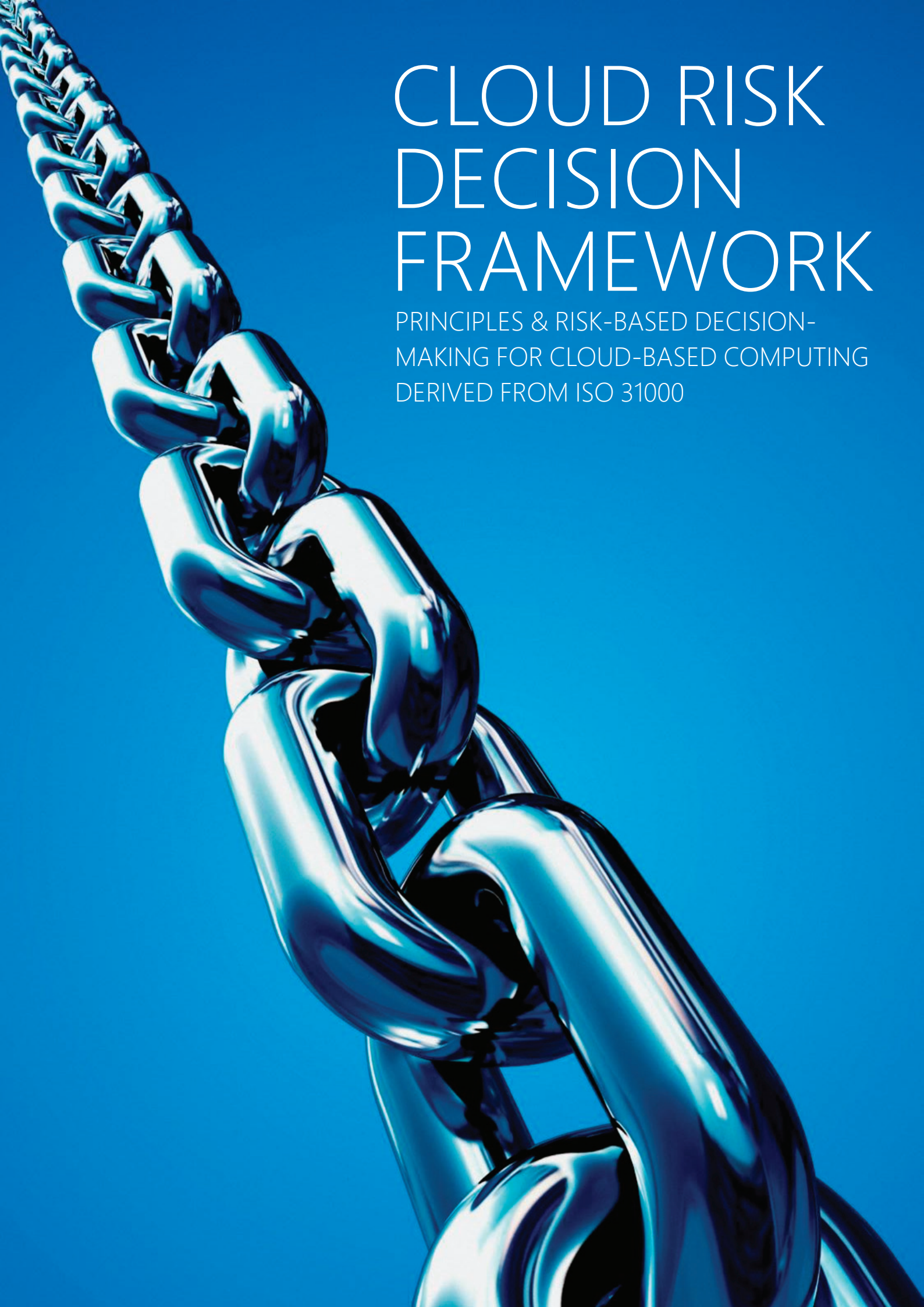

# CLOUD RISK DECISION FRAMEWORK

PRINCIPLES & RISK-BASED DECISION-MAKING FOR CLOUD-BASED COMPUTING DERIVED FROM ISO 31000

# TABLE OF CONTENTS

# INTRODUCTION

## Why use a risk approach for cloud selection?

### *Cloud changes the game – risks change and you need to know how.*

***"Doing nothing may pose the greatest risk of all"***

***Risk management is the effect of uncertainty on objectives***

Many organisations are embracing cloud computing for substantial cost reductions, performance improvements and greater scalability. It allows you to externalise many of the resources previously managed within your enterprise. Unlike traditional outsourcing, which has typically been provided by one or multiple suppliers, cloud computing involves a broad range of suppliers whose varying approaches to security, governance, resilience, availability and privacy create a level of uncertainty for organisations. This creates perceived risk.

There is potential to improve both security and privacy relative to existing deployments. Security has now moved beyond basic perimeter defence against hackers to facing the enormity of well-funded international criminal groups and state-sponsored cyber espionage. Funding and resourcing to mitigate this level of threat is becoming increasingly challenging for all but the largest organisations. On the other hand, cloud operators can amortise security costs over a broad population of users to a higher standard.

It is critical for an organisation to make a balanced assessment because doing nothing may pose the greatest risk of all.

Risk management is defined in ISO 31000 as "The effect of uncertainty on objectives" and therefore externalising IT resources via the cloud, changes the risk profile for the workload and organisation.
This demands a formalised approach to understanding and addressing the risk when considering a cloud-based option.

Currently, many organisations are ill-prepared to identify and weigh-up the risk landscape associated with a cloud option.

This document is part of a set of tools designed to help organisations to objectively identify, analyse, assess and determine potential risk treatment alternatives for many business risks related to their proposed cloud strategy, and to provide value to this decision-making process.

# The specific focus for this guide

## *To help you make a decision about a candidate cloud project.*

This document and its accompanying tools are not intended to replace a comprehensive Enterprise Risk Management practice within an organisation. Rather, they serve as support in the decision-making process as per the Risk Management best practice guidance outlined in ISO 31000.

A good number of organisations do not operate an Enterprise Risk Management program. Risk associated with ICT deployment and operations is largely controlled through the rubric of 'information security'. When environments operate within a contained enterprise and are slow-moving, security provides a logical proxy for IT risk management. However, when direct organisational control of IT assets is diminished and shared along an elongated supply chain that extends beyond the enterprise, a more holistic and formalised means of managing risk must be employed. This is particularly true when dealing with project, or decision-related risk.

Organisations contemplating the use of cloud computing face a decision: operating an existing IT capability within their own IT environment versus a cloud-based alternative. Experience has shown that leveraging cloud computing warrants a broad-based assessment set against both the IT and business objectives. In some cases, the risk profile associated with a move to cloud services will increase, in some cases it will reduce, and in many others, the risk profile will simply change with risks migrating from one domain to another.

This guide investigates how risks increase, decrease or move based on changing IT deployment scenarios. It enables a preliminary business case to be built with reference to the cost, value and risk dimensions.

Although primarily intended to support cloud-based scenarios, the approach is also equally valid for other IT decision making requirements.

**Example case study**

A step-by-step example of how to use the Risk Evaluation Framework has been provided based on a real scenario.

In our example, a government agency, 'Department of Citizen Engagement' (DoCE) was investigating the benefits of cloud computing and discussed specific offerings with several vendors.

The agency remained uncertain about the viability of proceeding to develop a business case due to the perceived risk around their existing in-house capability. They needed an approach which allowed them to balance the cost, value and risk aspects of the cloud proposal in a systematic way that also provided an audit trail for decision making.

In part C, we follow the process used by this government agency to explore the change in risk profile upon consideration of cloud computing and how they arrived at their decision.

# HOW TO USE THIS GUIDE

This guide has been organised to assist IT and non-IT individuals to evaluate potential cloud-based IT capability. No additional training should be required as this guide provides a well-structured process that should be easily followed by a competent business practitioner.

The guide comprises four parts:

| | |
|---|---|
| **Part A** | Introduction to Risk Management process and ISO 31000<br>This section provides you with the 'what', an overview of Enterprise Risk Management (ERM) utilising the international standard ISO 31000. It is intended to provide context and alignment with existing practice in organisations already operating ERM.<br>It also describes the elements required for the evaluation exercise. |
| **Part B** | Using the Risk Framework to evaluate a cloud-based option This section enables you to apply the general principles and process outlined in Part A to the risk assessment of a specific cloud-based project decision. |
| **Part C** | Putting this together: Example Case Study<br>This section helps you understand the 'how' through the use of an example case study.<br>Describe how it works: In this part, we provide a typical example of a cloud-based risk-management review to substantiate the process. |
| **Part D** | Practical Tools<br>The process of undertaking a risk evaluation is helped significantly through the use of tools that provide standardised ways of ordering the process, capturing and analysing information, and evaluating the results.<br>These tools are provided as a set of model templates and available as a companion set of Microsoft Excel files. |

# PART A: INTRODUCTION TO RISK MANAGEMENT PROCESS AND ISO 31000

## What is Risk Management?

This Cloud Risk Assessment Framework is based on the ISO 31000 standard. This section describes the high-level components of the standard, then clarifies the specific parts we will employ and why.

Firstly, how do we define 'risk'? We can frame risk as "the chance of something happening that will have an impact upon the organisation's objectives". It is measured in terms of impact and likelihood. The international standard ISO 31000 sums this up as, "the effect of uncertainty on objectives." Managing this uncertainty is central to the organisation's ability to function.

The international standard ISO 31000 will be used as an umbrella framework in approaching Cloud Risk Evaluation throughout this document. We will also focus specifically on evaluating risk associated with two or more alternative IT capability options.

This section will cover:

- A Risk Framework as informed by ISO 31000 including Principles and Process
- Description of the elements in the program
- The objectives for Risk Management and how these can be applied to Cloud-related strategic decision
- What information/decision the ERM program will yield and what to expect as an outcome

# ISO 31000 generalised risk-management framework approach

The ISO 31000 approach consists of three main parts: a set of principles, a risk lifecycle framework and a process for dealing with risk. Because our focus is on making a decision between competing options, this paper will focus just on the **Process component** of the ISO 31000 standard.

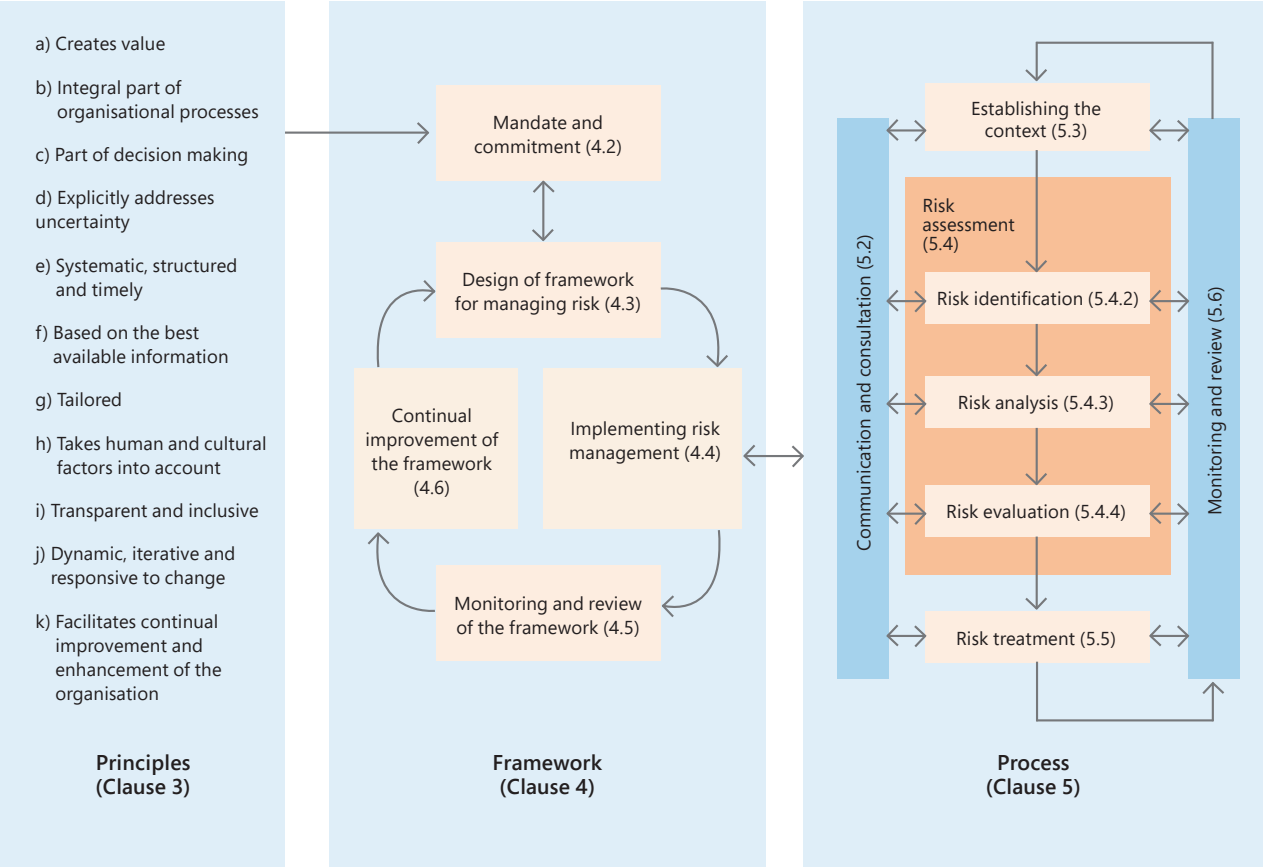


*Figure A-1 – Schematic of ISO 31000 Risk Management*

# Applying the Process

This diagram expands on the 'Process' component and shows the six steps that will be used to evaluate risk for a cloud-services candidate.

We will apply this process to the case study in Section C and optimise each step for the evaluation of a cloud candidate.

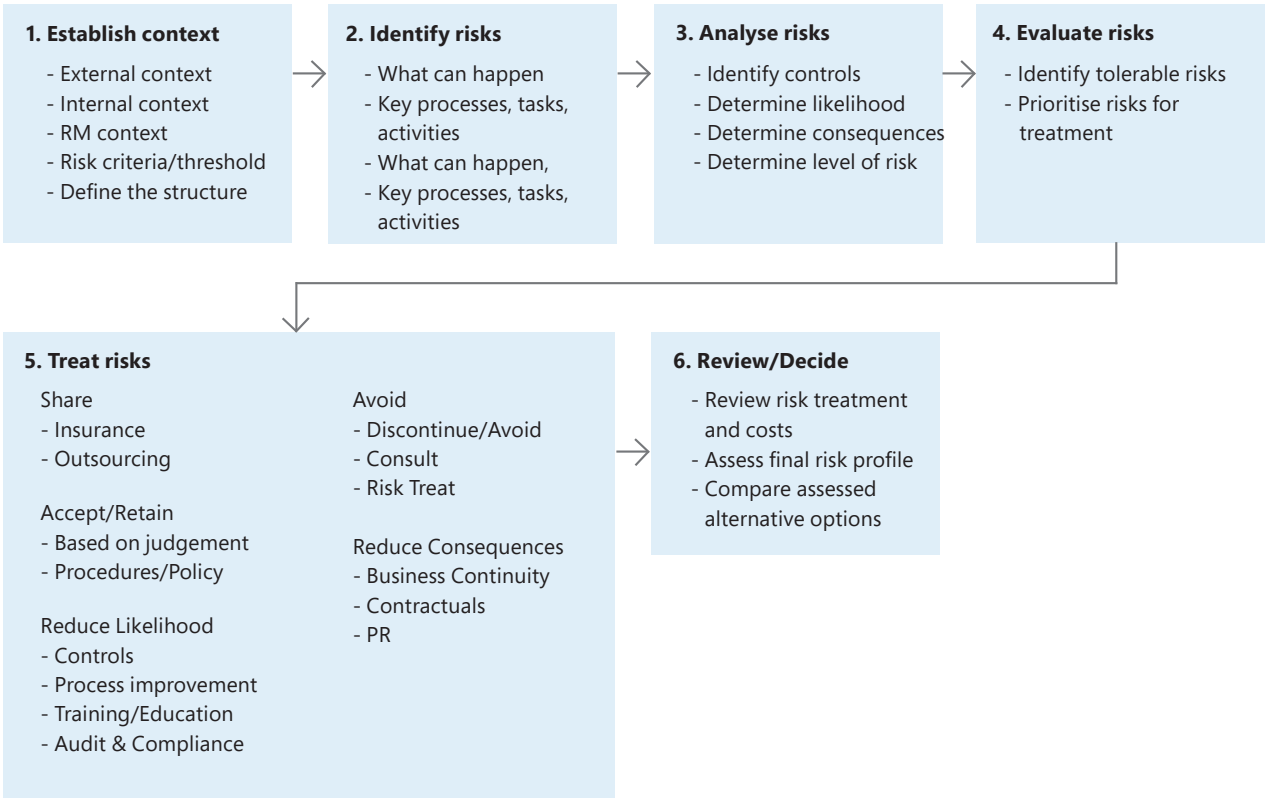


*Figure A-2 – Schematic of ISO 31000 Risk Management*

# PART B: USING THE RISK FRAMEWORK TO EVALUATE A CLOUD-BASED OPTION

Here we use the general ISO Risk process and apply it to the evaluation of a cloud-services option.

## Preparing for the process

The overall process looks like this:

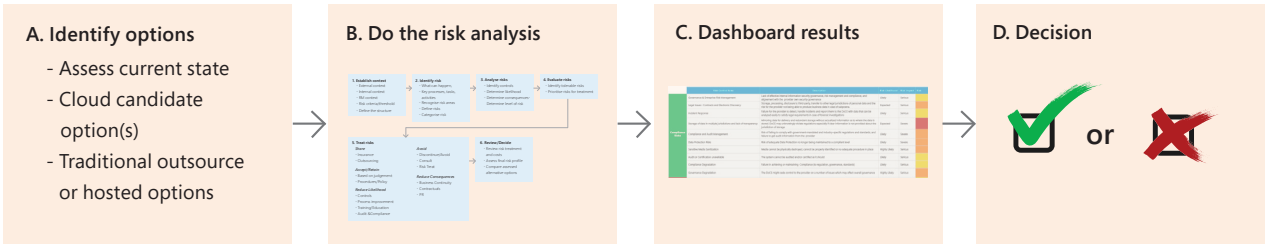


*Figure B-1 – Schematic of ISO 31000 Risk Management*

## Identifying the options

This analysis assumes that the organisation is considering cloud services. It is likely that some form of functionality already operates within the IT department and, where it exists, it should be included in the evaluation along with any other relevant options. It is worthwhile considering the following questions:

1. What capability are we seeking to access?
2. How is this currently delivered and accessed by the organisation?
3. What cloud alternative (Private, Hybrid, Public, etc.) is the target of analysis?
4. Are there other alternatives that should be included – such as non-cloud hosted, for instance?

# Doing the Risk Analysis

## *1. Risk management context*

The purpose of this Risk Management initiative is to assess the potential to leverage a particular IT capability through the use of a cloud-delivered IT service via a third party vendor.

**What is under review?**

The IT capability may involve Communications and Compute infrastructure (Infrastructure as a Service), a full development and run-time platform (Platform as a Service), or a specific application or workload (Application as a Service). A full definition of these descriptions of cloud computing can be found at the NIST site.[1]

Example issues for consideration:

- Understand any changes in the risk landscape resulting from externalising to a Cloud environment IT workloads or systems such as Messaging, Collaboration and Sharing.
- It is necessary to clarify the boundaries of the system being targeted: what it contains; and what it entails, including associated upstream and downstream systems. It is equally important to ensure that the context identifies what is NOT part of the scope of either the discussion or the evaluation.
- The context will establish what is in and out of the boundaries for discussion and evaluation. The context or scope will be documented and serve as input to the risk-assessment process.

**Relevant Government Policy and Regulatory Environment**

What specific government or national legislation or regulation exists that might impact the risk analysis and the scope of choices available.

- Privacy regulations and any technology policy guidelines.
- Any government information access or intercept requirements
- Recordkeeping regulation and guidelines
- Industry-specific security guidance

**Corporate Policy and Guidelines**

Most organisations have some level of guidance for governance and business-level decision-making that should be consulted as context. This may include:

- Corporate social responsibility
- Sustainability stance
- Innovation stance

**Community expectations**

Are there specific areas that demand particular attention such as 'Duty of Care' in the education sector or high-level secrecy in the defence sector?

**Risk Appetite Criteria**

Risk criteria should reflect the things that the organisation determines as important and so will differ between organisations. These should include at least the following:

- Risk appetite: at what point does the risk become unacceptable?
- How will likelihood be defined (e.g. frequency over what timeframe)?
- Definitions of impact and likelihood and their respective measurement scales.

[1] NIST Cloud definitions: http://www.nist.gov/itl/cloud/upload/cloud-def-v15.pdf

**Evaluating Impact and Likelihood**

An accepted way to represent risk exposure in a structured way is through the following formula:

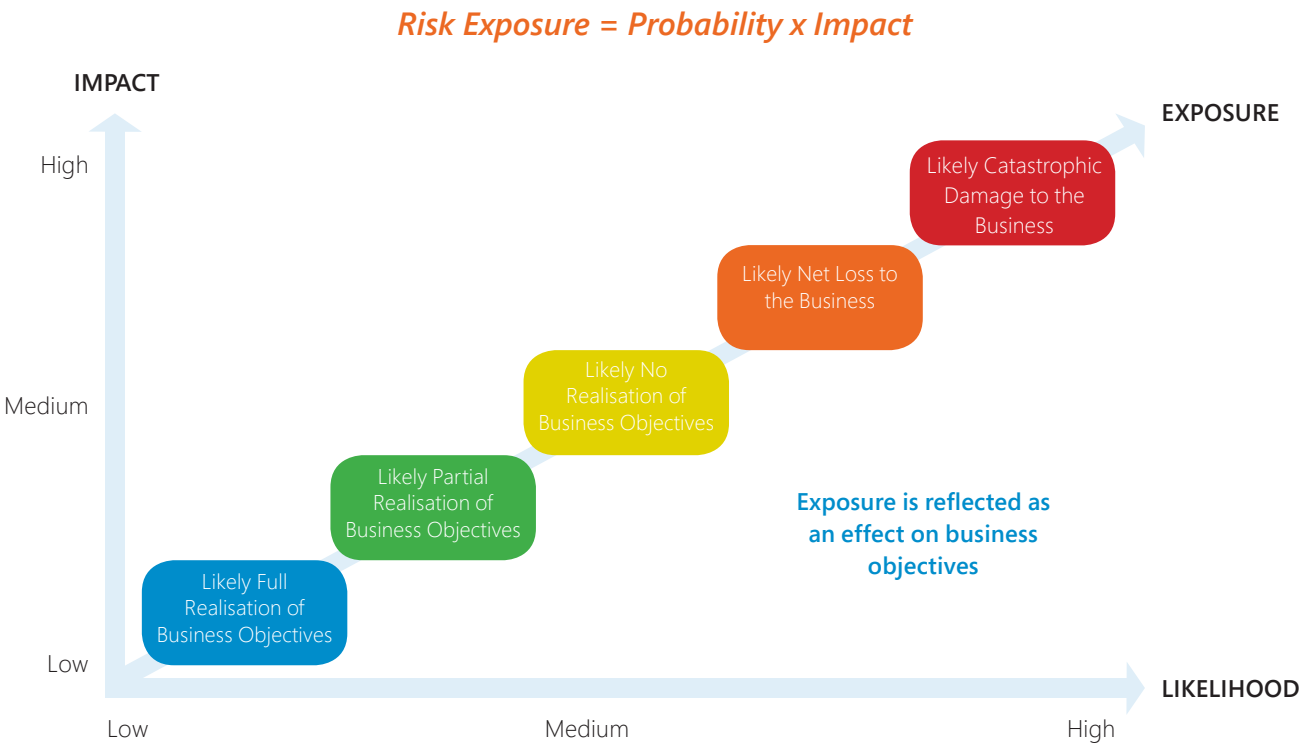


***Figure B-2 – Risk Exposure***

Both Risk and Impact are separately evaluated for each risk domain and the following classifications will be used throughout.

### Risk Impacts

The template below is included in the Excel spreadsheet that accompanies this paper and should suit most organisations with minimal change. It should however be given sufficient thoughts and be endorsed by all stakeholders prior to being used.

| Score | Rating | Definition | Description of Impact | | | |
|---|---|---|---|---|---|---|
| | | | Duration | Organisational and operational scope | Reputational impact on stakeholders (i.e., citizens, civil servants ) | Legal/ Compliance/ Environmental Impact |
| 5 | Catastrophic | Severe or complete damage to asset or reputation e.g. externally visible and affects department's operation and citizen's confidence. Substantial support costs or business commitments canceled. | Significant Recovery Period | Government-wide: Inability to continue operation globally | Permanent loss of stakeholder confidence resulting in legal action, interruption in operations as a whole | Global restrictions on performing activities across agencies and departments |
| 4 | Severe | Serious but not complete damage to asset or reputation e.g. externally visible and affects department's operation and citizen's confidence. Substantial support costs or business commitments canceled. | Recoverable in the Long Term (i.e., 12-24 months) | 2 or more departments/ agencies Significant, ongoing interruptions to operations within 2 or more departments/ agencies | Sustained operation degradation for citizens or preventing civil servant from meeting their SLA | Prohibited from conducting operations in certain departments or geographies. |
| 3 | Serious | Moderate damage or loss, e.g. affects internal operation, cause increase in operational costs or reduction of SLA performance. Noticeable impact to support costs and productivity. No measurable business impact. | Recoverable in the Short Term (i.e., 6-12 months) | 1 or more department or agency: Moderate impact within 1 or more department | Moderate loss in 1 or more stakeholder groups | Significant fines or limitations in conducting operations in certain departments or geographies. |
| 2 | Mild | Little damage or loss, e.g. affects internal operations cannot measure increase in costs. No measurable impact, minor increases in support or infrastructure costs. | Temporary (i.e., less than 6 months) | 1 department or agency affected | Limited to minor/ short-term loss in 1 stakeholder group | Limited actions against the government with limited effects on operations. |
| 1 | Low | Minor or no change in asset. Absorbed by normal business operations - No measurable impact to support costs, productivity, or business commitments. | Minimal Impact | | | |

***Figure B-3 – Template Risk Impacts***

### Risk Likelihood

Similarly, the template below for Risk Likelihood is also included in the Excel spreadsheet that accompanies this paper. It should however be given sufficient thoughts and be endorsed by all stakeholders prior to being used.

| | | Definition | | |
|---|---|---|---|---|
| Score | Likelihood Rating | Consideration | Probability | Frequency |
| 5 | Expected | The risk event or circumstance is relatively certain to occur, or has occurred within the past 6 months | 90-100% | Almost Quarterly |
| 4 | Highly Likely | The risk event or circumstance is highly likely to occur | 70-90% | Yearly |
| 3 | Likely | The risk event or circumstance is more likely to occur than not | 50-70% | Every 2 to 4 Years |
| 2 | Not Likely | The risk event or circumstance occurring is possible | 10-50% | Every 4 to 6 Years |
| 1 | Slight | The risk event or circumstance is only remotely probable | < 10% | Every 7 Years and Beyond |

***Figure B-4 – Risk Likelihoods***

## 2. Risk identification

The Risk Assessment Process requires three steps:

- Identify Risks
- Analyse Risks
- Evaluate Risks

First identify the risks associated with the system to review. Gather information from a variety of relevant data sources and stakeholders within the organisation.

Then consider all the risks associated with the target system covered by the program.

Involve a wide range of stakeholders, from different disciplines within the organisation, such as business, finance, security, BCP and IT, and ensure that the ultimate business owner is included at some phase of the process and at final sign-off on conclusions.

| | Risk Control Area |
|---|---|
| **Compliance Risks** | Governance & Entreprise Risk Management |
| | Legal Issues : Contracts and Electronic Discovery |
| | Incident Response |
| | Storage of data in multiple jurisdictions and lack of transparency |
| | Compliance and Audit Management |
| | Data Protection Risks |
| | Sensitive Media Sanitization |
| | Audit or Certification unavailable |
| | Compliance Degradation |
| | Governance Degradation |
| **Strategic Risks** | Information Management and Data Security |
| | Interoperability and Portability |
| | Poor Provider Selection |
| | Organizational Readiness |
| | Lack of Supplier Redundancy |
| | Lock-In |
| | Data classification on DoCE side |
| | Data migration from on-premise into the cloud (regardless whether public, private or hybrid) |
| **Operational Risks** | Data Center Operations |
| | Log & Tracing failure |
| | Backup Failure |
| | Information Management and Data Security |
| | Impact on current internal operational procedures |
| | Integration into existing business solutions |
| | Malicious Activities from an Insider |
| | Sensitive Information Leakage |
| | Operations management |
| | Subpoena and e-discovery |
| | Unauthorized access to premises |
| | Theft of Computer Equipment |
| | Security of the endpoint (e.g. laptop, pc, smartphone, slate) from which the cloud service is consumed. |
| | Human Resource Constraints |
| | Natural Disasters |
| | Licensing Risks |
| | Traditional Security, Business Continuity and Disaster Recovery |
| **Market & Finance Risks** | Loss of reputation |
| | Service Termination or Failure |
| | Isolation Failure |
| | Capacity Management |
| | Environment Agility / Time to Market |
| | Incident Response |

*Figure B-5 – Risk identification*

### Mapping the Risk

To accelerate the risk mapping process, this risk framework comes populated with a template of commonly accepted business risks usually associated with typical IT systems subject to be externalised to the Cloud and broadly aligned with the Cloud Security Alliance Cloud controls Matrix[2].

However, the stakeholders should not limit themselves to this template. Some risks are very specific to certain industries, cultures and geographies; they might not be included in the template and would need to be added to the final risk map.

## *3. Risk analysis*

### What to use

The risk analysis is a formal process through which the stakeholders will determine the forecast likelihood and impact for each and every identified risk. Risks should then be prioritised, with the highest likelihood and highest impact risks being a top priority, and the lowest likelihood and impact being the least priority.

If quantitative information is available, such as logs, monitoring, reports, audit and previous incidents, it should be used to rate the risk, and be reported as a comment alongside the risk rating.

Qualitative information, mostly derived from the cumulative experience of the stakeholders, will be used as well.

### Who you should involve

If need be, external third-party inputs, such as Gartner, Forrester, other industry experts and actual Cloud providers should be sought and factored into the risk analysis.

### What to ask your vendor

The vendor of the proposed Cloud solution should be asked to provide information about any compensating controls or means by which they will mitigate any identified risk as part of the analysis phase. This information could include descriptions of how the vendor's own controls align to those of the Cloud Security Alliance[3].

The rule regarding the integration of these mitigating controls is this:

If the system being analysed already has mitigating controls in place, the risk analysis should integrate these and, therefore, the result found in the risk map should be the 'residual risks'.

If the system being analysed is hypothetical, the risk analysis should not cover the mitigating controls, as these will be covered during a later phase in the program where details of a possible specific solution will be available and required. This gives more visibility and improved reasoning to the decision team as to which mitigating controls would need to be deployed on target systems.

[2] Cloud Security Alliance, Cloud Controls Matrix: https://cloudsecurityalliance.org/research/ccm/

[3] Cloud Security Alliance, Cloud Controls Matrix: https://cloudsecurityalliance.org/research/ccm/

## 4. Risk evaluation

A team composed of subject-matter experts and business owners would evaluate the risks based on their knowledge and representation. The result of this team activity would be a draft risk-evaluation document.

For example:

> *The risk of downtime for the target system was reported by the subject-matter experts as "having an important impact", whereas the business team reflected that, from their perspective, the impact associated with that risk was critical instead.*

We use a case study in the next
section to demonstrate how the Cloud-based risk management program works, and provide results for the decision process.

In our case study, we use an example of a government department considering externalising their email system.

## 5. Risk treatment

Risk Treatment [4] [5] decisions are based on the overall risk rating and may include an evaluation of the risk relative to the cost of remediation.

There are four options available for risk treatment:

1. Risk reduction or elimination. Follow mitigation strategies
   and Enterprise Risk Management (ERM) practices to reduce the probability and impact of risks. Plan for failures and ensure failover approach is identified.

2. Risk retention or acceptance. Determine the organisation can tolerate the risk introduced by the cloud solution. Ensure you compare enterprise risk tolerance to solution risk profile.

3. Risk avoidance. Choose not to adopt the cloud solution and avoid the risks introduced by the initial cloud solution.

4. Risk transfer. Cloud insurance is an emerging field that enables risk transfer to a third party. Alternatively, warranties and SLAs can be used to transfer the risk to the cloud provider. Vendor assurances and SLAs should be taken into consideration.

Risk treatment options should be selected based on the outcome of the risk assessment, the expected cost for implementing these options and the expected benefits from these options.

All considered options should be factored to enable them to be considered as part of a cost, value and risk evaluation of multiple potential mitigations.

**Integrating Compensating Controls**

It is important that mitigation process is included in the cloud risk map in order to derive a more realistic evaluation of the risks, identify the necessary controls and generate a residual risk map.

Controls are activities that reduce the likelihood or impact of a risk should it manifest. Inherent risk levels are determined by the likelihood or exposure to a risk without considering what controls are in place. Residual risk levels are determined by taking the inherent risk level and evaluating how effective a control is at reducing the risk. Control effectiveness is the determination of how well a particular control reduces an identified risk.

[4] ISO 27001 4.2.1.f
[5] NIST SP 800-30 3.8, 3.9, 4.1

**Cost-Benefit Analysis**

Some risks may require a quantitative assessment supporting cost/benefit analysis. For the purposes of this effort, any cost/benefit analysis should be high-level estimates only, and should serve to further any discussion about whether a risk will be reduced. Once risks requiring cost-benefit analysis have been identified, the appropriate Risk Owners will review potential solutions. A high-level business case will be evaluated to determine if a feasible solution exists to address the risk based on:

- cost of remediation;
- business benefit;
- risk reduction;
- feasibility; and dependencies.

Based on this review, the risk may be remediated or not as described in the Results and Decisions section below.

## *6. Review & consider*

Following the completion of the previous steps, information should then exist to enable a reasonable decision to be made about the feasibility of the candidate cloud-capability as a way of providing the IT capability required by the organisation.

Information about risk should be shared between the decision-maker and the other stakeholders. An organisation should develop risk communication plans for normal operations as well as for emergency situations. Therefore, risk communication activity should be performed continually. The coordination between major decision-makers and stakeholders may be achieved by the formation of a committee where debate about risks, their prioritisation and appropriate treatment, and acceptance can take place.

In order to effectively mitigate risks, controls should be implemented by:

- Prioritising actions;
- Evaluating control-options' recommendations;
- Conducting a Cost-Benefits analysis;
- Developing a safeguard implementation plan; and
- Implementing a selected control.

# *Results and Decisions*

Once the six steps of the Risk Analysis have been completed, a decision needs to be made about the viability of the proposal. The use of a 'traffic light' system to identify a profile of the various risks enables a broad range of stakeholders to understand the process and output of the analysis. This is particularly useful when presenting to non-technical stakeholders, such as a board or senior business decision-makers.

The table to the right gives you an example of how this can be set out. It can also be useful to represent the findings of multiple candidate options, with the ratings set alongside each other as a way of demonstrating how the risk profile changes with each option.

### CONCLUSION

The Conclusion section will summarise the findings, together with a recommendation, and will probably include additional information in support of any positive outcome for the candidate proposal.

It should address the following:

**I.** Overview of proposed cloud-based proposal;

**II.** Short summary of involved stakeholders and relevant business impact;

**III.** Dashboard summary of risk movements by high-level domain with any supporting analysis; and

**IV.** Recommendation to the business, incorporating any costed mitigations required for the full business case.

| | Risk Control Area | Risk Likelihood | Risk Impact | |
|---|---|---|---|---|
| **Compliance Risks** | Governance & Entreprise Risk Management | Likely | Serious | |
| | Legal Issues : Contracts and Electronic Discovery | Expected | Serious | |
| | Incident Response | Likely | Serious | |
| | Storage of data in multiple jurisdictions and lack of transparency | Expected | Severe | |
| | Compliance and Audit Management | Likely | Severe | |
| | Data Protection Risks | Likely | Severe | |
| | Sensitive Media Sanitization | Highly Likely | Serious | |
| | Audit or Certification unavailable | Likely | Serious | |
| | Compliance Degradation | Likely | Serious | |
| | Governance Degradation | Highly Likely | Serious | |
| **Strategic Risks** | Information Management and Data Security | Likely | Serious | |
| | Interoperability and Portability | Likely | Serious | |
| | Poor Provider Selection | Not Likely | Serious | |
| | Organizational Readiness | Not Likely | Mild | |
| | Lack of Supplier Redundancy | Highly Likely | Mild | |
| | Lock-In | Likely | Mild | |
| | Data classification on DoCE side | Highly Likely | Serious | |
| | Data migration from on-premise into the cloud (regardless whether public, private or hybrid) | Likely | Serious | |
| **Operational Risks** | Data Center Operations | Likely | Severe | |
| | Log & Tracing failure | Not Likely | Severe | |
| | Backup Failure | Likely | Severe | |
| | Information Management and Data Security | Likely | Severe | |
| | Impact on current internal operational procedures | Likely | Mild | |
| | Inaccurate Modeling of Resource Usage / Resource Exhaustion | Not Likely | Mild | |
| | Integration into existing business solutions | Likely | Serious | |
| | Malicious Activities from an Insider | Likely | Serious | |
| | Sensitive Information Leakage | Likely | Serious | |
| | Operations management | Likely | Serious | |
| | Subpoena and e-discovery | Likely | Serious | |
| | Unauthorized access to premises | Likely | Serious | |
| | Theft of Computer Equipment | Likely | Severe | |
| | Security of the endpoint (e.g. laptop, pc, smartphone, slate) from which the cloud service is consumed. | Not Likely | Serious | |
| | Human Resource Constraints | Slight | Mild | |
| | Natural Disasters | Likely | Catastrophic | |
| | Licensing Risks | Not Likely | Severe | |
| | Traditional Security, Business Continuity and Disaster Recovery | Likely | Severe | |
| **Market & Finance Risks** | Loss of reputation | Highly Likely | Serious | |
| | Service Termination or Failure | Likely | Catastrophic | |
| | Isolation Failure | Likely | Catastrophic | |
| | Capacity Management | Likely | Mild | |
| | Environment Agility / Time to Market | Slight | Mild | |
| | Incident Response | Likely | Serious | |

***Figure B-6 – Risk dashboard***

# PART C: PUTTING IT TOGETHER – EXAMPLE CASE STUDY

## *Background and Drivers*

The IT department for the Department of Citizen Engagement (DoCE) supports the IT needs of several bureaus and other departments. Whilst this has operated adequately in the past, user numbers and the level of their requirements have increased steadily over the past few years. This has made meeting load requirements more challenging, given increasing budget pressures and dwindling access to in-house expertise.

Additionally, although the general level of security is adequate, recent concerns have been raised about a perceived complacency amongst the operations team – with real potential to lead to a serious security incident for the organisation, such as data theft or external cyber security breach.

Some of the bureaus were required to comply with to stringent regulatory requirements and policies, especially related to data use and classification that were raised as a potential impediment to any decision in favour of cloud solutions.

The agency agreed to use the Risk Assessment Framework as a way to fully evaluate the cost, value and risk aspects of the proposed cloud approach.

## Step 1: Establishing the context

The target workload for consideration was an email system. The system consisted of several separate email systems from the same vendor but of varying generations. The agency wished to move to a single, consolidated platform to remain 'ever-green' and provide on-going flexibility of delivery to varying devices and channels.

**Scope**

The scope for the evaluation consisted of:

**I.** The core messaging system;

**II.** Identity & access systems necessary to support the messaging system;

**III.** Relevant devices consuming the messaging; and

**IV**. Business processes impacted by the mail system.

A list of all the components (IT and otherwise) associated with the current government messaging system is generated by OGCIO and submitted to stakeholders for validation.

The agency used internal and external people to build their risk landscape (identifying all the risks they are subject to).

**Impact & Likelihood**

They spent time agreeing on the measures of 'Likelihood' and 'Impact' that would be used as part of the risk assessment. They found they spent more time than anticipated actually coming to an agreement about the descriptions and numerical scales for their measures. However, the extra time proved very useful as it enabled them to adopt a common perspective for their risks and impact, which served to strengthen the final evaluation. DoCE elected to use the following definitions of Impact and Likelihood to assess each risk domain. They then used the product of Impact X Likelihood to arrive at a rating for each.

| Score | Likelihood Rating | Consideration | Probability | Frequency |
|---|---|---|---|---|
| 5 | Expected | The risk event or circumstance is relatively certain to occur, or has occurred within the past 6 months | 90-100% | Almost Quarterly |
| 4 | Highly Likely | The risk event or circumstance is highly likely to occur | 70-90% | Yearly |
| 3 | Likely | The risk event or circumstance is more likely to occur than not | 50-70% | Every 2 to 4 Years |
| 2 | Not Likely | The risk event or circumstance occurring is possible | 10-50% | Every 4 to 6 Years |
| 1 | Slight | The risk event or circumstance is only remotely probable | < 10% | Every 7 Years and Beyond |

*Figure C-1 – DoCE Likelihood measurement table*

| Score | Rating | Definition | Description of Impact | | | |
|---|---|---|---|---|---|---|
| | | | Duration | Organizational and operational scope | Reputational impact on stakeholders (i.e., citizens, civil servants ) | Legal/ Compliance/ Environmental Impact |
| 5 | Catastrophic | Severe or complete damage to asset or reputation e.g. externally visible and affects department's operation and citizen's confidence. Substantial support costs or business commitments canceled. | Significant Recovery Period | Government-wide: Inability to continue operation globally | Permanent loss of stakeholder confidence resulting in legal action, interruption in operations as a whole | Global restrictions on performing activities across agencies and departments |
| 4 | Severe | Serious but not complete damage to asset or reputation e.g. externally visible and affects department's operation and citizen's confidence. Substantial support costs or business commitments canceled. | Recoverable in the Long Term (i.e., 12-24 months) | 2 or more departments/ agencies Significant, ongoing interruptions to operations within 2 or more departments/ agencies | Sustained operation degradation for citizens or preventing civil servant from meeting their SLA | Prohibited from conducting operations in certain departments or geographies. |
| 3 | Serious | Moderate damage or loss, e.g. affects internal operation, cause increase in operational costs or reduction of SLA performance. Noticeable impact to support costs and productivity. No measurable business impact. | Recoverable in the Short Term (i.e., 6-12 months) | 1 or more department or agency: Moderate impact within 1 or more department | Moderate loss in 1 or more stakeholder groups | Significant fines or limitations in conducting operations in certain departments or geographies. |
| 2 | Mild | Little damage or loss, e.g. affects internal operations cannot measure increase in costs. No measurable impact, minor increases in support or infrastructure costs. | Temporary (i.e., less than 6 months) | 1 department or agency affected | Limited to minor/ short-term loss in 1 stakeholder group | Limited actions against the government with limited effects on operations. |
| 1 | Low | Minor or no change in asset. Absorbed by normal business operations - No measurable impact to support costs, productivity, or business commitments. | Minimal Impact | | | |

*Figure C-2 – DoCE Impact measurement table*

**Stakeholders**

Here is a list of relevant stakeholders pulled together for the analysis:

- Appointee from Operations;
- Appointee from the budget department;
- Appointee from the legal team;
- CIO;
- Member of the IT Security team; and
- Member of the Business Continuity team.

The CIO was appointed as the owner of the program.

# Step 2: Identify risks

The agency first evaluated their existing environment. Although there was initially some reluctance, several stakeholders believed it necessary to benchmark their existing system. However, the step was ultimately agreed as essential, as it revealed some critical risks in the existing environments that were known to only a few within the agency, and initially perceived as benign.

These included:

- Inefficient data classification;
- Risk of loss or compromise of logs;
- Capacity Management; and
- Isolation failure (denial of service).

Their assessment of the overall risk landscape included a specific focus on the areas below.

**Risk Landscape external**

What are the policy or regulatory considerations? A review of relevant regulatory considerations was developed and included the following:

| Requirements/ considerations | High-level description |
|---|---|
| Recordkeeping and archiving requirements | - State and Federal recordkeeping acts cover this project.<br>- There is a requirement for retention and lifecycle management for some classes of documents that will need to be considered. |
| Privacy | Both state and national privacy regimes may impact this project. |
| Data protection | There is a state requirement to protect certain classifications of data both in transit and at rest. |
| Secure email markings policy | A national code exists governing the application of classification markings to all email. |

***Figure C-3 – Regulatory Considerations***

### Risk Landscape internal

The agency evaluated their current risk landscape and systems against the main areas outlined in the Risk Evaluation Framework and arrived at the output in Figure C-4:

| | Risk Control Area | Description | Risk Likelihood | Risk Impact |
|---|---|---|---|---|
| Compliance Risks | Governance & Entreprise Risk Management | Lack of effective internal information security governance, risk management and compliance, and alignement with the provider own security governance | Likely | Serious |
| | Legal Issues : Contracts and Electronic Discovery | Storage, processing, disclosure to third-party, transfer to other legal jurisdictions of personal data and the risk for the provider not being able to produce business data in case of subpoena | Expected | Serious |
| | Incident Response | Failure for the provider to detect, handle incidents and report them to the DoCE with data that can be analyzed easily to satisfy legal requirements in case of forensic investigations | Likely | Serious |
| | Storage of data in multiple jurisdictions and lack of transparency | Mirroring data for delivery and redundant storage without actualized information as to where the data is stored. DoCE may unknowingly violate regulations especially if clear information is not provided about the jurisdiction of storage | Expected | Severe |
| | Compliance and Audit Management | Risk of failing to comply with government-mandated and industry-specific regulations and standards, and failure to get audit information from the provider | Likely | Severe |
| | Data Protection Risks | Risk of adequate Data Protection no longer being maintained to a compliant level | Likely | Severe |
| | Sensitive Media Sanitization | Media cannot be physically destroyed, cannot be properly identified or no adequate procedure in place | Highly Likely | Serious |
| | Audit or Certification unavailable | The system cannot be audited and/or certified as it should | Likely | Serious |
| | Compliance Degradation | Failure in achieving or maintaining Compliance (to regulation, governance, standards) | Likely | Serious |
| | Governance Degradation | The DoCE might cede control to the provider on a number of issues which may affect overall governance | Highly Likely | Serious |
| Strategic Risks | Information Management and Data Security | Loose identification of sensitive data or protection of data in transit or stored in the cloud, and prevention of data leakage | Likely | Serious |
| | Interoperability and Portability | Unable to make business applications interoperate between providers and lack of standards to minimize the risk of vendor lock-in | Likely | Serious |
| | Poor Provider Selection | Selection of technology or service provide sub-optimal, resulting in system operational degradation | Not Likely | Serious |
| | Organizational Readiness | Unable to achieve strategic alignment, cultural and workforce readiness, championship, and stakeholder buy-in | Not Likely | Mild |
| | Lack of Supplier Redundancy | Unable to identify / contract an alternative supplier source | Highly Likely | Mild |
| | Lock-In | Risk associated with the migration from an in-house IT environment to an external Provider, and from one provider to another | Likely | Mild |
| | Data classification on DoCE side | Inappropriate data classification and definition of mitigating controls leading to being unable to define requirements towards the provider | Highly Likely | Serious |
| | Data migration from on-premise into the cloud (whether public, private or hybrid) | Difficulty to move legacy data into a cloud based environment | Likely | Serious |
| Operational Risks | Data Center Operations | Failure for the provider to respect management standards and best practices and implement security controls in accordance to sensitivity of business services | Likely | Severe |
| | Log & Tracing failure | Loss or Compromise of Operational Logs (including Security Logs) | Not Likely | Severe |
| | Backup Failure | Misplacement or theft of Backup information | Likely | Severe |
| | Information Management and Data Security | Loose identification of sensitive data or protection of data in transit or stored in the cloud, and prevention of data leakage | Likely | Severe |
| | Impact on current internal operational procedures | Review of existing operational procedures regarding change management, incident/problem management, business continuity management | Likely | Mild |
| | Inaccurate Modeling of Resource Usage / Resource Exhaustion | Temporary failure to provide additional capacity and/or to meet Service Level Agreement. | Not Likely | Mild |
| | Integration into existing business solutions | Difficulty of Integration into legacy/current environment (interfaces) | Likely | Serious |
| | Malicious Activities from an Insider | Privileged users (e.g. Administrator) performing unauthorized activities on the system (data theft, tampering...) | Likely | Serious |
| | Sensitive Information Leakage | Accidental or Malicious activity leading to sensitive information being exposed to otherwise unauthorised group | Likely | Serious |
| | Operations management | Provider performs operations in a manner not meeting compliance requirements (e.g. Change management, patch management) | Likely | Serious |
| | Subpoena and e-discovery | Confiscation of critical system as a result of subpoena by law-enforcement agencies or civil suits | Likely | Serious |
| | Unauthorized access to premises | Unauthorized access to premises Including physical acccess to machines and other facilities | Likely | Serious |
| | Theft of Computer Equipment | Systems or Data be stolen | Likely | Severe |
| | Security of endpoint (laptop, pc, etc.) from which the cloud service is consumed. | Inability to provide adequate policies/controls to secure the end-point | Not Likely | Serious |
| | Human Resource Constraints | Inability to find and retain the right resources to ensure service and support | Slight | Mild |
| | Natural Disasters | Handling of Natural Disaster Situations (Business Continuity Management) | Likely | Catastrophic |
| | Licensing Risks | Unable to handle Natural Disaster Situations (Business Continuity Management) | Not Likely | Severe |
| | Traditional Security, Business Continuity and Disaster Recovery | Failure for the provider to implement datacenters security, business continuity and disaster recovery plans | Likely | Severe |
| Market & Finance Risks | Loss of reputation | In-house system: risk of some significant and public incidents / In the Cloud: risk with Cloud Provider or co-tenant activities | Highly Likely | Serious |
| | Service Termination or Failure | The Service can no longer be provided as assumed | Likely | Catastrophic |
| | Isolation Failure | Access to the Service is temporarily denied, possibly leading to reputational, critical or financial issues | Likely | Catastrophic |
| | Capacity Management | Inadequate Resource Provisioning and Investment in Infrastructure | Likely | Mild |
| | Environment Agility / Time to Market | Latency or overall difficulty in being able to adjust the systems' characteristics (performance, architecture, segregation) to address dynamic environment | Slight | Mild |
| | Incident Response | The provider could not detect, handle incidents and report them to the DoCE with data that can be analyzed easily to satisfy legal requirements in case of forensic investigations | Likely | Serious |

*Figure C-4 – Risk of existing system*

# Steps 3 & 4: Analyse and Evaluate risks

The agency reviewed the risk associated with utilising a generic public cloud offering. That is, what would be the risks if the agency were to deploy all the email and IM system to a public cloud without any special protection.

The agency then selected several specific public cloud solutions and evaluated more closely how the risks identified in the generic public cloud review would be reduced, and what would be the resulting landscape.

After evaluating each area for both Risk Likelihood and Impact, and then mapping in the template, they arrived at a completed assessment as follows, including the 'traffic light' summary of risk against each line item.

## Calculating the risk rating

The traffic light colours were determined by a simple Likelihood x Impact function with a possible 1-25 rating. Five levels of risk were identified as follows:

| Risk | Very High | High | Moderate | Low | Very low |
|---|---|---|---|---|---|
| L x I | 21-25 | 16-20 | 11-15 | 6-10 | 1-5 |
| Code | | | | | |

*Figure C-5 – Calculating risk codes*

| | Risk Control Area | Description | Risk Likelihood | Risk Impact | Risk |
|---|---|---|---|---|---|
| Compliance Risks | Governance & Entreprise Risk Management | Lack of effective internal information security governance, risk management and compliance, and alignement with the provider own security governance | Likely | Serious | |
| | Legal Issues : Contracts and Electronic Discovery | Storage, processing, disclosure to third-party, transfer to other legal jurisdictions of personal data and the risk for the provider not being able to produce business data in case of subpoena | Expected | Serious | |
| | Incident Response | Failure for the provider to detect, handle incidents and report them to the DoCE with data that can be analyzed easily to satisfy legal requirements in case of forensic investigations | Likely | Serious | |
| | Storage of data in multiple jurisdictions and lack of transparency | Mirroring data for delivery and redundant storage without actualized information as to where the data is stored. DoCE may unknowingly violate regulations especially if clear information is not provided about the jurisdiction of storage | Expected | Severe | |
| | Compliance and Audit Management | Risk of failing to comply with government-mandated and industry-specific regulations and standards, and failure to get audit information from the provider | Likely | Severe | |
| | Data Protection Risks | Risk of adequate Data Protection no longer being maintained to a compliant level | Likely | Severe | |
| | Sensitive Media Sanitization | Media cannot be physically destroyed, cannot be properly identified or no adequate procedure in place | Highly Likely | Serious | |
| | Audit or Certification unavailable | The system cannot be audited and/or certified as it should | Likely | Serious | |
| | Compliance Degradation | Failure in achieving or maintaining Compliance (to regulation, governance, standards) | Likely | Serious | |
| | Governance Degradation | The DoCE might cede control to the provider on a number of issues which may affect overall governance | Highly Likely | Serious | |
| Strategic Risks | Information Management and Data Security | Loose identification of sensitive data or protection of data in transit or stored in the cloud, and prevention of data leakage | Likely | Serious | |
| | Interoperability and Portability | Unable to make business applications interoperate between providers and lack of standards to minimize the risk of vendor lock-in | Likely | Serious | |
| | Poor Provider Selection | Selection of technology or service provide sub-optimal, resulting in system operational degradation | Not Likely | Serious | |
| | Organizational Readiness | Unable to achieve strategic alignment, cultural and workforce readiness, championship, and stakeholder buy-in | Not Likely | Mild | |
| | Lack of Supplier Redundancy | Unable to identify / contract an alternative supplier source | Highly Likely | Mild | |
| | Lock-In | Risk associated with the migration from an in-house IT environment to an external Provider, and from one provider to another | Likely | Mild | |
| | Data classification on DoCE side | Inappropriate data classification and definition of mitigating controls leading to being unable to define requirements towards the provider | Highly Likely | Serious | |
| | Data migration from on-premise into the cloud (regardless | Difficulty to move legacy data into a cloud based environment | Likely | Serious | |
| Operational Risks | Data Center Operations | Failure for the provider to respect management standards and best practices and implement security controls in accordance to sensitivity of business services | Likely | Severe | |
| | Log & Tracing failure | Loss or Compromise of Operational Logs (including Security Logs) | Not Likely | Severe | |
| | Backup Failure | Misplacement or theft of Backup information | Likely | Severe | |
| | Information Management and Data Security | Loose identification of sensitive data or protection of data in transit or stored in the cloud, and prevention of data leakage | Likely | Severe | |
| | Impact on current internal operational procedures | Review of existing operational procedures regarding change management, incident/problem management, business continuity management | Likely | Mild | |
| | Inaccurate Modeling of Resource Usage / Resource Exhaustion | Temporary failure to provide additional capacity and/or to meet Service Level Agreement. | Not Likely | Mild | |
| | Integration into existing business solutions | Difficulty of Integration into legacy/current environment (interfaces) | Likely | Serious | |
| | Malicious Activities from an Insider | Privileged users (e.g. Administrator) performing unauthorized activities on the system (data theft, tampering...) | Likely | Serious | |
| | Sensitive Information Leakage | Accidental or Malicious activity leading to sensitive information being exposed to otherwise unauthorised group | Likely | Serious | |
| | Operations management | Provider performs operations in a manner not meeting compliance requirements (e.g. Change management, patch management) | Likely | Serious | |
| | Subpoena and e-discovery | Confiscation of critical system as a result of subpoena by law-enforcement agencies or civil suits | Likely | Serious | |
| | Unauthorized access to premises | Unauthorized access to premises Including physical acccess to machines and other facilities | Likely | Serious | |
| | Theft of Computer Equipment | Systems or Data be stolen | Likely | Severe | |
| | Security of the endpoint (e.g. laptop, pc, smartphone, slate) | Inability to provide adequate policies/controls to secure the end-point | Not Likely | Serious | |
| | Human Resource Constraints | Inability to find and retain the right resources to ensure service and support | Slight | Mild | |
| | Natural Disasters | Handling of Natural Disaster Situations (Business Continuity Management) | Likely | Catastrophic | |
| | Licensing Risks | Unable to handle Natural Disaster Situations (Business Continuity Management) | Not Likely | Severe | |
| | Traditional Security, Business Continuity and Disaster Recovery | Failure for the provider to implement datacenters security, business continuity and disaster recovery plans | Likely | Severe | |
| Market & Finance Risks | Loss of reputation | In-house system: risk of some significant and public incidents / In the Cloud: risk with Cloud Provider or co-tenant activities | Highly Likely | Serious | |
| | Service Termination or Failure | The Service can no longer be provided as assumed | Likely | Catastrophic | |
| | Isolation Failure | Access to the Service is temporarily denied, possibly leading to reputational, critical or financial issues | Likely | Catastrophic | |
| | Capacity Management | Inadequate Resource Provisioning and Investment in Infrastructure | Likely | Mild | |
| | Environment Agility / Time to Market | Latency or overall difficulty in being able to adjust the systems' characteristics (performance, architecture, segregation) to address dynamic environment | Slight | Mild | |
| | Incident Response | The provider could not detect, handle incidents and report them to the DoCE with data that can be analyzed easily to satisfy legal requirements in case of forensic investigations | Likely | Serious | |

*Figure C-6 – Risk evaluation for DoCE Public Cloud scenario*

Overall, the agency found that some non-regulatory risks could be reasonably managed:

- Security;
- Data Classification;
- Integration;
- Governance degradation; and
- Datacentre operations.

When they compared the Public Cloud scenario with the analysis for their own existing system, the agency also found that some risks would be significantly reduced with a move to public cloud.

However, they decided that the risks associated with regulation and governance were too critical to allow a public cloud strategy to be considered in the context of moving the entire agency's mail and IM systems.

# Step 5: Treat risks

The agency then looked at a hybrid cloud solution to effectively push a non-critical/less regulated system out to a public cloud, but retain the more critical and regulated information onshore.

As with Steps 3 and 4, the agency risk-assessed this hybrid cloud solution first for Impact and Likelihood, and called out key risks that would need to be addressed.

**Compensating controls and vendor mitigations**

In order to arrive at a more comprehensive final position for this proposed hybrid cloud approach, the agency also spent time identifying and qualifying possible risk-mitigations associated with the key identified risks. Some of these risks were able to be treated by the agency themselves. For example, in the 'Operational Risk' domain, the handling of security-classified data was identified as risky and the agency decided that a suitable mitigation was an action for them:

- *"Need to clean up Data Classification and deployment BEFORE handing over to Cloud Provider + agree upon specific SLAs related to data protection."*

In a number of other instances, the agency needed to rely on the cloud vendor to treat the risk and, therefore, stipulated this as a requirement in a subsequent RFP. The agency found they were able to efficiently manage most vendor questions of risk treatment by aligning the key risk areas with specific controls from the Cloud Security Alliance Cloud Controls Matrix (CCM[6]).

The CCM is specifically designed to provide fundamental security principles to guide cloud vendors and to assist prospective cloud customers in assessing the overall security risk of a cloud provider. It provides a controls framework that gives detailed understanding of security concepts and principles that are aligned to the Cloud Security Alliance guidance in 13 domains.

**Using standardised controls with vendors**

One of the high compliance risks identified related to storage of data in multiple locations and potential vendors were expected to be able to point to audited controls they used that were relevant to treating this particular risk. An example of a vendor response for one such control is shown in the following table.

Using such a standard way to map areas of risk concern for the agency against a set of granular controls also provided the agency with an on-going way to audit their own decision-making.

[4] CSA CCM - https://cloudsecurityalliance.org/research/ccm/

| Control ID In CCM | Description (CCM Version R1.1. Final) | Vendor Response |
|---|---|---|
| DG-02<br><br>Data Governance - Classification | Data and objects containing data, shall be assigned a classification based on data type, jurisdiction of origin, jurisdiction domiciled, context, legal constraints, contractual constraints, value, sensitivity, criticality to the organisation and third-party obligation for retention and prevention of unauthorised disclosure or misuse. | Company X's Online Services standards provide guidance for classifying assets of several applicable security-classification categories, and implement a standard set of Security and privacy attributes.<br><br>"Information classification" is covered under the ISO 27001 standards, specifically addressed in Annex A, domain 7.2. For more information, review the publicly available ISO standards we are certified against. |

***Figure C-7 – Example vendor response for risk treatment using Cloud Security Alliance CCM***

The result indicated across the board, all the risks that would have been considered 'blocking factors' were addressed. In addition, several of the risks present in the existing system would be addressed in the public cloud approach.

## Step 6: Review and decide

The agency decided to utilise the generated reports, including the final colour-coded risk dashboard to document and submit their position to the executive council. They concluded that the agency should proceed with a more thorough investigation of the hybrid-cloud solution.

This was completed by agreeing on the specific risk treatments required. These were included in a detailed requirements list, which formed part of a subsequent Request for Proposal that was put out to the market.

## Ultimate decision

Eventually, the agency selected one of only two cloud suppliers that was able to meet the requirements distilled from the Cloud Risk Analysis, and progressively moved their email and collaboration to the hybrid-cloud solution. They are now considering the externalisation of other systems as well, and will use the same risk-assessment framework.

# PART D: PRACTICAL TOOLS & CHECKLISTS

The following tables are captured from the accompanying Excel spreadsheet and serve as the basic tools and checklists required for completing this process. As noted earlier, these can and should be adapted to the specific needs of the organisation and computing tasks being evaluated.

## *Appendix 1. Model template: Risk Management Process – Rating Criteria for Inherent Impact*

| Score | Rating | Operating Income | Definition | Description of Impact | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | | Impact on Value (EPS - Impact on Annual Guidance) | Duration | Organizational and operational scope | Reputational impact on stakeholders (i.e., citizens, civil servants ) | Legal/ Compliance/ Environmental Impact |
| 5 | Critical | > 11%<br>> $2.5B | Severe or complete damage to asset or reputation e.g. externally visible and affects department's operation and citizen's confidence. Substantial support costs or business commitments canceled. | Significant reduction in market capitalization, signifant draw on liquidity reserve (EPS > $0.25) | Significant Recovery Period | Government-wide: Inability to continue operations globally | Permanent loss of stakeholder confidence resulting in legal action, interruption in operations as a whole | Global restrictions on performing activities across agencies and departments |
| 4 | High | > 4.4%<br>> $1B | Serious but not complete damage to asset or reputation e.g. externally visible and affects department's operation and citizen's confidence. Substantial support costs or business commitments canceled. | Substantial reduction in market capitalization, substantial draw on liquidity reserve (EPS > $0.10) | Recoverable in the Long Term (i.e., 24 - 36 months) | 2 or more departments/ agencies: Significant, ongoing interruptions to operations within 2 or more departments/ agencies | Sustained operation degradation for citizens or preventing civil servant from meeting their SLA | Prohibited from conducting operations in certain departments or geographies |
| 3 | Moderate | >2.2%<br>> $500M | Moderate damage or loss, e.g. affects internal operation, cause increase in operational costs or reduction of SLA performance. Noticeable impact to support costs and productivity. No measurable business impact. | Limited reduction in market capitalization, limited draw on operating cash flow (EPS > $0.05 | Recoverable in the Short Term (i.e.,12 -24 months) | "1 or more department or agency: Moderate impact within 1 or more departments | Moderate loss in 1 or more stakeholder groups | Significant fines or limitations in conducting operations in certain departments or geographies |
| 2 | Low | > 1.10%<br>> $250M | Little damage or loss, e.g. affects internal operations cannot measure increase in costs. No measurable impact, minor increases in support or infrastructure costs. | Missed forecast(s) and/or budget(s), limited draw on operating cash flow (EPS > $0.025) | Temporary (i.e., less than 12 months) | 1 department or agency: Limited impact within 1 department or agency | Limited to minor/ short-term loss in 1 stakeholder group | Limited actions against the government with limited effects on operations |
| 1 | Minimal | > 0.50%<br>> $100M | Minor or no change in asset. Absorbed by normal business operations - No measurable impact to support costs, productivity, or business commitments. | (EPS - $0.01) | Minimal Impact | | | |

***NOTE:*** *When evaluating the* ***impact*** *of a particular risk event or circumstance, assume that the* ***management activities or controls do not exist or fail in either design or operation and as a result fail to mitigate the impact of the risk occurring****. The table provides guidance for choosing a score of 1 through 5. A risk should be evaluated based on the most relevant impact, and does not need to address multiple columns.*

## *Appendix 2. Model template: Risk Management Process – Rating Criteria for Inherent Likelihood*

| Score | Likelihood Rating | Consideration | Probability | Frequency |
|---|---|---|---|---|
| 5 | Expected | The risk event or circumstance is relatively certain to occur, or has occurred within the past 6 months | 90-100% | Almost Quarterly |
| 4 | Highly Likely | The risk event or circumstance is highly likely to occur | 70-90% | Yearly |
| 3 | Likely | The risk event or circumstance is more likely to occur than not | 50-70% | Every 2 to 4 Years |
| 2 | Not Likely | The risk event or circumstance occurring is possible | 10-50% | Every 4 to 6 Years |
| 1 | Slight | The risk event or circumstance is only remotely probable | < 10% | Every 7 Years and Beyond |

***NOTE:*** *When evaluating the* ***likelihood*** *of a particular risk event or circumstance occurring, make the evaluation* ***absent of the current management activities or controls that exist to mitigate the likelihood of the risk occurring.*** *The table provides guidance for choosing a score of 1 through 5. A risk should be evaluated based on the most relevant probability or frequency column above, and does not need to address multiple columns.*

# *Appendix 3. Template Cloud-Based Relevant Risk Domains*

| | Risk Control Area | Description |
|---|---|---|
| Compliance Risks | Governance & Entreprise Risk Management | Lack of effective internal information security governance, risk management and compliance, and alignement with the provider own security governance |
| | Legal Issues : Contracts and Electronic Discovery | Storage, processing, disclosure to third-party, transfer to other legal jurisdictions of personal data and the risk for the provider not being able to produce business data in case of subpoena |
| | Incident Response | Failure for the provider to detect, handle incidents and report them to the DoCE with data that can be analyzed easily to satisfy legal requirements in case of forensic investigations |
| | Storage of data in multiple jurisdictions and lack of transparency | Mirroring data for delivery and redundant storage without actualized information as to where the data is stored. DoCE may unknowingly violate regulations especially if clear information is not provided about the jurisdiction of storage |
| | Compliance and Audit Management | Risk of failing to comply with government-mandated and industry-specific regulations and standards, and failure to get audit information from the provider |
| | Data Protection Risks | Risk of adequate Data Protection no longer being maintained to a compliant level |
| | Sensitive Media Sanitization | Media cannot be physically destroyed, cannot be properly identified or no adequate procedure in place |
| | Audit or Certification unavailable | The system cannot be audited and/or certified as it should |
| | Compliance Degradation | Failure in achieving or maintaining Compliance (to regulation, governance, standards) |
| | Governance Degradation | The DoCE might cede control to the provider on a number of issues which may affect overall governance |
| Strategic Risks | Information Management and Data Security | Loose identification of sensitive data or protection of data in transit or stored in the cloud, and prevention of data leakage |
| | Interoperability and Portability | Unable to make business applications interoperate between providers and lack of standards to minimize the risk of vendor lock-in |
| | Poor Provider Selection | Selection of technology or service provide sub-optimal, resulting in system operational degradation |
| | Organizational Readiness | Unable to achieve strategic alignment, cultural and workforce readiness, championship, and stakeholder buy-in |
| | Lack of Supplier Redundancy | Unable to identify / contract an alternative supplier source |
| | Lock-In | Risk associated with the migration from an in-house IT environment to an external Provider, and from one provider to another |
| | Data classification on DoCE side | Inappropriate data classification and definition of mitigating controls leading to being unable to define requirements towards the provider |
| | Data migration from on-premise into the cloud (regardless | Difficulty to move legacy data into a cloud based environment |
| Operational Risks | Data Center Operations | Failure for the provider to respect management standards and best practices and implement security controls in accordance to sensitivity of business services |
| | Log & Tracing failure | Loss or Compromise of Operational Logs (including Security Logs) |
| | Backup Failure | Misplacement or theft of Backup information |
| | Information Management and Data Security | Loose identification of sensitive data or protection of data in transit or stored in the cloud, and prevention of data leakage |
| | Impact on current internal operational procedures | Review of existing operational procedures regarding change management, incident/problem management, business continuity management |
| | Inaccurate Modeling of Resource Usage / Resource Exhaustion | Temporary failure to provide additional capacity and/or to meet Service Level Agreement. |
| | Integration into existing business solutions | Difficulty of Integration into legacy/current environment (interfaces) |
| | Malicious Activities from an Insider | Privileged users (e.g. Administrator) performing unauthorized activities on the system (data theft, tampering...) |
| | Sensitive Information Leakage | Accidental or Malicious activity leading to sensitive information being exposed to otherwise unauthorised group |
| | Operations management | Provider performs operations in a manner not meeting compliance requirements (e.g. Change management, patch management) |
| | Subpoena and e-discovery | Confiscation of critical system as a result of subpoena by law-enforcement agencies or civil suits |
| | Unauthorized access to premises | Unauthorized access to premises Including physical acccess to machines and other facilities |
| | Theft of Computer Equipment | Systems or Data be stolen |
| | Security of the endpoint (e.g. laptop, pc, smartphone, slate) | Inability to provide adequate policies/controls to secure the end-point |
| | Human Resource Constraints | Inability to find and retain the right resources to ensure service and support |
| | Natural Disasters | Handling of Natural Disaster Situations (Business Continuity Management) |
| | Licensing Risks | Unable to handle Natural Disaster Situations (Business Continuity Management) |
| | Traditional Security, Business Continuity and Disaster Recovery | Failure for the provider to implement datacenters security, business continuity and disaster recovery plans |
| Market & Finance Risks | Loss of reputation | In-house system: risk of some significant and public incidents / In the Cloud: risk with Cloud Provider or co-tenant activities |
| | Service Termination or Failure | The Service can no longer be provided as assumed |
| | Isolation Failure | Access to the Service is temporarily denied, possibly leading to reputational, critical or financial issues |
| | Capacity Management | Inadequate Resource Provisioning and Investment in Infrastructure |
| | Environment Agility / Time to Market | Latency or overall difficulty in being able to adjust the systems' characteristics (performance, architecture, segregation) to address dynamic environment |
| | Incident Response | The provider could not detect, handle incidents and report them to the DoCE with data that can be analyzed easily to satisfy legal requirements in case of forensic investigations |

# DISCLAIMER

This document has been prepared by Microsoft to provide an overarching risk-management framework to allow organisations to conduct a risk-based assessment of a move to the cloud.

This document is provided on an "as is" basis and to the maximum extent permitted by law Microsoft disclaims all conditions, warranties and guarantees, express or implied, including but not limited to any warranty or guarantee that the use of the framework set out in this document will not infringe any rights or any warranty or guarantee of merchantability or fitness for a particular purpose. Before using the framework set out in this document, you should evaluate its suitability for your organisation. In particular, if you choose to act upon the output of the framework, then you do so at your own risk.





## *Authors*

Greg Stone – Chief Technology Officer, Microsoft Australia
Pierre Noel – Chief Security Adviser, Microsoft Asia

## *Contributors*

Michael Thatcher – Chief Technology Officer, Microsoft Asia
James Kavanagh – Chief Security Advisor, Microsoft Australia
Bill Marriott – Information Security Manager, Microsoft Services
Kellie Anne Chainier - Director Public Sector Cloud Computing
Monika Josi - Chief Security Advisor, Microsoft EMEA

Microsoft