TechNote

New Capital Model Solution

Version: 0.6

# Document control

**Amendment History**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version** | **Release Date** | **Effective Date** | **Amended By** | **Comments** |
| 0.1 | 07/12/2018 |  | Arvind Surani | First draft |
| 0.2 | 10/12/2018 |  | Arvind Surani | Updated after initial review by GHO IT. |
| 0.3 | 11/12/2018 |  | Martin Parrott | Updated with Design Issues table |
| 0.4 | 22/03/2019 |  | Arvind Surani | Updated after feedback and to include further design detail from M&GPru Enterprise Services, WTW and SecondFloor. Summary of key design decisions has also been included in this document (incorporating feedback received on KDD document v0.7). |
| 0.5 | 09/05/2019 |  | Arvind Surani | Incorporated latest feedback, and final details on infrastructure. |
| 0.6 | 23/05/2019 |  | Arvind Surani | Updated after further feedback, and added David as an approver. |

**Document Information**

|  |  |
| --- | --- |
| **Document…** | **Details** |
| Title | TechNote New Capital Model Solution |
| Prepared by | Arvind Surani |
| Information Classification | Restricted |
| Owner / Location | Ashwin Tandlam / GHO IT |

**Approvals List**

| **Name** | **Position** | **Signature / Email html** | **Date Approved** |
| --- | --- | --- | --- |
| Ashwin Tandlam | Architecture Manager |  |  |
| JC Le Saux | Senior Manager |  |  |
| David Van Der Merwe | Risk Modelling Manager - Capital Modelling |  |  |

**Distribution List**

| **Name** | **Position** |
| --- | --- |
| Louse Tennant | Manager SII Platform Applications |
| Paul Ross | Senior Manager Business Systems |
| Simon Daniell | SII Technical Team Lead |
| Ola Olaopa | Project Manager, Actuarial Systems |
| Barry Remzi | GHO Security Manager |
| Robert Baskerville | GHO Security |
| Lailesh Jinan | M&GPru Enterprise Services Project Design Consultant |

**Related Documentation**

| **Title** | **Owner** |
| --- | --- |
| ICM Technology Design Overview v5.4 - ICM Replacement | Paul Ross |
| ICMI\_R-001 - RAFM project Management\_1\_0 | JC Le Saux |
| ICMI\_R-002\_ICM\_components\_with\_ICM\_Project\_1\_0 | JC Le Saux |
| ICMI\_R-003 - ICM Runs outputv1\_0 | JC Le Saux |
| ICM - RiskAgility FM - Integration\_v16\_v3 | WTW |
| ICM Database Options v0.4 | Paul Ross |
| Solvency II KDD Towers Watson Vgrid v0.7 | Paul Ross |
| Storage Design - New Capital Model Solution v1.0 | Paul Ross |

Contents

[Document control 2](#_Toc4146935)

[Contents 4](#_Toc4146936)

[1. Introduction 5](#_Toc4146937)

[1.1. Topic 5](#_Toc4146938)

[1.1. Scope 5](#_Toc4146939)

[1.1.1. In Scope 5](#_Toc4146940)

[1.1.2. Out of Scope 5](#_Toc4146941)

[1.2. Intended Audience 5](#_Toc4146942)

[2. Business Solution Design 6](#_Toc4146943)

[2.1. High Level Business Requirements 6](#_Toc4146944)

[2.2. User Story / Use Case 6](#_Toc4146945)

[2.3. User Context 6](#_Toc4146946)

[2.4. User locations 7](#_Toc4146947)

[2.5. Key Design Constraints 7](#_Toc4146954)

[2.6. Dependencies 7](#_Toc4146956)

[2.7. Risks 8](#_Toc4146957)

[2.8. Issues 8](#_Toc4146960)

[2.9. Work carried out to date 8](#_Toc4146964)

[2.10. Key design decisions summary 9](#_Toc4146965)

[3. Technical Solution Design 10](#_Toc4146966)

[3.1. Overview of Technical Solution 10](#_Toc4146990)

[3.1.1. System Components 12](#_Toc4146991)

[3.2. RAFM Execution Server Components 14](#_Toc4146992)

[3.2.1. ICM vGrid job execution 16](#_Toc4146993)

[3.3. Shared storage design 18](#_Toc4146995)

[3.4. Network Connectivity 20](#_Toc4146997)

[4. Physical Architecture 21](#_Toc4146998)

[4.1. Current State 21](#_Toc4146999)

[4.2. Target State 23](#_Toc4147000)

[4.3. Physical/Virtual Deployment 25](#_Toc4147001)

[4.3.1. Server Specification 25](#_Toc4147003)

[4.4. Design Assumptions 30](#_Toc4147004)

[5. Security 31](#_Toc4147005)

[5.1. Authentication & Authorisation 31](#_Toc4147006)

[5.2. Data 31](#_Toc4147007)

[Glossary 33](#_Toc4147008)

# Introduction

* 1. Topic

The ICM (Internal Capital Model) solution is used by Prudential GHO and BU actuarial teams to build and run the full group wide simulations needed to produce the required group consolidated results to support external and internal needs.

As part of a dedicated programme and following a comprehensive market review, a replacement for the calculation components of the current ICM solution has been identified. The new ICM solution is from the vendor Willis Towers Watson, using their technology solution RAFM (Risk Agility Financial Modeller) and vGrid (cloud-enabled grid).

The implementation approach is Software as a Service (SaaS), and access to the solution will be required across all geographies. Access to the solution will be through both a desktop implementation of RAFM and via a new instance of the SecondFloor ICM workflow engine.

## Scope

## In Scope

* High level technical design for the new Internal Capital Model solution

## Out of Scope

* Functional details of the solution.

## Intended Audience

This note represents the basis for the high-level technical design of new Internal Capital Model solution. The intended audience is GHO Capital Modelling, GHO Security and M&GPru Enterprise Services.

# Business Solution Design

## High Level Business Requirements

The requirements of this solution are detailed in the following set of documents.

* ICMI\_R-001 - RAFM project Management\_1\_0
* ICMI\_R-002\_ICM\_components\_with\_ICM\_Project\_1\_0
* ICMI\_R-003 - ICM Runs outputv1\_0

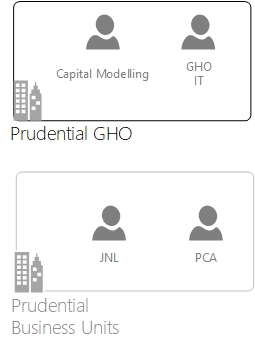
A summary of the requirements are also maintained in the ICM Technology Design Overview document.

## User Story / Use Case

The following use cases have been modelled for the solution:

* lite model development process
* risk scenario generation
* capital model calculation run standard results
* capital model calculation run lite model detailed output results (scheduled reports)
* post processing

## User Context



The total number of users across all Business Units is about 100 users. However, the majority of these users will be light users, who will access the system on an infrequent basis.

## User locations

The solution is to be used on a group wide basis for a limited number of users. These include GHO Reporting team, PCA and JNL business units. Support team and ICM development team complete the set of users.

GHO Users

* London

PCA Users

* Hong Kong

JNL Users

* Lansing

## **Key Design Constraints**

The following design constraints exist in the solution:

| **Constraint** | **Impact of constraint** | **Owned By** |
| --- | --- | --- |
| Operational separation of Prudential plc from MandGPru, is moving all GHO systems onto cloud-based data centres. | * Design of the new solution should take into consideration a migration of all system components to a cloud-based deployment | Project |

## **Dependencies**

|  |  |  |
| --- | --- | --- |
| **Service** | **Dependency on** | **Owner of dependency** |
| ICM interface user access for JNL users | The project has a dependency on the continued provision of an alternative desktop access method for the ICM user interface, for JNL users.  JNL have decommissioned direct access to Citrix virtual desktop (GWA portal), which is currently used to access to the ICM user interface. JNL IT have provisioned a “cocooned” virtual desktop with Citrix, only for the specific users that require access to GHO systems. | Project |

## **Risks**

|  |  |  |
| --- | --- | --- |
| **Risk** | **Action** | **Owner** |
| The project has a has a dependency on skilled resources across a number of vendors (WTW, SecondFloor, M&GPru Enterprise Services). There is a risk that the project is delayed due to resourcing constraints. | Work closely with all vendors to ensure project delivery is progressing to schedule. | Project |
| The operational separation of MandGPru from Prudential plc will result in network separation of GHO from the Woking / Hayes data centres. The new ICM solution is to be implemented in Woking / Hayes data centres, prior to operational separation. There is a risk to the continuity of the service. | Ensure appropriate agreements are in place for GHO to continue with the shared use of Woking / Hayes data centres. | Project |

## **Issues**

The agile nature of this project and its challenging timescale have necessitated moving forward with the provision of infrastructure without a design, the following are the key issues – dependencies are on deliverable artefacts and impact will be on the project cost / timeline / quality. These are NOT Key Design Decisions which are documented elsewhere.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Issue ID | Issue | Description | Artefact Dependency | Impact on Project | Ownership |
| #1 | Second Floor Agent Design | Performance requirements are not available as the performance characteristics of the code will depend on the structure of the models the throughput and the grid performance | Technote  Application Solution Overview  Storage Design  Sequence Diagrams | Cost - Time - Quality | Second Floor |

## **Work carried out to date**

A proof of concept was completed with WTW in Q2 2018. Also, the RAFM client has been installed and packaged for GHO desktop devices.

JNL and PCA have confirmed that the RAFM client can be installed on their desktop devices. The activity to formally install and package is scheduled for Q2 2019.

M&GPru Enterprise Services have provisioned the infrastructure across all environments.

SecondFloor have delivered the ICM interface software to enable end to end testing.

WTW have delivered the RAFM TaskRunner software, capital model build and have also provisioned a Prudential GHO vGrid service to enable end to end testing.

## **Key design decisions summary**

A number of key design decisions are detailed in “Solvency II KDD Towers Watson Vgrid v0.7” document, which was issued and reviewed by all the stakeholders during March 2019.

The following table provides a summary of key design decisions, which have now all been incorporated into the design of the solution.

|  |  |  |  |
| --- | --- | --- | --- |
| # | Design topic | Design considerations | Design decision |
| 1 | WTW vGrid tenancy | Single tenancy - increased cost / DR complexity / technical debt  Multi tenancy – fixed release cycles / shared infrastructure | Multi Tenancy agreed and contract with WTW has been signed. |
| 2 | RAFM licence server | On-premise – increased infrastructure cost / impact of GWAN performance / DR complexity  WTW cloud licence service – proven solution / lower cost and complexity | WTW cloud licence service agreed and has been used through all phases of the project. |
| 3 | RAFM executable deployment | GWA portal - increased infrastructure cost / impact of GWAN performance  End user compute device – improved user experience, dependency on BU IT resources | End user compute device deployment agreed. RAFM executable successfully deployed to GHO, PCA and JNL devices. |
| 4 | WTW TaskRunner deployment requirements | Impact to resiliency and ability to execute parallel | Two servers to be deployed in Woking data centre. |
| 5 | JNL retiring Citrix receiver on end user compute devices. | Access to GWA portal via Citrix receiver, is still required for ICM user interface and the ability to upload and download data | JNL have agreed to provide access to specific users of GHO systems, via a “cocooned” virtual desktop with Citrix receiver. |
| 6 | Shared storage requirements across linux / windows platforms | Increased cost and complexity of provisioning a solution that can provide shared storage directly accessible across both platforms | Standard shared storage being provisioned separately for linux and windows platforms. The transfer of data across the platforms will be managed by the ICM application through the use of the ICM database. |
| 7 | Sharing of database infrastructure | Significant reduction in costs achieved through sharing of database infrastructure. The existing database infrastructure has sufficient spare capacity.  TSA agreement will need to be agreed with Dallas. | The ICM and RCT database infrastructure will be shared with Dallas. |

# Technical Solution Design

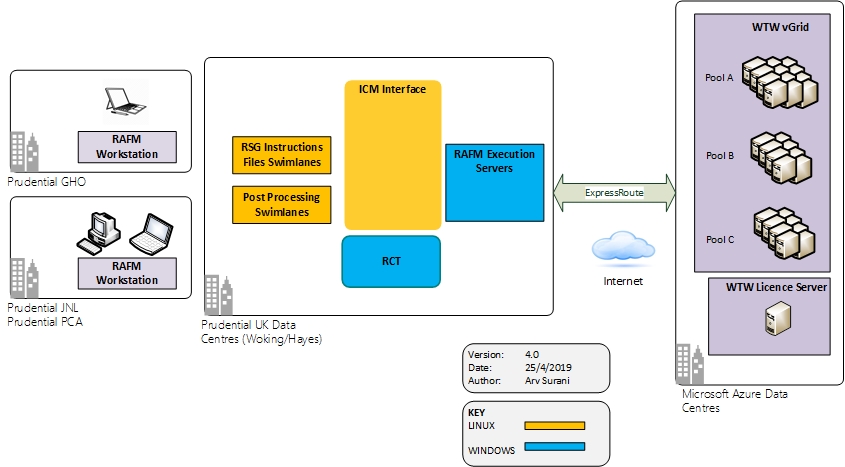
## **Overview of Technical Solution**

The initial Internal Capital Models were produced by the Business Units using an Excel based prototype solution, with the end-state technology solution delivered through a series of staged releases. This system was then moved to a solution that centred around the IBM Algorithmics modelling software and an on-premise high-performance computing (HPC) grid.

The new Internal Capital Model solution uses the Risk Agility FM product from WTW. Also, the new Internal Capital Model solution replaces the on-premise grid with a WTW managed vGrid service, that is flexible and scalable. The vGrid service will be used for both Production and “Sandbox” runs. Users will also have the option to download all the run components from the ICM front end with a view to run/debug their code on a desktop.

To minimise change, components of the existing Internal Capital Model solution have been retained and modified.

The diagram on the following page provides a high-level overview of the new Internal Capital Model solution.

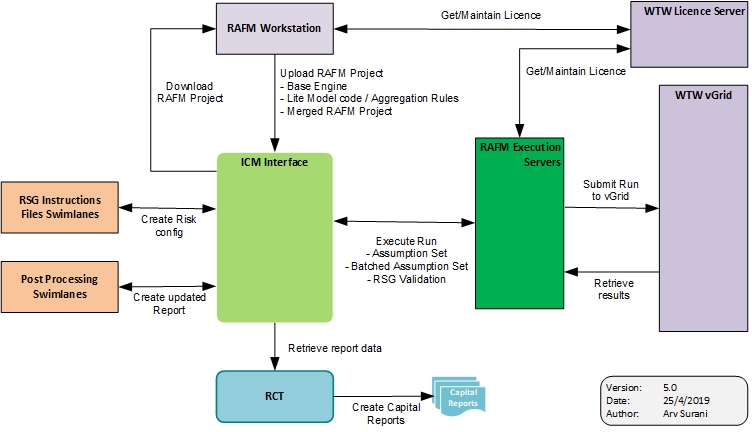


## System Components

The following table provides further detail on the dependent components and systems and integrations.

| System | Role | Impact on Existing System |
| --- | --- | --- |
| RAFM Workstation | Desktop implementation of the RAFM modelling system. This component will be used for the development of Lite models and aggregation rules. | Installation and maintenance of this new client software will be required and will be deployed on end user devices at GHO, JNL and PCA. |
| ICM Interface | Coordination and control mechanism for the ICM solution. | System will be a new instance, that is modified to integrate with RAFM (Workstation + TaskRunner) and to meet new requirements. |
| RSG Instructions Files Swimlane | To provide compute processing to generate RSG instruction set that can be used for the just in time risk scenario generation. | Component will be cloned from existing Internal Capital Model solution. |
| Post Processing Swimlane | To provide compute processing for post processing of vGrid output data, such as BU trimming of group wide data. | Component will be cloned from existing Internal Capital Model solution. |
| WTW vGrid | SaaS component to provide flexible and highly scalable compute capability for the Capital Model simulation. | None |
| WTW Licence Server | SaaS component that validates RAFM licences that are deployed on RAFM Execution Servers and RAFM Workstations. | None |
| RAFM Execution Servers | To enable the ICM interface to integrate with WTW vGrid. Will host SecondFloor RAFM agent and WTW RAFM TaskRunner. | None |
| RCT | Production of final balance sheet reports. | System will be a new instance that is modified to meet updated requirements. |

The diagram on the following page provides a high-level view of the components with data flows.



## **RAFM Execution Server Components**

The diagram on the following page provides further detail on the components within the RAFM execution server. This includes a detailed view of the data flows between the RAFM execution server, ICM interface and WTW services (vGrid, licence server).

The SecondFloor RAFM Agent and the RAFM TaskRunner are new components. The infrastructure design for the RAFM execution servers both in terms of quantity of server and their specification, has been informed by the following:

* CPU / Memory consumption of SecondFloor RAFM Agent
* CPU / Memory consumption of RAFM TaskRunner
* Required number of concurrent vGrid Runs
* Requirement for high availability

WTW have determined that RAFM TaskRunner has a peak memory consumption of 250MB, for a production sized run. The RAFM TaskRunner runs an ETL (Extract, Transform, Load) process to send files to the vGrid service. A single vGrid Run, requires multiple files to be used, however a CPU core is required for each ETL process. Therefore, the concurrent number of ETL processes is bounded by the number of cores on the RAFM execution server.

The SecondFloor RAFM Agent will be required to invoke RAFM TaskRunner, through a command line interface. In addition, the RAFM Agent will also be required to save all returned data from the vGrid Run, in the ICM interface database. SecondFloor have estimated that 3 cores and 3GB of RAM will be required for the RAFM Agent to process 4 concurrent runs.

The design for the production execution servers is detailed as follows:

* 2 servers Woking data centre (active), 2 servers Hayes data centre (passive)
* 12 cores of CPU processing power, 64GB RAM memory for each server

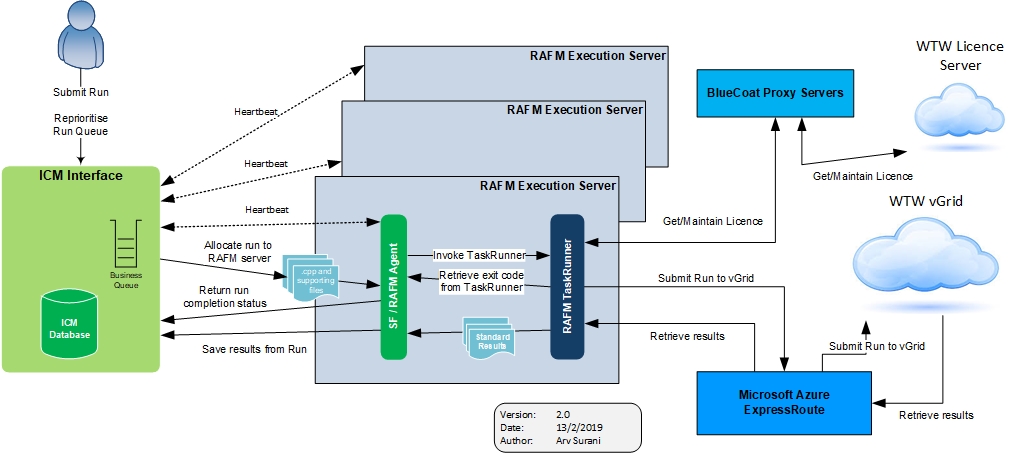
SecondFloor have provided the following detail to provide insight into the ICM application design.

The execution server is identified as a type of batch server. The RSG Instructions Files swimlane and Post Processing swimlane, are also identified as batch servers.

All batch servers announce themselves to the ICM web server during start-up. ICM keeps track of the batch servers by periodically sending heartbeat requests to each one of them. Each batch server responds to the heartbeat request by sending a heartbeat response. The number of batch jobs that can be run concurrently on a given batch server is specified by a configuration property and it can be different for each batch server.

The ICM application also holds the number of pools available on vGrid and manages the queue of jobs that need to be executed on vGrid. The ICM application allocates jobs to an execution server on a round robin basis and keeps track of the assignment and completion of vGrid runs. However, if there is any breakdown of communication between RAFM TaskRunner and vGrid, the ICM application would be unaware of this failure and would assume the run was still executing.

Testing of the execution servers under full load, will be used to accurately determine the number of concurrent runs that each server is able to execute.



## **ICM vGrid job execution**

The following section provides the detailed steps for the execution of a run on vGrid.

**ICM web server**

1. The user triggers a run (Assumption Set -> Run)
2. The run is saved in the database and marked as queued
3. ICM queries the database periodically and makes a list of all queued runs, detailed as follows
   1. RAFM calculation engine supports RAFM runs through TaskRunner and comprises of Assumption Set runs and RSG Standalone runs
   2. RSG engine supports generation of the RSG Instruction set in csv format and comprises of Scenario Assumption Set runs.
   3. Post Processing calculation engine which at present comprises of BU trimmed reports
4. ICM sorts the list of queued runs by creation time and by the business unit that triggered the run (i.e. GHO, PCA, JNL)
5. ICM cycles through this list and for each run it carries out the following:
   1. Attempts to find a batch server that can be used for this run. A batch server can be used for a given run if:
      1. It is available - it has responded to the heartbeat in a timely manner
      2. It is not reserved (we don’t reserve batch servers for vGrid runs so this condition will be true)
      3. Its calculation engine supports the requested type of run (for example an execution server supports 2 types of runs: Assumption Set runs and RSG Standalone runs)
      4. It is currently running fewer concurrent runs than the maximum number of concurrent runs (jobs) supported by that server
   2. If a usable batch server has been found
      1. ICM registers the run for the given batch server (runs are tracked for all batch servers)
      2. Check for available pool in ICM (pool that is enabled and not reserved)
         1. If there is an available pool, reserve the pool and send the run to the given batch server (using JMS messaging)
         2. If there is no available pool, we go to step 5 by taking the next run from the ordered list of queued runs.
   3. If no usable batch server, go to step 3

**Execution server (SecondFloor RAFM agent)**

1. The RAFM agent creates a (temporary) directory for the given run
2. The RAFM agent generates all required files for the run by extracting them from ICM database and writing them to the directory on the execution server
3. The RAFM agent starts RAFM TaskRunner.
4. RAFM TaskRunner loads the files into memory, for the run using an ETL process
5. RAFM TaskRunner zips the files and sends to WTW vGrid for execution
6. Once WTW vGrid execution has completed, results files are transferred back to execution server and unzipped to the directory on the execution server
7. RAFM TaskRunner returns a run execution status code to the RAFM agent
8. RAFM agent saves logs files that are associated with the executed run in the ICM database
9. If the run was successful, the standard results files are saved to the ICM database
10. The RAFM TaskRunner return status code is processed:
    1. If RAFM TaskRunner returns a success code, a successful completion message is sent to the ICM web server through a corresponding JMS message
    2. If RAFM Task Runner returns failure return code, a failed run message is sent to the ICM web server through a corresponding JMS message
11. If configured the run directory is deleted
12. During the run execution the execution server responds to heartbeat requests from the ICM web server and in the heartbeat response message, specifies the ids of runs being executed and the maximum number of runs supported.

**ICM web server**

1. Upon receiving a completion message from the execution server, deregister the run for the given execution server.
2. Release the pool reservation, if there was a pool reserved.
3. Mark the run
   1. Completed successfully for a successfully completion message
   2. Failed for a failure completion message

## **Shared storage design**

There is a requirement for the ICM interface (web server), swimlane servers and RAFM execution servers to access shared data using files. The proposed architecture involves both Linux and Windows servers, and M&GPru Enterprise Services have confirmed that there is currently no standard option for shared storage, that is accessible from both operating systems.

The current Internal Capital Model solution uses IBM GPFS storage to provision data for the on-premise, high performance computing grid. It has been determined that high performance storage such as GPFS is not required, as the new solution no longer requires RSG files to be written to storage prior to Lite Model simulation. Subsequently, there is no longer a case for rapidly accessing sizeable files at the point of processing.

The following considerations have determined the storage design that has been proposed by M&GPru Enterprise Services.

* WTW TaskRunner provides integration with vGrid, and only runs on the windows operating system. This introduced windows servers to the ICM application that was otherwise a linux estate
* M&GPru Enterprise Services Storage team, have informed the project that they currently do not have a standard storage solution that provides shared storage across windows and linux servers

The following diagram provides a high-level view of the storage design.



Windows shared storage [\\files.webservices.group](file://files.webservices.group) for GHO systems is available at Woking/Hayes data centres. However due to the volume requirements, M&GPru Enterprise Services have recommended dedicated file servers for this solution, that provide access to windows shared storage.

As there is currently no existing linux shared storage in Woking/Hayes data centres, new file servers are being provisioned to provide access to linux shared storage. This storage will be accessible from the ICM web server, RSG Instructions Files swimlanes and Post Processing swimlane. The new shared storage will match the service that is available for the existing windows shared storage and will have dedicated severs for production, pre-production and non-production.

This design for the windows and linux shared storage is detailed as follows:

**Storage volume capacity**

The current GPFS solution has 20TB of storage. The new solution will require a reduced amount of storage, as full sets of results data are not being returned from vGrid, with standard results being <50MB. There are a few use cases which will require significantly more data to be held on shared storage. The current estimates for overall volume for shared storage are as follows.

* Windows – 8TB
* Linux – 1TB

The M&GPru Enterprise Services storage team have confirmed that 2TB is available immediately for each platform, and this can be increased to 10TB in 6 months’ time. There are two use cases that have been impacted against the storage design.

* scheduled reports – rather than standard reports, a more detailed report is returned from a vGrid run. This data is expected to have significantly larger volume approaching 1GB in size, but will immediately be zipped and inserted into the ICM database and then deleted from shared storage. This approach has been adopted as the ICM user interface cannot directly access windows shared storage.
* RSG model scenario generation only – the ability to access a full set of RSG scenarios. This data will be written to the windows shared storage, and is to be accessible across all business units. This data is expected to require significant volume (500k RSG will be of the order of 20GB, however initial ICM operations will rely on 100k RSG executions).

**Resilience**

The windows and linux shared storage is provided by a set of virtual servers separated across environments. The underlying storage device has an SLA of 99.9% availability.

**Recoverability**

Both the windows and linux storage is back up as a snapshot in the following manner.

|  |  |  |  |
| --- | --- | --- | --- |
| **Environment** | **Incremental** | **Full** | **Retention  Backup Archive** |
| test, development | daily | weekly | 35 days |
| pre-production | daily | weekly | 35 days |
| production | daily | weekly monthly | 1 Year 7 Years |

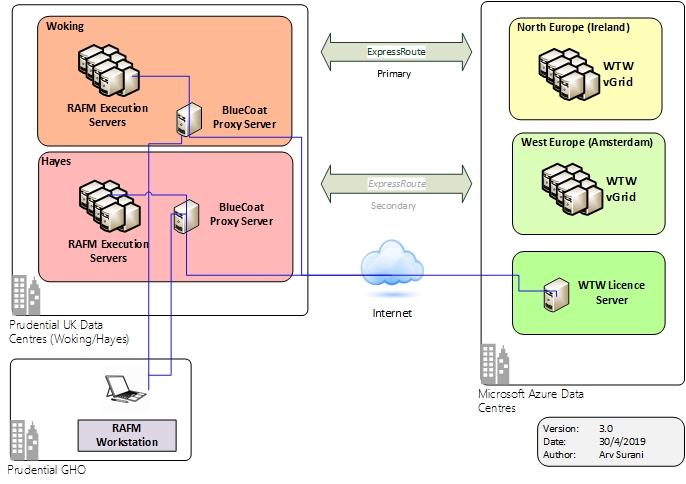
**Disaster Recovery**

The Woking and Hayes data centres communicate through two 8Gbps network connections. The shared storage is active in Woking and passive in Hayes. The storage data is synchronously replicated between Woking and Hayes. Therefore, the RPO (recovery point objective) is close to zero, which means that data loss will be minimal in a disaster event.

Passive network file servers are provisioned in Hayes and would become active during a full failover scenario only. RTO (recovery time objective) for disaster recovery is 24 hours and is in line with the current SLA for GHO systems.

## **Network Connectivity**

The following diagram provides a high-level view of the components of the ICM solution and their network locations.



The connection to Microsoft Azure will be routed via the existing ExpressRoute connection, between Woking/Hayes data centres and Microsoft Azure. The network traffic is directed primarily between Woking data centre and Microsoft Azure. The network connection from Hayes data centre and Microsoft Azure is only utilised as a backup.

The ExpressRoute connection has a maximum of 1 Gbps bandwidth, and currently 700 Mbps is available. The M&GPru Enterprise Services network team have stated that the ExpressRoute connection is shared with M&GPru.

Microsoft network peering will be used within Microsoft Azure to complete the network connection through to WTW vGrid.

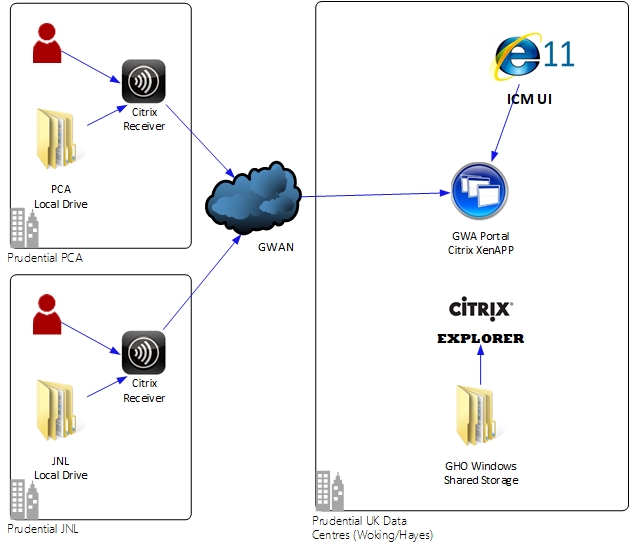
Communication between desktops running RAFM workstation and the WTW licence server utilises the standard internet connectivity which is routed through GHO BlueCoat proxy servers. It should be noted that communication between execution servers and the WTW licence server is routed through the GHO BlueCoat proxy servers.

Users based in PCA and JNL will continue to access the ICM application using the Citrix GWA portal. This provides them with the ability to load business unit specific model data into ICM from local storage. This is achieved through the use of drive mapping on Citrix explorer, which is also available on the GWA portal.

In addition, a new drive mapping is being added to the Citrix explorer, that enables PCA and JNL users to access data held on the GHO provisioned windows shared storage. Access to the shared storage is controlled through the active directory. This utilises the GHO domain (webservices.group) one way forest transitive trust with PCA domain (pru.intranet.asia) and JNL domain (jacksonnational.com).

Permissions will be restricted to ensure that users can only access data that is specific to their business unit.

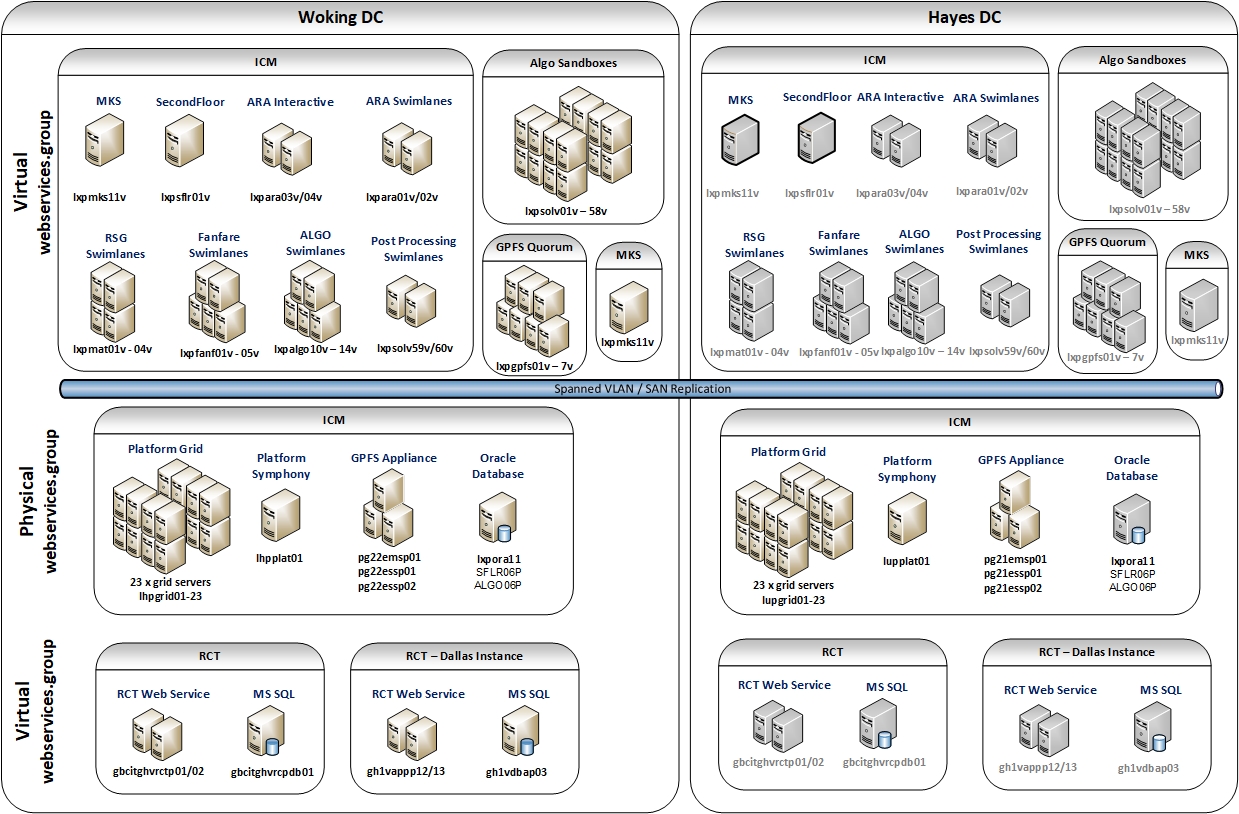
The following diagram provides a high level overview of access through the GWA portal.



# Physical Architecture

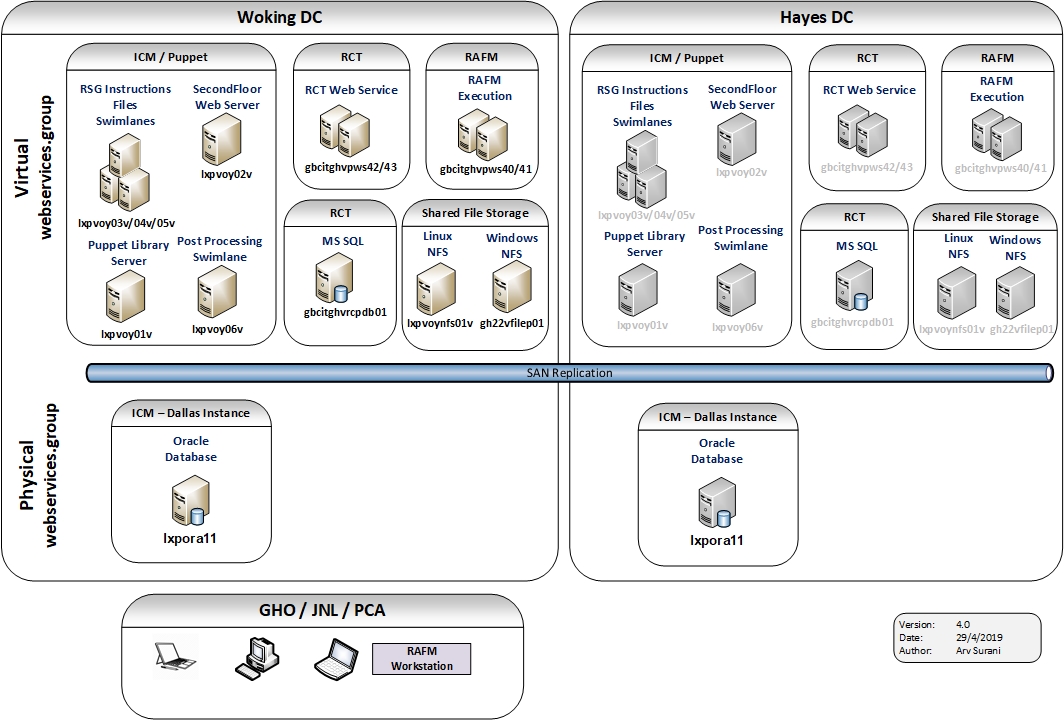
## **Current State**

The diagram on the next page provides details of the current production implementation of the ICM solution.

.

## **Target State**

The following diagram provides a high-level view of the proposed internal infrastructure for the new Internal Capital Model solution.



The following environments are being provisioned for the new Internal Capital Model solution:

* Production (with Disaster Recovery)
* Pre-Production
* Test
  + Environment 1
  + Environment 2
  + Environment 3
* Development

The ICM database for the new solution will be a new instance of an Oracle database on the existing the ICM database servers, across all the environments.

The RCT databases will also be new instances of databases on the existing RCT database servers. However, Dallas are building a new instance of RCT in Production using new infrastructure, to enable early use of the system, prior to separation. Therefore, the RCT database servers will not be shared in the Production environment.

The capacity data in terms of cpu processing, memory, disk input/output, network throughput was reviewed by the capacity planning team, for both sets of database services across all environments. The capacity planning team concluded that there is sufficient spare capacity to co-host new and existing databases.

Sharing of the database infrastructure has enabled a cost-effective option for the initial deployment of new ICM solution, and also ensures that existing IT assets are fully utilised.

The sharing of databases will require an appropriate TSA agreement to be in place, to ensure that the service can continue after operational separation. The TSA agreement will cover the following:

* Maintenance windows across all environments
* Procedure for raising production incidents
* Procedure for planning and implementing changes
* Disaster recovery planning and testing

## **Physical/Virtual Deployment**

## **Server Specification**

The section provides details of the servers across all the environments.

|  |  |  |
| --- | --- | --- |
| Environment | Server | Specification |
| **PRODUCTION** | lxpvoy01v  webservices.group  10.254.88.194  Library Server | CPU: 2 cores  Memory: 12GB  Operating System: RHEL 7.5  VLAN: 488  Storage: 37GB (root), 300GB |
| lxpvoy02v  webservices.group  10.254.88.195  ICM Web Server | CPU: 4 cores  Memory: 12GB  Operating System: RHEL 7.5  VLAN: 488  Storage: 36GB, 12GB |
| lxpvoy03v  webservices.group  10.254.88.196  RSG Instructions Files Swimlane | CPU: 2 cores  Memory: 40GB  Operating System: RHEL 7.5  VLAN: 488  Storage: 36GB, 12GB |
| lxpvoy04v  webservices.group  10.254.88.197  RSG Instructions Files Swimlane | CPU: 2 cores  Memory: 40GB  Operating System: RHEL 7.5  VLAN: 488  Storage: 36GB, 12GB |
| lxpvoy05v  webservices.group  10.254.88.198  RSG Instructions Files Swimlane | CPU: 2 cores  Memory: 40GB  Operating System: RHEL 7.5  VLAN: 488  Storage: 36GB, 12GB |
| lxpvoy06v  webservices.group  10.254.88.186  Post Processing Swimlane | CPU: 2 cores  Memory: 40GB  Operating System: RHEL 7.5  VLAN: 488  Storage: 36GB, 12GB |
| gbcitghvpws40  webservices.group  10.241.96.127  Execution Server | CPU: 12 cores  Memory: 64GB  Operating System: Windows Server 2012R2  VLAN: 1720  Storage: 50GB, 20GB |
| gbcitghvpws41  webservices.group  10.241.96.128  Execution Server | CPU: 12 cores  Memory: 64GB  Operating System: Windows Server 2012R2  VLAN: 1720  Storage: 50GB, 20GB |
| gbcitghvpws42  webservices.group  10.241.96.129  RCT Web Server | CPU: 4 cores  Memory: 16GB  Operating System: Windows Server 2012R2  VLAN: 1720  Storage: 50GB, 20GB |
| gbcitghvpws43  webservices.group  10.241.96.130  RCT Web Server | CPU: 4 cores  Memory: 16GB  Operating System: Windows Server 2012R2  VLAN: 1720  Storage: 50GB, 20GB |

|  |  |  |
| --- | --- | --- |
| Environment | Server | Specification |
| **PRE PRODUCTION** | lhevoy01v  webservices.group  10.254.95.65  ICM Web Server | CPU: 4 cores  Memory: 8GB  Operating System: RHEL 7.5  VLAN: 495  Storage: 36GB, 12GB |
| lhevoy02v  webservices.group  10.254.95.66  RSG Instructions Files Swimlane | CPU: 2 cores  Memory: 32GB  Operating System: RHEL 7.5  VLAN: 495  Storage: 36GB, 12GB |
| lhevoy03v  webservices.group  10.254.95.67  Post Processing Swimlane | CPU: 2 cores  Memory: 12GB  Operating System: RHEL 7.5  VLAN: 495  Storage: 36GB, 12GB |
| gbcitghvrws25  webservices.group  10.240.98.86  Execution Server | CPU: 4 cores  Memory: 8GB  Operating System: Windows Server 2012R2  VLAN: 1598  Storage: 50GB, 20GB |
|  | gbcitghvrws23  webservices.group  10.240.98.245  RCT Web Server | CPU: 4 cores  Memory: 16GB  Operating System: Windows Server 2012 R2  VLAN: 1598  Storage: 50GB, 20GB |
|  | gbcitghvrws24  webservices.group  10.240.98.246  RCT Web Server | CPU: 4 cores  Memory: 16GB  Operating System: Windows Server 2012 R2  VLAN: 1598  Storage: 50GB, 10GB |

|  |  |  |
| --- | --- | --- |
| Environment | Server | Specification |
| **Test**  **Environment 1** | lhdvoy08v  webservices.group  10.254.94.227  ICM Web Server | CPU: 2 cores  Memory: 8GB  Operating System: RHEL 7.5  VLAN: 494  Storage: 37GB (root) |
| lhdvoy06v  webservices.group  10.254.94.225  RSG Instructions Files Swimlane | CPU: 2 cores  Memory: 32GB  Operating System: RHEL 7.5  VLAN: 494  Storage: 37GB (root) |
| lhdvoy12v  webservices.group  10.254.94.232  Post Processing Swimlane | CPU: 2 cores  Memory: 12GB  Operating System: RHEL 7.5  VLAN: 494  Storage: 37GB (root) |
| gbcit22vdws05  webservices.group  10.240.101.246  Execution Server | CPU: 4 cores  Memory: 8GB  Operating System: Windows Server 2012 R2  VLAN: 1501  Storage: 50GB, 100GB |
| gbcit22vdws08  webservices.group  10.240.101.239  RCT Web Server | CPU: 4 cores  Memory: 8GB  Operating System: Windows Server 2012R2  VLAN: 1501  Storage: 50GB, 20GB |
| **Test**  **Environment 2** | lhdvoy05v  webservices.group  10.254.94.224  ICM Web Server | CPU: 2 cores  Memory: 8GB  Operating System: RHEL 7.5  VLAN: 494  Storage: 37GB (root) |
| lhdvoy07v  webservices.group  10.254.94.226  RSG Instructions Files Swimlane | CPU: 2 cores  Memory: 32GB  Operating System: RHEL 7.5  VLAN: 494  Storage: 37GB (root) |
| lhdvoy13v  webservices.group  10.254.94.233  Post Processing Swimlane | CPU: 2 cores  Memory: 12GB  Operating System: RHEL 7.5  VLAN: 494  Storage: 37GB (root) |
| gbcit22vdws03  webservices.group  10.240.101.236  Execution Server | CPU: 4 cores  Memory: 8GB  Operating System: Windows Server 2012 R2  VLAN: 1501  Storage: 50GB, 100GB |
|  | gbcit22vdws07  webservices.group  10.240.101.69  Execution Server | CPU: 4 cores  Memory: 8GB  Operating System: Windows Server 2012 R2  VLAN: 1501  Storage: 50GB, 100GB |
|  | gbcit22vtws02  webservices.group  10.240.101.41  RCT Web Server | CPU: 4 cores  Memory: 16GB  Operating System: Windows Server 2012 R2  VLAN: 1501  Storage: 60GB, 120GB |
|  | lhdvoy09v  webservices.group  10.254.94.228  ICM Web Server | CPU: 2 cores  Memory: 8GB  Operating System: RHEL 7.5  VLAN: 494  Storage: 36GB (root), 12GB |
| **Test**  **Environment 3** | lhdvoy10v  webservices.group  10.254.94.229  RSG Instructions Files Swimlane | CPU: 2 cores  Memory: 32GB  Operating System: RHEL 7.5  VLAN: 494  Storage: 36GB (root), 12GB |
|  | lhdvoy14v  webservices.group  10.254.94.234  Post Processing Swimlane | CPU: 2 cores  Memory: 12GB  Operating System: RHEL 7.5  VLAN: 494  Storage: 37GB (root) |
|  | gbcit22vdws06  webservices.group  10.240.101.68  Execution Server | CPU: 4 cores  Memory: 8GB  Operating System: Windows Server 2012 R2  VLAN: 1501  Storage: 50GB, 100GB |

|  |  |  |
| --- | --- | --- |
| Environment | Server | Specification |
| **DEVELOPMENT** | lhdvoy04v  webservices.group  10.254.94.223  ICM Web Server | CPU: 4 cores  Memory: 8GB  Operating System: RHEL 7.5  VLAN: 494  Storage: 37GB (root) |
| lhdvoy02v  webservices.group  10.254.94.222  RSG Instructions Files Swimlane | CPU: 2 cores  Memory: 32GB  Operating System: RHEL 7.5  VLAN: 494  Storage: 37GB (root) |
| lhdvoy11v  webservices.group  10.254.94.231  Post Processing Swimlane | CPU: 2 cores  Memory: 12GB  Operating System: RHEL 7.5  VLAN: 494  Storage: 37GB (root) |
| gbcit22vdws02  webservices.group  10.240.101.235  Execution Server | CPU: 4 cores  Memory: 8GB  Operating System: Windows Server 2012 R2  VLAN: 1501  Storage: 50GB, 100GB |
|  | gbcit22vdws04  webservices.group  10.240.101.245  RCT Web Server | CPU: 4 cores  Memory: 16GB  Operating System: Windows Server 2012 R2  VLAN: 1501  Storage: 50GB, 100GB |
|  | gbcitghvddb05  intra.dev.local  10.240.101.237  RCT SQL Database Server | CPU: 4 cores  Memory: 16GB  Operating System: Windows Server 2012 R2  VLAN: 1501  Storage: 50GB, 300GB |

|  |  |  |
| --- | --- | --- |
| Description | Server / *Environment* | Specification |
| **Network File Share** | lhdvoynfs01v  webservices.group  10.254.94.230  NFS Storage Server  Linux  *DEVELOPMENT / TEST* | CPU: 4 cores  Memory: 8GB  Operating System: RHEL 7.5  VLAN: 494  Storage: 1TB |
| lhevoynfs01v  webservices.group  10.254.95.69  NFS Storage Server  Linux  *PRE PRODUCTION* | CPU: 4 cores  Memory: 8GB  Operating System: RHEL 7.5  VLAN: 495  Storage: 36GB, 12GB, 1TB |
| lxpvoynfs01v  webservices.group  10.254.88.199  NFS Storage Server  Linux  *PRODUCTION* | CPU: 2 cores  Memory: 40GB  Operating System: RHEL 7.5  VLAN: 488  Storage: 36GB, 12GB, 1TB |
| gh22vfilez01  webservices.group  10.240.101.108  NFS Storage Server  Windows  *DEVELOPMENT / TEST* | CPU: 4 cores  Memory: 8GB  Operating System: Windows Server 2012 R2  VLAN: 1501  Storage: 50GB, 1TB |
|  | gh22vfileu01  webservices.group  10.240.98.87  NFS Storage Server  Windows  *PRE PRODUCTION* | CPU: 4 cores  Memory: 8GB  Operating System: Windows Server 2012 R2  VLAN: 1598  Storage: 50GB, 1TB |
|  | gh22vfilep01  webservices.group  10.240.97.238  NFS Storage Server  Windows  *PRODUCTION* | CPU: 4 cores  Memory: 8GB  Operating System: Windows Server 2012 R2  VLAN: 1720  Storage: 50GB, 2TB |

## Design Assumptions

To meet project timescales a number of working assumptions have been incorporated into the design. These are detailed in the list below.

* The MKS application will not be required for source/version control. It has been assumed that source/version control functionality will not require the provisioning of any new application.

Rationale: MKS has been historically used to store versions of RSG models. This requirement disappears as the RSG models will now be tracked via RAFM base engines. The application support team now use GIT for version control.

* The server specification for the RSG Instructions Files swimlanes is a copy of the existing RSG swimlanes. The assumption is that this specification will be sufficient for the processing requirements of the new RSG Instructions Files swimlanes.

Rationale: Based on the current use cases RSG Instructions Files swimlanes workload is expected to be lower than the existing RSG swimlanes. Therefore, the specification is expected to be sufficient. This may need to be increased in the future, if new use cases are identified.

* It has been assumed that M&G Prudential UK will not require access to the new solution.

Rationale: Operational separation will result in M&G Prudential being a separately listed company.

* It has been assumed that shared storage provisioned for Linux and Windows servers, will have sufficient performance to meet business requirements of the new solution.

Rationale: A requirement for on-premise high-performance storage in the previous solution has been removed by the use of WTW vGrid.

* The existing instance of the production RCT database server will not be used by Dallas.

Rationale: Dallas have started a project to create a new production instance of the RCT application to enable them to use the application prior to separation.

# Security

## **Authentication & Authorisation**

**ICM interface**

Authentication and authorisation will remain the same for the new solution. Users request access through the Access Request system and existing processes will be used for approval. The ICM interface has full role-based access control and user management. Capital Modelling team is the administrator to this system.

The Access Request system will add users to active directory groups setup for ICM interface users. Centrify interrogates the active directory groups and provisions the users on the Linux servers, when the ICM interface is deployed. GHO IT support users are expected to be provisioned direct access to the Linux servers using Centrify.

Single sign-on authentication is enabled through integration with Kerberos.

**RAFM Workstation**

RAFM Workstation product does not provide any user management. The existing security controls on end user devices will be relied upon to provide access control. However, it should be noted that RAFM Workstation will only operate if a licence has been allocated and is validated on a continual basis with WTW licence server.

**RAFM TaskRunner**

RAFM TaskRunner is a windows command line tool and does not provide any user management. The existing security controls on windows servers will be relied upon to provide access control. However, it should be noted that RAFM TaskRunner will only operate if a licence has been allocated and is validated on a continual basis with WTW licence server.

**WTW vGrid**

WTW vGrid is a managed service deployed in Microsoft Azure. This service currently only supports credentials based on Azure Active Directory (AAD) user name and password. These credentials will be stored on the RAFM execution server and held securely using Windows Credentials Manager.

The owners of this password will need to setup a process to ensure they log into vGrid every 90 days to update this account’s password, as well as updating the RAFM TaskRunner configuration. Failure to do so will result in the account being locked out for security reasons.

It is also expected that a limited set of GHO users will also have direct access to the WTW vGrid through a browser-based user interface (web portal). User will be authenticated by manually entering user name and password.

## **Data**

The data classification for the data held in the new Internal Capital Model solution is restricted.

It should be noted that the RCT system holds data that is classified as strictly confidential. The RCT system only sources data from the ICM solution and does not provide a feed of data back to the ICM solution.

* **Secure Data at Rest**

**ICM**

The data is not encrypted at rest in the new Internal Capital Model solution. The data resides in the following locations.

* ICM Oracle database
* Windows shared storage
* Linux shared storage

**WTW vGrid**

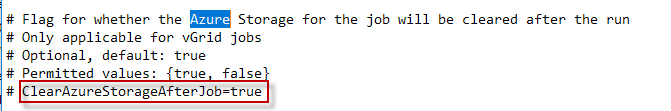
WTW vGrid web portal and its usage information database is multi-tenanted. Data separation is based on assignment of users to a client instance of the portal.

However, the vGrid virtual machines and storage are single tenanted for both primary and secondary data centres. Therefore, stored data is segregated for each client. The following data will be held on vGrid:

* Usage Information – It is a *pay as you go* service therefore core hours used to run on vGrid are recorded
* User Details - stored within our Azure Active Directory tenant
* Client specific data - for instance upper scale of allocated machines, Azure data centre region, contact information for billing.

Data that is related to the capital model is stored in blob storage during a run on vGrid and is deleted after successful job completion. Therefore, this type of data is not expected to be retained in the WTW vGrid service.

TaskRunner configuration will have the following value set and that ensures that the data is not retained on vGrid after a run (including when a run fails):



In addition, the WTW vGrid service for Prudential has been configured with a housekeeping purge setting of 1 day.

**RCT**

It should be noted that data held in the RCT system is encrypted using TDE on the SQL Server database.

* **Secure Data in transit**

**ICM interface**

The ICM interface has a browser-based UI (user interface), that is secured using HTTPS TLS v1.2. The HTTPS encryption is between the load balancer and the end user browser, and not directly on the ICM SecondFloor web server.

**RAFM Workstation**

The UI will only be accessible locally on the end user device.

**RAFM TaskRunner - WTW vGrid**

The transfer of data between RAFM TaskRunner and WTW vGrid is secured using HTTPS TLS v1.2.

**RCT**

RCT has a windows-based client and also an excel add-in. Communication to the RCT web server and these clients is secured using HTTPS TLS v1.0.

# Glossary

|  |  |
| --- | --- |
| **Term** | **Description** |
| PCA | Prudential Corporation Asia – customer facing business unit (multiple Asian countries) |
| GHO | Group Head Office (City of London) |
| JNL | Jackson National Life - customer facing business unit (USA) |
| WTW | Willis Towers Watson (NASDAQ: WLTW) is a global advisory, broking and solutions company. Willis Towers Watson has 40,000 employees serving more than 140 countries.  They are the vendor for the Risk Agility FM. |
| RAFM | Risk Agility FM is a financial modelling software product from Willis Towers Watson. |
| WTW vGrid | WTW managed service that provides a flexible high compute capability that implements the RAFM product |
| RAFM Workstation | Desktop implementation of the RAFM product |
| RCT | Report and Consolidation Tool is a system that produces final reports that are released and published. |
| SecondFloor | SecondFloor are a risk and regulatory solutions provider, who were founded in 2005 and are based in the Netherlands. SecondFloor were acquired by Cleversoft in May 2019.  They are the vendor for the ICM interface. |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |