no less onerous than those that apply for the CSP itself and the CSP must be held responsible for the acts and omissions of its Sub-contractors. 3. The PSB Services Contract should clearly set out the roles and responsibilities of the CSP and any other entity which may act as a lead or prime supplier for a project. **NOTE:** Sub-contractors may be added, removed or replaced during the course of the contract.	1. CSPs may use Sub-contractors for the provision of services and this is often not visible to the PSB. In some instances, CSPs may agree to list the Sub-contractors used in the provision of the services, thereby enabling PSBs to assess the implications of the sub-contract arrangement. 2. The obligations relating to the performance of the services by Sub-contractors (and, in particular, as they relate to security, compliance with applicable legislation etc.) should be no less onerous than those applying to the CSP. This would provide further assurance to the PSB in relation to the obligations of Sub-contractors. 3. In some instances, an entity other than the CSP (for example, a Systems Integrator) may "prime" the implementation and support of services. Where relevant, the PSB Services Contract should address this to ensure that the obligations of the CSP are not diminished by the involvement of a Systems Integrator to lead the services implementation project or its subsequent first/second level support of services post-implementation.

Topic	Checklist Item/Question	PSB Considerations	Reasons for PSB Considerations
Data Retrieval Charges	Data Retrieval Costs	1. The PSB Services Contract should call out explicitly what data downloads will be provided by the CSP, whether these downloads are to be provided free-of-charge (or not). The PSB Services Contract should also clearly set out the basis for charging for any data downloads which are not provided free-of-charge. The PSB Services Contract should also specify any related limitations on data downloads.	1. Data downloads and related costs should be clearly set out. PSBs should ascertain if downloads will be provided free-of-charge or will be subject to a charge (for example, a number of downloads may be facilitated on a free-of-charge basis per year and any downloads required in excess of that may be chargeable). Any prospective limitations that may apply with regard to how much data can be downloaded per day should be agreed and clearly specified.
Confidentiality	Confidentiality Provisions	1. PSBs should ensure that there are adequate confidentiality provisions in their PSB Services Contract with the CSP and should seek legal advice as required.	1. Confidentiality provisions must be included in the PSB Services Contract with the CSP.

Contractual and Commercial Considerations – Section 3

Topic	Checklist Item/Question	PSB Considerations	Reasons for PSB Considerations
Pricing Models	a. Pricing Transparency / Complexity	1. The PSB Services Contract should include all pricing elements and the basis for calculating charges for the cloud services and any other related services during the contract term.	1. The PSB Services Contract should contain full transparency on the pricing model, consumption units (for example, virtual machine compute pricing, storage price per GB/TB by storage tier, offline storage pricing per GB/TB, number of users, number of transactions, professional services resource pricing by resource type). Normally, this will be set out in a pricing addendum to the contract. The CSP's Order Form will likely contain the pricing breakdown for the contract based on the scope of requirements defined through the tender process.
		2. Where feasible, the PSB should consider immediate service requirements as well the service volumes and associated pricing that are likely to apply over the contract term.	2. Upfront capacity planning by the PSB is a necessity, not only to address the initial scope and usage requirements but should also contain a profile of planned usage by service component over the contract term.
		3. The PSB should be adequately informed in relation to CSP pricing regimes and any related factors that require to be considered in order to complete a comprehensive TCO analysis.	3. Because of the complexity of pricing for cloud services, it is essential that the PSB conducts research on the service consumption and pricing models that apply in the cloud services market that is the subject of the tender. To achieve this clarity, PSBs should consider using the services of independent cloud experts and solution architects (including cloud broker services) to identify the pricing model and likely cost elements based on the PSB's requirements.
		4. If necessary, independent expert advice should be sought to assist in understanding complex CSP pricing models.	4. The PSB should have sufficient transparency on how pricing is calculated by the CSP over the lifetime of the PSB Services Contract (lifecycle costing) to enable alignment with a TCO assessment. CSPs may propose different pricing models which can be difficult to evaluate fairly on a like-for-like basis. The PSB should understand that many SaaS licensing models may provide multiple pricing options and will likely migrate to alternative metrics over time (for example, Robotic Process Automation pricing which may be based on process inputs, process outputs or business outcomes).

Topic	Checklist Item/Question	PSB Considerations	Reasons for PSB Considerations
		5. The PSB should consider renewal pricing factors to provide certainty in relation to likely costs in the event that the PSB wishes to renew the contract after the initial term. PSBs should consider limiting any price increase after the initial contract term to the applicable Irish CPI rate or a set percentage. Ideally the increase should be limited to the lower of the two. 6. PSBs should clearly call out the pricing model(s) they require, including the metrics relating to same, in the tender documentation.	5. Cloud service pricing must be aligned to the contract term and, on renewal, if applicable, at the end of the contract term, any subscription price uplift should be limited (for example, "then-current CPI rate in Ireland or 3%, whichever is the lower"). 6. As noted above, CSPs may propose different pricing models which can be difficult to evaluate fairly on a like-for-like basis,
	b. Cost Metrics	1. The PSB should ensure that the PSB Services Contract addresses the pricing regimes for the immediate services and, where feasible, any further services that may be required during the contract term, ideally through a services rate card. The tender documentation should specify all elements of the support services costs, which should be aligned with support service levels set out in the SLA to be incorporated into the PSB Services Contract. Overall, PSBs should ensure certainty in their PSB Services Contract with the CSP regarding the factors which may impact cost over the term of the contract.	1. There are many cost elements and metrics involved in cloud service contracts that should be considered upfront. These include, but are not limited to: – deployment and configuration costs; – ongoing management of SaaS, in particular in relation to usage of data and other price-sensitive components of the service (such as CPU usage, storage etc.); – support costs (for example, to achieve the required service levels, a premium support offering may be required which will be provided at a premium to the standard support charges); – APIs (which may, for example, be charged on a per transaction basis, as opposed to per API); – custom objects (which can include cost of development, test and integration, as well as the cost of custom maintenance over time); – "sandboxes" (for example, test environments and the cost of resources such as software licences, storage and compute capacity and capabilities to be deployed within those environments); – online and offline storage costs; – resource consumption limits and incremental costs associated with exceeding them; – costs associated with resolution of integration issues and problems;

Topic	Checklist Item/Question	PSB Considerations	Reasons for PSB Considerations
			– data migration costs to extract and transform data before it can be used in a cloud service environment or application.
	c. Time-based Pricing Benefits	1. Many CSPs provide their services using a "pay as you go" model which may be appropriate in certain circumstances to meet particular project requirements. Depending on the circumstances, PSBs should also consider the benefits of pricing discounts associated with fixed, longer-term contract commitments against the potential restrictions relating to CSP commercial lock-in resulting from a longer term. 2. The PSB should consider any CSP pricing offerings against its business case and budget (for example, considerations in relation to capex and opex spend and lifetime TCO).	1. A key metric for CSPs is lifetime customer value. The quantum of services and duration for which the services are consumed are key positive influencers on this metric. CSPs will generally offer attractive pricing for the services in return for a longer term contract. 2. PSBs should consider beneficial pricing offerings against the prospect of CSP commercial lock-in and inability to move (without incurring significant cost) to alternative CSPs during or at the end of the contract term. PSBs should also consider the duration of the contract in the context of Public Procurement Regulations and guidelines to ensure the contract duration does not restrict competition in the market.
	d. Penalties and Pricing Realignment with Usage	1. PSBs should ensure that they fully understand the commercial usage regimes (and related penalties for non-compliance) that apply to the cloud services they are procuring. 2. The PSB Services Contract should adequately address the PSB's immediate requirements and provide clarity around the effect of any increases or decreases in the cloud services over time and how these will be handled commercially. The PSB Services Contract should deal with temporary variations in demand.	1. PSBs need to be aware of any additional service usage or SaaS compliance costs and ensure, for example, that their operational processes protect against SaaS compliance penalties. This may be regulated to some extent by the involvement of the CSP in limiting usage, rather than the CSP allowing unlimited usage and charging for it after the fact. 2. PSBs should only pay for the services they are contracted for. However, where usage exceeds the contracted values, a "true-up/true-down" mechanism may be used to deal with variances against the contracted values. PSBs should consider the following: – it is often the case that the CSP may allow the PSB to scale subscriptions up dynamically and as required (often as a "true-up", subject to additional fees) but may

Topic	Checklist Item/Question	PSB Considerations	Reasons for PSB Considerations
			only scale down at the end of a contract year ("true down"); – PSBs should ensure that burst activity (e.g. peaks at year end) will return to normal levels after bursts are catered for.
		3. PSBs should ensure that, ideally, any increases in services consumption should be specifically agreed in advance so that inadvertent incurring of additional, unbudgeted costs are avoided.	3. Cloud services are sometimes delivered as "self-management" capabilities (for example, Backend as a Service - 'BaaS') where the CSP provides fully managed services to run and deploy applications. These need to be considered carefully in terms of incurring inadvertent additional costs from over-utilisation of unlimited services.
	e. Cloud TCO	1. Total cost of ownership assesses the lifetime costs of procuring a cloud services solution. All relevant cost components and factors (opex and capex) that may apply across the term of the contract should be considered when assessing the total cost of cloud services.	1. Cloud total cost of ownership (TCO) should be considered from a number of perspectives, including: – initial implementation costs, including data migration; – ongoing subscription /consumption costs; – additional backup / storage / encryption costs; – termination costs (this may be particularly significant in the event of early termination) and exit costs.
Other Contract Considerations	a. Non-Diminishing Services	1. The PSB Services Contract should explicitly contain all terms and conditions; this would entail not relying on URL-linked terms and conditions which may be subject to unilateral change over time. Where CSP terms and conditions are located at a URL, PSBs should take care to download the content of the URL and include it in the contract.	1. PSBs should consider any elements of the CSP Agreement that may be linked to URLs. All terms and conditions should be called out (downloaded from the URL, if required) and set out explicitly in the signed contract. PSBs should not accept any changes on the basis of URL-linked content changing. This provides protection against the possibility of service functionalities being re-bundled, unacceptable changes to service levels or other terms and conditions which may pose potential risk for PSBs.
		2. The PSB Services Contract should stipulate that "click-through" agreements must not apply and should be disabled. However, if click-through agreements are unavoidable, the PSB should ensure that its PSB Services Contract takes precedence over potentially conflicting click-through terms and conditions.	2. Click-through agreements should not be acceptable unless the main PSB Services Contract takes precedence over any potential conflicting terms.

Topic	Checklist Item/Question	PSB Considerations	Reasons for PSB Considerations
	b. Force Majeure	1. The PSB Services Contract should specifically state which events will result in force majeure and stipulate that a force majeure event does not exist unless, for example, both the primary and secondary systems have failed. 2. PSBs should refer to the standard State contracts for standard force majeure provisions and seek legal advice as required.	1. PSBs should ensure that force majeure is adequately defined. For cloud services, force majeure provisions should specify that a force majeure event does not exist unless both the primary and secondary systems have failed. A clear and concise definition of force majeure will ensure that it is not used as a "catch all" reason for excused performance. 2. Other elements of force majeure will be set out in the standard State contracts.
	c. BYOL (Bring-Your-Own-Licence)	1. PSBs should have an awareness of the quantity and type of pre-existing licences which may be required to migrate to the cloud. PSBs should ensure that the on-premises to cloud conversion mechanisms are clear and how on-premises legacy licence support regimes will be replaced, for example, by licence subscriptions in the cloud. PSBs should seek expert advice (including from their legacy software providers), if necessary, to ensure clarity on these complex topics.	1. Many CSPs allow for third party licence migration from on-premises to the cloud. PSBs need to be aware of the entitlements and limitations in relation to this, including: – where licences can be moved; – for legacy systems, any permitted transfer of pre-existing licences in the cloud where migration to PaaS or IaaS is contemplated; – any restrictions or additional pricing which may apply where on-premises software licences are being moved into a cloud environment; – how to calculate the conversion ratios (for example, on-premises licensing models to cloud variants); – do single usage (on-premises or cloud, but not both) or dual usage (both on-premises and cloud) rights apply; – any time limitation on the migration of licences from on-premises environments to the cloud; – the existence of any software asset management (SAM) tools to monitor usage in order to ensure compliance with the licensing rules and metrics.
	d. Service Levels and Service Credits	1. PSBs should ensure that the services are adequately described and the SLA and key performance metrics are well defined. This should include key operational and performance criteria against which the CSP's performance will be measured, including:	1. Service credits are often the main remedies set out by CSPs for poor or inadequate performance. This requires careful consideration when service level agreements (SLAs) are being defined by PSBs. These considerations should include:

Topic	Checklist Item/Question	PSB Considerations	Reasons for PSB Considerations
		a. responsibility for tracking performance metrics should be clearly set out in the PSB Services Contract;	a. ensure all elements of the services and the SLA are included in the PSB Services Contract and that responsibility for tracking performance is assigned;
		b. service availability parameters should be clearly set out in the PSB Services Contract;	b. service availability times should be clear (for example, services must be available on Irish working days, even if these are bank/public holidays in the host country);
		c. planned and unplanned downtime should be clearly defined and, where relevant, any unplanned downtime should be notified in a timely way (for example, 3 to 5 days advance notification required for any unplanned maintenance). Downtime should not include scheduled or emergency maintenance;	c. "planned downtime" (as well as planned and unplanned maintenance) needs to be clearly defined (including whether limited access to functionality may be available during planned downtime), as well as definitions of such terms as "micro outages";
		d. ensure clarity in the PSB Services Contract regarding "carry-over" of planned downtime;	d. planned downtime must not be carried forward from period to period; that is, the planned downtime period is set for a discrete period such as a month and, if not used, should not carry forward to another period;
		e. PSBs should ensure that the PSB Services Contract stipulates that URLs are not acceptable as part of the terms and conditions as these can be unilaterally changed without notice by the CSP;	e. the services terms and conditions should not be subject to change without the PSB's agreement (thus the requirement for caution in relation to URL-linked agreements or provisions in CSP Agreements);
		f. the PSB Services Contract should stipulate the required system "uptime";	f. agree how system availability is defined (this is a key metric and may typically be 99.95% uptime for a "base" service level; however higher uptime/availability measures may be offered/achievable but may incur additional cost);
		g. the PSB Services Contract should ideally set out the incident resolution response and target or aspirational resolution or workaround timelines;	g. incidents, outages and problems must be dealt with by the CSP within defined timescales;
		h. the SLA should include a mechanism for calculating service credits for full or partial service failures and it should be clear and unambiguous.	h. the SLA must state if service credits apply in the event of incidents or unplanned downtime for total service or elements of it (for example, a subset of users). Many CSP

Topic	Checklist Item/Question	PSB Considerations	Reasons for PSB Considerations
		The PSB Services Contract should address the consequences of persistent failures and whether these may lead to contract termination rights;	SLAs will not include incident resolution times as a key performance metric, although some Tier 2 or Tier 3 CSP SLAs may allow them (and workaround time may be counted as part of the incident resolution time);
		i. the PSB Services Contract should clearly define the responsible party for software upgrades and updates. For example, for IaaS services, the software may be under the control of the PSB and no CSP responsibility would apply; however, SaaS, and to some extent, PaaS, services would result in some or all responsibility for software updates sitting with the CSP. The SLA should state, for example, that security updates must be provided within a defined number of days;	i. SLA provisions in relation to software updates and upgrades need to be carefully considered; for example, upgrades or updates may impact the continued operation of software in PaaS environments whereas SaaS software updates generally occur seamlessly where a single code base for multi-tenanted usage is employed by the CSP;
		j. PSBs should ensure that the SLA in the PSB Services Contract clearly states how many versions of the environments, operating systems and/or application software will be supported by the CSP. The PSB Services Contract should clearly define the parties' obligations relating to version currency.	j. the SLA must explicitly state how many versions of the environments / operating systems and application software will be supported (e.g. n, n-1, n-2, where "n" is the most recent version).
	e. Software Upgrades and Updates	1. For SaaS contracts, the PSB should understand the key differences between software customisation and software configuration regimes, which may be quite different to those applying to on-premises software. 2. For non-SaaS CSP services, the PSB should understand fully the software implementation activities and whether CSP resources will be required to support the implementation and acceptance of software into the cloud services environment, as well as the version management procedures that will apply over time.	1. It should be noted that customisations are generally not provided in SaaS environments (any "customisations" are generally delivered through configuration tools). 2. For SaaS, the upgrade and updates timing is dictated by the SaaS CSP. PaaS and IaaS upgrades are generally potentially less impactful unless there are changes to the operating systems, drivers or other components which may affect the functionality of PSB software.

Topic	Checklist Item/Question	PSB Considerations	Reasons for PSB Considerations
		3. The PSB Services Contract should set out any UAT procedures and the basis upon which UAT resources and services will be provided and charged by the CSP. In addition, the PSB Services Contract should clearly state how often upgrades will be required, the version currency (e.g. n, n-1, n-2 where n is the most recent version) that will be supported by the CSP and for how long.	3. For non-SaaS environments, PSBs should consider the following: – user acceptance testing (UAT) is generally required as a component of software implementation projects; – CSP resources required for UAT will likely be chargeable; – PSBs should have clarity as to how many non-current versions the client may be able to stay on (e.g. n, n-1, n-2 where n is the most recent version) for a limited period of time.
	f. Change of Legal Entity (Novation of contracts)	1. PSBs should carefully consider the impact of change of legal entity (e.g. change of government department name) and seek legal advice to ensure these provisions are drafted adequately, particularly as they relate to formation and re-formation of Government departments or agencies. The right to assign the benefits of the agreement between PSBs is desirable to ensure that reorganisation of PSBs does not inadvertently lead to a dilution of benefits.	1. PSBs should ensure that the PSB Services Contract provides adequate protections where a PSB changes its legal identity (for example, agreement that any replacement legal entity shall have the same entitlement to use the services and an agreed pricing model will apply to cover any additional usage charges). This should also address rights of assignment by either party.

Contractual and Commercial Considerations – Section 4

Topic	Checklist Item/Question	PSB Considerations	Reasons for PSB Considerations
Other General Topics Relating To Cloud Services Acquisition	a. Distinction between Tier 1, Tier 2 CSPs, Resellers and Systems Integrators	1. PSBs should understand the "tiered" market ranking of CSPs and the role of Resellers and Systems Integrators in the market, as well as the context and structure of their CSP Agreements. 2. PSBs should have an understanding of the typical contracting structures that apply and how the different parties (CSPs, Resellers and System Integrators) interact and come together to deliver cloud services solutions. 3. The PSB Services Contract should adequately address any risks inherent in Reseller / Systems Integrator / Sub-contractor arrangements. Expert and/or legal advice should be sought for assistance in respect of any proposed or potential sub-contracting arrangements.	1. CSP Tier 1 includes "Hyperscalers" and it should be noted that their CSP Agreements tend to be quite broad and all-encompassing. CSP Tier 2 includes other global suppliers and their CSP Agreements may be less comprehensive than the Tier 1 CSPs. 2. Resellers are more open to changing agreement terms and conditions in many cases as they "broker" the deal and may accept risk which the PSB is passing to them without passing the risk on to the CSP. 3. Systems Integrators tend to have their own terms and conditions under which they contract (professional/consulting services agreement, support services agreement etc.); these are often augmented services to those provided by the CSP (for example, the Systems Integrator may provide in-life support services for support levels 1 or 2 and interact with the CSP for level 3 support). Care should be taken when implementing Reseller or Systems Integrator arrangements that they do not conflict with or undermine the provisions in the PSB Services Contract.
	b. "Most Favoured Nation"	1. PSBs should carefully consider whether this is a provision that should be part of the PSB Services Contract or whether it may lead to an unfair expectation of tender respondents.	1. Some CSPs may agree "most favoured nation" provisions with some government or very large customers. These provisions generally state that the customer terms are no less beneficial than those provided to other customers. However, Tier 1 / Tier 2 CSPs are unlikely to agree to those provisions for most customers. Resellers or System Integrators, on the other hand, may be more flexible around this topic.
	c. IPR Provisions in State Contracts	1. PSBs should have a good understanding of the role of intellectual property rights (IPR) in cloud services and, in particular, SaaS.	1. The creation of IPR is dependent on the cloud services context. For example, some SaaS providers provide development/configuration tools for clients to develop their own applications in the cloud. In line with the policy of

Topic	Checklist Item/Question	PSB Considerations	Reasons for PSB Considerations
			maintaining a single instance/multi-tenant design, SaaS providers do not allow modifications to the code base and any modifications are implemented through configuration tools to maintain the integrity of the underlying code base.
		2. PSBs should consider as a matter of policy whether customisations will be allowed or whether the only adjustment to out-of-the-box (OOTB) features and functions will be by way of configuration, using the CSP-provided configuration tools which are designed to maintain currency with the underlying SaaS code base.	2. Where software customisations are facilitated by cloud services providers, the PSB needs to consider: – the implications of implementing customisations; – who will own the IPR in the customisations; – the effect it may have on the support regime that may be required to maintain the customisations; – the issues that may arise in terms of restrictions on availing of future updates/upgrades due to the effort and cost of re-engineering the customisations into later software versions/releases.
	d. Reputational Damage	1. CSPs will generally not accept liability for reputational damage resulting from the use of their services. Therefore, there is a significant obligation on PSBs to ensure that any potential for reputational damage is mitigated as fully as possible. This should include: – ensuring robust and comprehensive provisions exist in the PSB Services Contract to address data security and data protection breaches; – inclusion of comprehensive and robust SLAs that enable enforcement of remedies such as service credits when breaches occur.	1. PSBs need to consider the State's responsibility and potential exposure to risk if adverse events occur in relation to Data Protection and Data Security. The indemnities and liabilities in the PSB Services Contract will generally reflect the remedies available in the event that adverse events occur.
		2. PSBs should satisfy themselves that CSPs are appropriately certified in relation to their XaaS services. Refer to the OGCIO Guidance note for further information relating to CSP certification.[15]	2. CSP internal policies, processes and certifications to such standards as ISO 20000 (IT Service Management), ISO27001 (Information Security Management), ISO 27017 (IT Cloud Security), ISO 9001 (Quality Management Systems) and ISO 14001 (Environmental Management) can provide some reassurance regarding CSP capabilities.

[15] https://www.gov.ie/en/publication/078d54-cloud-computing-advice-note-october-2019/

Topic	Checklist Item/Question	PSB Considerations	Reasons for PSB Considerations
		3. PSBs should satisfy themselves that the CSP is capable of delivering the services in accordance with good industry practice and in accordance with the risk mitigation measures in the PSB Services Contract, with provision for service credits included to incentivise adherence by the CSP to its SLA.	3. The Service Levels for incident management and associated service credits for service failures can provide a commercial incentive for CSPs to ensure adverse events do not occur or, if they do occur, that they are dealt with promptly in line with the SLA.
	e. PSB areas of Specific Caution	1. PSBs should familiarise themselves with the shared responsibilities that apply in the context of cloud services. These tend to vary in accordance with the cloud services context, graduating from the IaaS context (which would entail lesser responsibility for the CSP and more responsibility for the PSB) to SaaS, where the CSP is responsible for delivering an overall solution.	1. In the IaaS model, customers bear responsibility for: – their content; – applications built on the infrastructure; – configurations to encryption and security features, where applicable; and – access controls; but CSPs remain responsible for, and must have the ability to protect and maintain: – the infrastructure and platform; and – the overall multi-tenant environment and services provided to their customers.
		2. PSBs should pay particular attention to the commercial aspects of the services delivery models that CSPs employ and ensure that they have full visibility of the costs of the service and understand the drivers behind those costs.	2. Controlled spending: CSPs should provide reporting, monitoring, and forecasting tools that allow PSBs to, for example: – monitor usage (e.g. CPU, users, transactions etc.) and spend at both summary and granular levels; – get alerts as to when usage and spend hit custom thresholds; and – estimate usage and spend in order to plan future cloud budgets; and these tools should generally be specified as requirements when procuring cloud services.
		3. PSBs should have clarity around the cloud services lifecycle and should develop an understanding of the CSP's cloud services roadmap before contracting for the services, as well as keeping abreast of any planned changes through the	3. CSPs can typically provide a useful timeline of up to 36 months for certain services, with support for those services diminishing over that timeline. Where feasible, these should be addressed in the PSB Services Contract through specific provisions relating to express agreement for any changes to the services.

Topic	Checklist Item/Question	PSB Considerations	Reasons for PSB Considerations
		PSB/CSP governance and relationship management processes. **NOTE:** PSBs must ensure that they carry out a Data Classification exercise before moving to the cloud, in compliance with GDPR requirements.	

Appendix 2: Cloud Services Data Protection Guidelines[16]

Schrems II CJEU Judgment

In PSB Services Contracts, CSPs must comply with their obligations under Chapter V of the GDPR. PSBs must remain aware of the evolving nature of Data Protection legislation, as highlighted by the 2020 Schrems II CJEU Judgment, further described below.

On 16 July 2020, the Court of Justice of the European Union (CJEU) issued a judgement in what has become known as the Schrems II case. This relates to the use of the EU "Standard Contractual Clauses" (SCCs) (also known as "Model Clauses") to govern the transfer of data outside the EU or reliance on the Privacy Shield framework for transfers of personal data to the US. Over 5,000 US organisations are Privacy Shield certified and many of these organisations are global technology services providers, including outsourcing firms and cloud services providers.

As the Privacy Shield framework has been deemed invalid for the transfer of personal data between EU and US organisations, the CJEU judgment imposes a significant burden in relation to the use of the Standard Contractual Clauses. While the use of SCCs remains valid as a mechanism to govern the transfer of personal data outside the EU, organisations relying on these Standard Contractual Clauses have a heightened due diligence obligation in relation to their use and individual EU data protection authorities may prohibit or restrict data transfers if they believe the Standard Contractual Clauses will not be complied with.

The Irish Data Protection Commissioner, commenting on the CJEU judgment, stated "it is clear that, in practice, the application of the SCCs transfer mechanism to transfers of personal data to the United States is now questionable. This is an issue that will require further and careful examination, not least because assessments will need to be made on a case by case basis."

Therefore, PSBs will need to ensure that they have appropriate legal advice regarding the implementation of provisions relating to the protection of personal data and the mechanisms which are used to govern the transfer of data outside the EU.

[16] Refer to guidance information from the European Data Protection Supervisor (EDPS) https://edps.europa.eu/