CalQRisk

Cloud Migration Risk Assessment Guidance

Version 1 – June 2025

Table of Contents

Foreword 3
Introduction 3
Risk Assessment 3
1. Strategic Risk Considerations 4
2. Governance Risk Considerations 4
3. Operational Risk Considerations 4
4. Environmental Risk Considerations 8
5. Capital Risk Considerations 8
6. Financial Risk Considerations 8
7. Legal/Compliance/Conduct Risk Considerations 8
8. Reputational Risk Considerations 8
9. Risk Evaluation 9
Summary 10
Appendix 1 – Cloud Migration Risk Assessment Checklist by Risk Category 12
Appendix 2 – Cloud Migration Risk Assessment Checklist by Migration Phase 14

CLOUD MIGRATION RISK ASSESSMENT GUIDANCE

Foreword

Individual Risk Management Officers (RMOs) take varying approaches to documenting their risk assessments, so this guidance document will take the form of questions for RMOs to consider under a range of risk categories. Depending on the topic being considered, some risk categories may not be particularly relevant to the assessment so the guidance will focus on the risk categories most likely to have a material impact on credit unions generally. Individual credit unions may have additional credit union-specific risks which are not covered in this document but please contact us if you need any further assistance.

The following risk assessment guidance for Cloud Migration (CM) includes a wide range of items for consideration. It should be noted at the outset that the scale of CM can vary enormously from one non-critical software solution hosted in the cloud through to the CU's core banking system and all associated applications being hosted in the cloud. This guide is weighted towards the more extensive CM project but can be adapted for use by each CU with relatively small CM projects depending upon their scale and complexity.

Introduction

The introduction to a CM risk assessment should place the proposal in the context of the CU's strategic plan.

- Does the proposal move the CU closer to its strategic goals, or further away from them?
- How does this development impact on the CU's strategic and financial objectives?

This section is the opportunity for the background to the proposal to be outlined and linked to any relevant CU plans.

Risk Assessment

When conducting a CM risk assessment, the following points should be considered in the context of your own credit union (CU) with its individual business model characteristics, financial performance, and risk profile.

There are a lot of areas to consider but each item mentioned below under the various categories of risk that the CU cannot currently address but would intend to, can form part of the CU's CM Risk Mitigation Plan arising from the initial risk assessment across a timeline that is feasible for the CU. This will provide a roadmap for where the CU aims to get to and in what timescale, which should be linked to the scale and complexity of the CU.

1. Strategic Risk Considerations

1.1. Does the CM proposal align with any of the CU's strategic objectives? If so, which one(s)? For example, a strategy to support the goal of improving the CU's operational resilience.

1.2. Has the CU confirmed that the chosen cloud-based solution incorporates scalability, that it will be able to increase or decrease capacity, and associated costs, to adjust to fluctuating business demands in the future? For example, increases in traffic, storage, computing power, and bandwidth as may be needed for the CU's business going forward.

1.3. Given the potential price differences between on-premises software solutions and cloud-based solutions, if part of the strategic decision-making process is to avail of cost savings in this area, has the CU confirmed that those proposed cost savings are realistic and achievable? Engagement with other CUs who have already completed this process could be of benefit in this regard, particularly if they have conducted their own lessons learned exercise post CM.

1.4. If a decision to migrate to the cloud has been made, has the CU confirmed that it will make a conscious effort to maximise the strategic benefits and efficiencies associated with a move to the cloud and sought appropriately qualified advice in this regard?

2. Governance Risk Considerations

2.1. Has a clear CM proposal and rationale been submitted to Board for approval?

2.2. Has an appropriate budget been approved for the CM project?

2.3. Have reporting arrangements been established to monitor and manage spending during the project?

2.4. Have ongoing Key Performance Indicators (KPIs) been defined for monitoring and review both during and after CM?

2.5. Has responsibility been assigned to a CU officer, or other appropriate person acting on the CU's behalf, to monitor and report on system and Outsourced Service Provider (OSP) performance on an ongoing basis?

3. Operational Risk Considerations

Outsourcing Risk Considerations

3.1. Has appropriate due diligence been conducted on the chosen cloud-based OSP? The due diligence process should include review of the OSP's security protocols, data protection policies, industry-standard certifications, business continuity plans etc.

3.2. Have relevant OSP Service Level Agreements and Data Processing Agreements been updated to reflect new cloud-based service?

3.3. Will the CM project improve IT support response times? For example, when technical support might have previously required an on-site visit but can now be completed centrally/remotely.

3.4. Could the move to the cloud result in an increase in the CU's dependency on the chosen OSP? If so, what other risk mitigation controls can be introduced in this regard?

3.5. Does CM result in a higher concentration risk in terms of a more limited number of cloud-based service providers available to the CU going forward or are more options now available to the CU?

3.6. Does the choice of CM OSP increase the concentration risk of systems failure affecting a wider range of CUs at the same time in the event of a shared disruption event?

CM Project risks

3.7. Is the CU located in an area well serviced with reliable broadband connection, and alternates available, if necessary, for operational resilience?

3.8. Does the CU have a comprehensive inventory of their current systems, data, databases and servers and their interdependencies? Or will the chosen CM OSP assist in conducting this analysis on the CU's behalf? If that is the case, a CU review stage will be important to ensure all relevant systems etc. have been identified and any material CU-specific customisation flagged sufficiently in advance.

3.9. Is there a clear understanding of the level of criticality of each of the systems being considered for migration to the cloud? The responses to 3.8 and 3.9 will impact on the most appropriate choice of migration strategy. Available migration treatments include:

- 3.9.1. Retain
- 3.9.2. Retire
- 3.9.3. Re-Hosting
- 3.9.4. Re-Platform
- 3.9.5. Re-Engineer
- 3.9.6. Replace

3.10. Has the CU decided as to whether all the CU's systems will be migrated to the cloud or is there an unavoidable requirement for any legacy system(s) to remain on-premises? This could have material implications for potential cost savings, achievable efficiencies etc. and could incur increased cost if integration work is required to ensure legacy on-premises elements of the CU's infrastructure continue to operate seamlessly with cloud-based elements. In this situation, reliable connectivity between on-premises and cloud-based systems will be vital to ensure ongoing data synchronization and data integrity.

3.11. If there are any systems which must remain on-premises, have any relevant recommendations been made by the CM OSP as to how they may best be handled going forward? Do any of these legacy systems pose a risk to the new cloud-based architecture?

3.12. Has the CU (or a suitably qualified OSP acting on the CU's behalf) conducted a thorough readiness assessment of the CU's current infrastructure and applications, as well as their interdependencies, prior to engaging in the CM project?

3.13. Has the OSP supplied a detailed project plan including a definition of the scope of the CM proposal and key project deliverables which accurately reflects the scale and complexity of the CU's current infrastructure?
3.14. Has the CU appointed an internal project manager (or other qualified person to act on the CU's behalf) to work with the OSP during the CM process and confirm project optimisation at all stages of the CM?
3.15. Has the CU's ICT infrastructure service provider confirmed that the CU's infrastructure is compatible with the proposed CM project, or made proposals for changes required to complete successful CM?
3.16. Have appropriate timelines been agreed between the CU and the CM OSP?
3.17. Have all interconnected software applications in use at the CU been sufficiently tested in advance of CM to confirm compatibility and ensure they will perform at expected level post migration?
3.18. Has a comprehensive testing programme been completed successfully prior to CM?
3.19. Has a process been agreed between the CU and the CM OSP for tracking project risks, issues, and escalations to ensure proper accountability and a resolution path?
3.20. Is there a clear path to achieving appropriate knowledge transfer during the project to enable ongoing effective management of the cloud platform, if required?

Other Operational Risk Considerations

3.21. Has the CU's operational resilience framework been updated to reflect the new cloud-based infrastructure?
3.22. Has the CU confirmed that anticipated operational resilience and disaster recovery improvements will materialise through this CM project? For example,
    3.22.1. Does the CM improve operational resilience arrangements in terms of ease of access and speed of restoration? What impact will it have on the CU's Recovery Time Objectives and Recovery Point Objectives?
    3.22.2. Will the CU be less dependent upon access to the CU building either out-of-hours or in the event of a disruptive event preventing physical access?
    3.22.3. Will the CM project result in the minimisation of system downtime and/or data loss in the event of a natural disaster or system failure?
    3.22.4. Can software upgrades be more streamlined once cloud-based?
    3.22.5. Will the CM facilitate remote or hybrid working arrangements if desired?
3.23. Has a robust access control system been put in place with privileged access to relevant areas and/or functionality?
3.24. Has the CU integrated the cloud-based solution(s) into its incident response plans?
3.25. Has the CU reviewed its cybersecurity insurance policy to ensure that it remains aligned with the investment in cloud-based technology, including running costs, replacement costs etc.?
3.26. Has the CU confirmed who is responsible for monitoring and reporting on suspicious activity around cloud configurations?
3.27. Has responsibility been assigned for subjecting the cloud-based solution to regular independent penetration testing, threat assessment and reporting to CUs on the outcome?

3.28. Has a cloud monitoring system, including detective controls, been established to ensure visibility by the CU in relation to ongoing compliance with relevant requirements, application performance, resource usage and potential security threats? Monitoring relevant cloud metrics will assist the CU (or a service provider acting on their behalf) to mitigate the associated risks by establishing an early warning system, monitoring control effectiveness, and responding promptly to incidents. Is reference to such monitoring/reporting arrangements included in the SLA?

3.29. Is it possible to make any operational productivity improvements or avail of associated efficiencies to maximise the return on investment in the CM project?

3.30. Have relevant procedures been updated or removed as appropriate? Remember it is important not to simply focus on replicating current procedures using cloud-based solutions without considering the value of the process itself and whether there are better options available using this new infrastructure.

3.31. If process changes are involved in the CM project which will impact on CU officers delivering CU services, has appropriate and timely training been planned for affected CU officers? It will be important to ensure all affected CU officers are made aware of any process or workflow changes in advance and the rationale for same in order to achieve cultural buy-in, make the transition as smooth as possible and hopefully avoid any hindrances to the migration process. Change can be challenging for many people irrespective of the benefits for them and/or the CU. Recognising effort and progress through the migration process can help CU officers adapt to the new cloud environment and maximise the benefits in a timely manner.

3.32. Can the CM project provide more options for CU staff in terms of remote or hybrid working arrangements or non-standard working hours/patterns, if desired?

Data Protection Risk Considerations

Moving to the cloud usually signifies less on-site data security concerns in terms of physical access to servers but can also introduce new data protection risks such as security of data in transit and data at rest off-site.

3.33. Has the CU confirmed which legal jurisdiction(s) their data in transit will move through and confirmed that this is in compliance with GDPR?

3.34. Has the CU confirmed which legal jurisdiction their data at rest will reside in and confirmed that this is in compliance with GDPR?

3.35. Has a rigorous data validation and error-checking testing programme been completed on the CU's data and systems prior to CM?

3.36. Has a robust system of data management been put in place post migration? Including but not limited to, secure deletion of data as and when appropriate, in compliance with legislation, regulation and internal policy.

3.37. Has the CU arranged for secure disposal of redundant hardware post migration (including certification of data destruction where appropriate) while allowing sufficient time to monitor performance in order to retain the capability to revert to server solution in the event of a material issue arising during or within reasonable time after the migration process?

4. Environmental Risk Considerations

4.1. Has the CU established the impact CM will have on its own carbon footprint? For example, will it:
  4.1.1. Reduce power consumption with removal of server(s)?
  4.1.2. Reduce need for specific 24/7 air conditioning in server room/area?
  4.1.3. Reduce need for humidity control environment for server(s)?

4.2. However, it is worth noting that server farms do have a significant carbon footprint themselves, so CM is not all positive from an environmental risk perspective.

5. Capital Risk Considerations

5.1. Does the CU have sufficient capital available to invest in the CM project without negatively impacting on legislative/regulatory capital requirements?

6. Financial Risk Considerations

6.1. Has a cost/benefit analysis been completed for the CM proposal? For example, are there cost savings to be made on back-up arrangements as compared with server mirroring for example?

6.2. What are the financial cost implications for the CU of moving away from buying, maintaining, and periodically replacing on-site servers?

6.3. Has a clear breakdown been provided to the CU of costs of migration as distinct from on-going costs?

6.4. Has a CU officer been assigned to monitor project implementation costs to ensure they remain within approved budget?

6.5. Has a cloud monitoring process been put in place to optimise cost effectiveness? Cloud monitoring usually involves KPIs such as system downtime, data breaches, resource allocation or misallocation. Such a monitoring system will be particularly important if, for example, the cost/charging structure is linked to cloud resource usage.

7. Legal/Compliance/Conduct Risk Considerations

7.1. Has the cloud service provider confirmed that their solution meets industry best practice in terms of both digital and physical security measures?

7.2. Has the cloud service provider confirmed that the solution complies with GDPR?

7.3. Has the cloud service provider confirmed that the solution complies with Payment Card Industry Data Security Standard if applicable?

7.4. Has the cloud service provider confirmed that the solution complies with any other industry requirements applicable to the specific activity being migrated to the cloud?

7.5. Is a post migration lessons-learned exercise planned for the CU post CM?

8. Reputational Risk Considerations

8.1. In the event of increased concentration risk as mentioned in 3.6 above, more CUs are likely to be affected by the same issues which could result in more widespread

reputational damage in the event of a disruptive incident. Consider the potential reputational risk which could be associated with such an event and how the CU might mitigate the risk of reputational damage in this situation. For example, does the CU have contact number(s) for a public relations expert who might be called upon in an emergency to assist the CU to manage the external communication process as part of its ongoing operational resilience framework? Has the CU updated its Communications Plan accordingly?

8.2. It is particularly important to ensure data security and regulatory compliance are maintained during and after CM as outlined above in the Operational Risk Considerations section. Failure to do so could result in data breaches, regulatory fines, and therefore associated reputational damage amongst members.

9. Risk Evaluation

Based on the answers to the above questions and for the purpose of this particular risk assessment, key summary risks should be evaluated by the RMO to determine inherent and residual risk. Some examples specific to this risk assessment (this is not an exhaustive list) could include:

CM Project-Related Risks

- Risk of incompatibility between the CU's existing infrastructure and the proposed cloud environment particularly in respect of legacy systems, highly customised applications, and/or other third-party software applications.
- Risk of data loss, corruption, and/or unauthorised access to CU data during migration and post-migration.
- Risk of failure to have an appropriate roll-back plan in place in the event of an issue with migration.
- Risk of failure to meet regulatory expectations or industry standards for cloud-based solutions.
- Risk of failure to appropriately manage project costs leading to cost overruns.
- Risk of failure of anticipated operational resilience improvements to materialise.
- Risk of loss of control over the CU's infrastructure making it more difficult to manage from either an operational and/or cost perspective.

The above risks could be used as a starting point for the RMO to create their own CM Project risk portfolio in the CU's risk management software where the risk scoring functionality could be used to flesh out the CM project risk register based on the findings of this CM proposal risk assessment. Different and/or additional user-added risks may be appropriate depending on the CU's own specific project and the associated OSP project plans. The 33 questions listed in Appendix 1 by category and also listed in Appendix 2 by migration phase may assist in this regard. This project-related portfolio should be excluded from the CU's general risk register as they are limited to the completion of the project itself.

If desired, the RMO could use the software functionality to link the project risks to the relevant ongoing risks which form part of the standard CU-wide risk register. Non-exhaustive examples of such risks are also listed below.

Ongoing Risks

- Failure of a Cloud service provider to deliver service
- Ineffective governance and integration of the Operational Resilience Framework
- ICT & Cyber Resilience strategies not effectively integrated with Operational Resilience
- Hardware/Software failure of a key IT system
- Confidential information being disclosed to unauthorised parties
- Sensitive information held offsite being lost or stolen
- Failure to comply with the Data Protection laws of the state
- Failure to maintain an appropriate information systems change management policy
- Failure to detect and respond to a cybersecurity breach in a timely manner
- Failure to appropriately and effectively manage a cybersecurity incident
- Poor Configuration Management
- Inadequate management of user access
- Inadequate cyber protection at the network boundary
- Failure to have an appropriate business continuity plan in place
- Failure to have appropriate outsourcing agreements in place
- Failure to have appropriate insurances in place

An example of how this could be displayed is as follows:

1) Risk of			
	Likelihood	**Consequence**	**Inherent Risk**
Pre-Controls			
Controls In Place		**Possible Additional Control Measures**	
	Likelihood	**Consequence**	**Residual Risk**
Post Controls			

If the CU uses risk management software, screenshots of the appropriate risk scoring screens could be dropped into this section of the risk assessment.

Summary

This section of the CM risk assessment should summarise the key areas of risk which the Board of Directors should be considering when discussing CM risks and give the opinion of the RMO as to whether existing risk mitigation controls would be expected to be effective in mitigating the risks associated with CM risk with a very clear rationale if that is the case, or whether additional identified controls would be required to bring the residual risk within the CU's risk appetite. Any key dependencies including resources and timelines should also be summarised here.

Any items mentioned under the various risk categories above which are relevant but not yet available to the CU, should form the basis of the CM Risk Mitigation Plan.

Appendix 1 – Cloud Migration Risk Assessment Checklist by Risk Category summarises the key elements required under each risk category.

Appendix 2 – Cloud Migration Risk Assessment Checklist by Migration Phase includes the same items as Appendix 1 but due to the nature of this particular topic is organised in order of pre-migration, migration and post-migration phases of the project.

If you have any questions regarding this guidance document or require further assistance, please contact me on +353 86 1762363, or email sandie.oleary@calqrisk.com

Appendix 1 – Cloud Migration Risk Assessment Checklist by Risk Category

Ref No.	Assessment Element	Completed Yes/No/Not Applicable	Within CU's Risk Tolerance Yes/No/Not Applicable
Strategic Risk			
CMSTR01	Has the board confirmed that the CM project aligns with the CU's strategic plan?		
CMSTR02	Has the CU sought confirmation from others who have completed a similar CM project that the associated strategic objectives were achieved?		
Governance Risk			
CMGOV01	Has the Board approved the CM project and budget?		
CMGOV02	Have CM project reporting arrangements & KPIs been established?		
CMGOV03	Has responsibility for monitoring and reporting on CM project progress been assigned?		
CMGOV04	Has responsibility for post-migration ongoing monitoring and reporting on the cloud-based system been assigned?		
Operational Risk			
CMOPE01	Has due diligence been completed on chosen CM OSP?		
CMOPE02	Have relevant SLA(s) and Data Processing Agreement(s) been updated or new SLA & DPA introduced?		
CMOPE03	Has the CU confirmed adequate broad band connection in area?		
CMOPE04	Is there a comprehensive inventory of current systems, data, databases, servers, and their interdependencies in place?		
CMOPE05	Has a migration strategy been confirmed based on system criticality?		
CMOPE06	Has a readiness assessment been completed for the CU's current infrastructure and applications?		
CMOPE07	Has a detailed project plan been provided by the OSP including scope, timelines etc.?		
CMOPE08	Has a project manager (internal or external) been assigned to act on the CU's behalf and monitor project risks?		
CMOPE09	Has a comprehensive programme of pre-migration testing been successfully completed?		
CMOPE10	Has an appropriate programme of knowledge transfer been established?		
CMOPE11	Has the CU confirmed compliance with GDPR requirements?		
CMOPE12	Has a rigorous data validation and error-checking programme been completed prior to CM?		
CMOPE13	Has a post-migration data management system been implemented?		

CMOPE14	Has any redundant hardware been disposed of appropriately including certification of data destruction where appropriate?		
CMOPE15	Has the CU's operational resilience framework been updated?		
CMOPE16	Has a cloud monitoring system been established?		
CMOPE17	Have associated procedures been updated or replaced?		
CMOPE18	Has relevant training been delivered?		
CMOPE19	Has a formal sign-off on successful migration been completed by both the OSP and the CU?		
Environmental Risk			
CMENV01	Has the CU established the impact of the CM project on its carbon footprint?		
Capital Risk			
CMCAP01	Can the CU afford the capital investment without negatively impacting its regulatory capital requirements?		
Financial Risk			
CMFIN01	Has a cost/benefit analysis been completed?		
CMFIN02	Has responsibility been assigned for monitoring & reporting on project implementation costs?		
CMFIN03	Has a post CM cloud cost monitoring process been established if appropriate?		
Legal/Compliance/Conduct Risk			
CMLCC01	Has it been confirmed that the CM solution meets industry best practice standards in all relevant areas?		
CMLCC02	Has a post-migration lessons learned exercise been completed?		
Reputational Risk			
CMREP01	Has a determination been made as to whether the CM increases the industry-wide concentration risk and therefore the potential reputational risk to the CU?		
CMREP02	If the reputational risk has increased, has the CU introduced appropriate controls?		

Appendix 2 – Cloud Migration Risk Assessment Checklist by Migration Phase

Ref No.	Assessment Element	Completed Yes/No/Not Applicable	Within CU's Risk Tolerance Yes/No/Not Applicable
Phase 1: Pre-Migration			
CMSTR01	Has the board confirmed that the CM project aligns with the CU's strategic plan?		
CMSTR02	Has the CU sought confirmation from others who have completed a similar CM project that the associated strategic objectives were achieved?		
CMGOV01	Has the Board approved the CM project and budget?		
CMGOV02	Have CM project reporting arrangements & KPIs been established?		
CMOPE01	Has due diligence been completed on chosen CM OSP?		
CMOPE02	Have relevant SLA(s) and Data Processing Agreement(s) been updated or new SLA & DPA introduced?		
CMOPE03	Has the CU confirmed adequate broad band connection in area?		
CMOPE04	Is there a comprehensive inventory of current systems, data, databases, servers, and their interdependencies in place?		
CMOPE05	Has a migration strategy been confirmed based on system criticality?		
CMOPE06	Has a readiness assessment been completed for the CU's current infrastructure and applications?		
CMOPE07	Has a detailed project plan been provided by the OSP including scope, timelines etc.?		
CMGOV03	Has responsibility for monitoring and reporting on CM project progress been assigned?		
CMOPE09	Has a comprehensive programme of pre-migration testing been successfully completed?		
CMOPE10	Has an appropriate programme of knowledge transfer been established?		
CMOPE11	Has the CU confirmed compliance with GDPR requirements?		
CMLCC01	Has it been confirmed that the CM solution meets industry best practice standards in all relevant areas?		
CMOPE16	Has a cloud monitoring system been established?		
CMOPE17	Have associated procedures been updated or replaced?		
CMOPE18	Has relevant training been delivered?		
CMCAP01	Can the CU afford the capital investment without negatively impacting its regulatory capital requirements?		
CMFIN01	Has a cost/benefit analysis been completed?		
CMFIN02	Has responsibility been assigned for monitoring & reporting on project implementation costs?		

CMREP01	Has a determination been made as to whether the CM increases the industry-wide concentration risk and therefore the potential reputational risk to the CU?		
CMREP02	If the reputational risk has increased, has the CU introduced appropriate controls?		
Phase 2: Migration			
CMOPE12	Has a rigorous data validation and error-checking programme been completed prior to CM?		
CMOPE08	Has a project manager (internal or external) been assigned to act on the CU's behalf and monitor project risks?		
CMOPE19	Has a formal sign-off on successful migration been completed by both the OSP and the CU?		
Phase 3: Post-Migration			
CMGOV04	Has responsibility for post-migration ongoing monitoring and reporting on the cloud-based system been assigned?		
CMOPE13	Has a post-migration data management system been implemented?		
CMOPE14	Has any redundant hardware been disposed of appropriately including certification of data destruction where appropriate?		
CMOPE15	Has the CU's operational resilience framework been updated?		
CMENV01	Has the CU established the impact of the CM project on its carbon footprint?		
CMFIN03	Has a post CM cloud cost monitoring process been established if appropriate?		
CMLCC02	Has a post-migration lessons learned exercise been completed?		