INSERT LOGO

CLOUD SERVICES POLICY

Classification: Internal

This document may only be shared externally to [Company Name] with written approval from the owner.

Version	Approved By	Owner	Date Last Updated	Review Frequency	Next Review	Comments

Contents

Purpose of This Document

This document offers direction for employees adopting cloud-based tools such as CRMs, content management, and collaboration tools.

Scope

The policy impacts all individuals and entities that make decisions regarding implementing Cloud tools on behalf of PRI.

Responsibilities

All staff should comply with this policy and report any breaches to their respective managers or the IT Department.

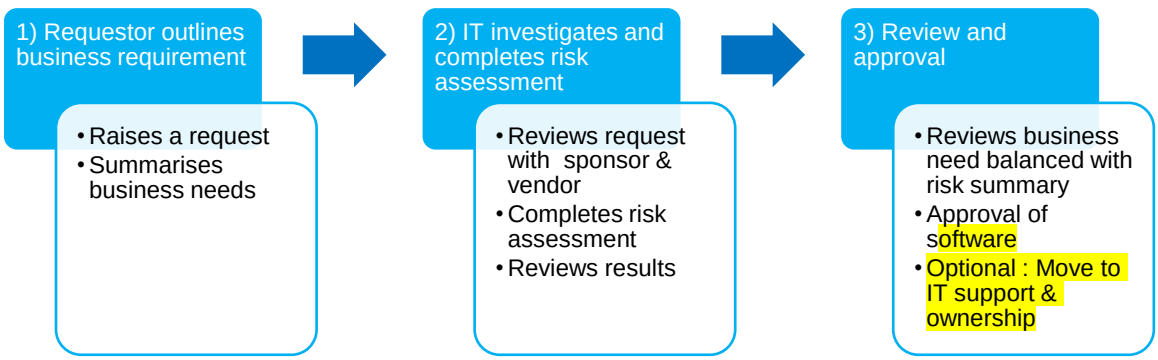
Exceptions

Any deviations from this policy should be formally requested through the IT Helpdesk.

Guidance for Individuals Wishing to Introduce a New Cloud Based Solution

- Those proposing a new Cloud tool should engage with the IT team [insert method here; email, request process, etc]
- IT will evaluate existing solutions for suitability before considering new ones.
- Failing to involve the IT team can lead to several risks, including non-compliance with GDPR.

Process Overview



Step 1 : Business requestor outlines business requirements

It is important for the requestor to summarise the reasoning behind the new Cloud solution so that a holistic corporate view of the business value, security, support, integration, and costs can be taken.

1. The requestor should raise a request using the [insert process here]

2. The IT team will then work with the requestor to document their high-level requirements.

Step 2 : IT investigates and completes risk assessment

3. The IT Team will ensure the Cloud request is then reviewed and prioritised.

   The outcome will either be to decline the request and provide feedback to the requestor on reasoning or assign ownership within the IT team for a more detailed review.

4. A member of the IT team will then perform a review of the Cloud solution, exploring areas such as security, administration, technology, and support.

   The review will complete a R5 - Supplier Performance Review record.

   Each of these areas will be graded as to their potential impact and complexity, thereby highlighting any areas of concern which are discovered.

5. Once all questions have been addressed, it is for the IT staff member to evaluate the overall level of risk to the organisation posed by the introduction of the Cloud service and present their findings to a senior member of the IT team for a final review.

Step 3 : IT Management review & approval

6. Further questions may be asked, but the analysis of Step 2 should provide a solid basis for an informed decision on how the implementation should proceed, and if there be any need for additional controls or support to be put in place.

7. Once approved, the IT member will add the details to the [R6 - Cloud service catalogue].

Guidance for IT Evaluation of a New Cloud Solution

General

- Where possible standardisation of solutions is preferable as duplication of applications that largely undertake the same job can introduce added complexity of support, training, security and costs.

  However, there may be solid reasoning for why another application should be introduced and each request will be reviewed on its own merits.

Legislative Compliance

- All Cloud solutions must adhere to the Information Security Policies
- All Cloud solutions must adhere to legislation and regulation (e.g. GDPR)

Data Security

- Investigate if backups are the responsibility of the customer or if the Cloud solution provides the ability to recover to a point in time as part of the offering. Please note; this differs from High Availability or Disaster Recovery solutions, and ideally puts control in the hands of the [COMPANY NAME] to recover data that may have been corrupted or destroyed by mistake.
- Clarify if there is a disaster recovery approach summarised by the vendor. This may be a full fail-over solution to another site, or high availability and multi availability zones. The level of DR is driven by the level of data security needed.
- Investigate where data is stored geographically. In most instances, this will not be an issue, but if sensitive commercial data or personal data is being processed, it may be of strong relevance as there may be concerns about local legislation or government access to data in certain regions of the world.

Authentication

- Explore if the solution can be easily integrated into existing services to provide single sign on. There are benefits in this including controlling access within IT; any user that is removed through the starters / leavers process will automatically render the Cloud access invalid.
- Multi-factor authentication – If the system can provide MFA, then it should be enabled to provide additional security. This can be using text codes or authentication apps, and ideally standardising on the already existing methods in IT.

Technology & Platform

- If data must be migrated into the system from an existing source, explore how this will happen. For example, are there in-built import / export tools that allow for data to be migrated, or must a third-party add-on be purchased? Depending upon the size and

nature of the data migration, it may be prudent to run a proof of concept, if there is any perceived risk.

- Exporting data in the future should also be evaluated. Does the solution allow for data to be easily extracted, and if so, in what format? Otherwise, there is a potential for vendor 'lock in' whereby it is not possible for [COMPANY NAME] to select an alternative solution in the future.
- If any regular configuration / code / logic changes are to be made to the solution, please identify if a staging or test environment should be established.

Service

- Evaluate if the vendor provides details on service level agreements and availability metrics.
- If the solution is part of a customer facing [COMPANY NAME] service (eg; Assessments) then it should be backed with Service Level Agreements that supports the PRI's service offerings.
- If the expectations for support reside with IT, then the relationship with the vendor should also sit with the IT department.
- Clarify any potentially hidden charges around support, setup, training, onboarding, etc that may impact the costs.

Administration

- If administration (adding, removing users, etc) is to be handled within the business, then expectations must be made clear on regular auditing of users, groups, security rights to ensure that users are not set up and forgotten about, and continue to have access after their need to do so has expired.
- Review how privileged access modes will be handled. For example, will there be one or many administrators of the system? Are there levels of access that should be carefully considered during implementation?