



IT Service Offerings Description Document

Authors: Kabir Hussein / David Boakes

Version: 4.0

Document Control Sheet

Name of document:	IT Service Offerings Description Document
Version:	Draft 4.0
Purpose of Document	Provide information on Service Offerings for ITS customers
Status:	Draft improvements to approved document
Owner:	IT Services Technical Design Authority
File location / Filename:	
Date of this version:	27 th Nov 2015
Produced by:	Kabir Hussein / David Boakes
Synopsis and outcomes of Equality and Diversity Impact Assessment:	
Enquiries on this document to:	IT Services PMO

Revision History

Revision Date	Summary of changes	Author(s)	Version Number
05/2014	Initial draft version reviewed.	Kabir Hussein	V0.01
11/06/2015	Initial updated draft version sent to internal SAM Project team	Kabir Hussein	V0.1
11/06/2015	Updated changes regarding support model	Kabir Hussein	V0.2
16/06/2015	Section 4.3 Statement on Research hosted support model added Section 3.2 Security classification statement added	Kabir Hussein	V0.3
22/06/2015	Application support section updated for Fully managed and hosted applications	Kabir Hussein	V0.4
24/06/2015	Research offering section amended. (DTL ref. no. 614 approved)	Kabir Hussein	V0.5
26/06/15	Approved by DTL ref 618	Kabir Hussein	V1.0
04/08/15	Updated version with new revised Service Offering. ITS Research team have been taken out of this document, will be presented in a separate document.	Kabir Hussein	V1.1
05/08/15	Updates added following review with the TDA team.	Kabir Hussein	V1.2
05/08/15	Minor updates from Tony Higgins.	Kabir Hussein	V1.3
07/08/15	Updates added based on suggestions from the ITS Lead via email.	Kabir Hussein	V1.4
07/08/15	Updates following review with TDA team.	Kabir Hussein	V1.5
19/08/15	Updates following review with Jonathan O'Regan	Kabir Hussein	V1.6
08/09/15	This was approved by the Lead Team at a meeting on 07/09/15 - Following reviews and updates through the TDA, the QMUL ITS Service Offerings Document was reviewed with the ITS AD's this morning and was approved.	Kabir Hussein	V2.0

	There was some discussion on how the offerings are presented to the schools and ensuring the appropriate criteria and expectations are clear for when each offering could be implemented. In particular, it was stressed again that IaaS was not to be the default option.		
17 Sep 15	Significant additions regarding service elements	Sandra Heydorn	Draft 2.1
	Review from Alan Ansell	Sandra Heydorn	Draft 2.2
25 Sep 15	Review from David Nye	Sandra Heydorn	Draft 2.3
7 Oct 15	Updates and Changes made	David Boakes	Draft 2.4
21 Oct 2015	Major changes to document	David Boakes	Draft 2.5
22 Oct 2015	Updates and Changes made	Alan Hardy	Draft 2.6
23 Oct 2015	Updates and Changes made	David Boakes	Draft 2.7
28 Oct 2015	Updates and Changes made based on feedback	David Boakes	Draft 2.8
2 Nov 2015	Updates and changes, including revision history	Johnathan O'Regan	Draft 2.9
3 Nov 2015	Minor changes, consistency check and typos corrected.	David Boakes	Draft 3.0
16 Nov 2015	Added Agents with relation to supporting offerings	David Boakes	Draft 3.1
26 th Nov 2015	Clarification of who can authorise an agent has been made against the System Admin Access fields in tables within sections 5.2, 5.3, 5.4 and 5.5.	Ian Douglas	Draft 3.2
27 th Nov 2015	Up-versioned to 4.0, DTL ref 954.		Approved V.4.0.

Table of Contents

1	Introduction to Document	6
2	Executive Summary	6
3	Service Management	7
3.1	Service Classification	7
3.2	Service Level	7
3.3	Support Contact Details	8
4	Primary Contacts and Escalation	8
5	Overview of IT Services Offerings	9
5.2	Fully-Managed Service	13
5.3	Platform as a Service (PaaS)	15
5.4	Infrastructure as a Service (IaaS).....	17
5.5	Software as a Service (SaaS)	19
6	Service Environment, Technologies & Configuration.....	21
6.1	Description of the Service	21
6.2	Datacentres	21
6.2.1	Built in Resilience	21
6.3	Virtualised infrastructure	22
6.3.1	Virtual Machine	22
6.4	Network	23
6.4.1	Global Traffic Manager	23
6.4.2	Local Traffic Manager	23
6.5	System & Data Backups	23
6.5.1	Definition of Data Recovery Times RTO/RPO.....	24
6.5.2	Backup and Data Retention Time.	24
6.5.3	Backup Restoration and Recovery Testing	24
6.6	System Recovery Targets.....	24
6.6.1	Server Hardware Recovery	24
6.6.2	Server Image Recovery	25
6.6.3	Application Data Recovery.....	25

6.6.4	Service Restoration and Recovery Testing	25
6.6.5	Recovery in the Event of the Loss of Datacentre (DC)	25
6.7	Monitoring and System Access	25
6.8	System Performance	26
7	Service Level Targets	27
8	Service Maintenance and Change Freezes	27
8.1	Change Freezes	27
9	Service Performance Reports and Reviews	28
10	Glossary	29

1 Introduction to Document

This document describes the main Service Offerings of the QMUL IT Services Department (ITS) and provides background information to customers as part of an introduction to the Service Level Agreement (SLA) documentation.

All changes to this document will be managed through the Service Level Management (SLM) review process and as appropriate the IT change management process.

2 Executive Summary

This document describes the various ITS Service Offerings provided by ITS and a high level overview of the environment and services available as part of the overall service “wrapper”.

The four key service offerings are:

- Fully Managed See Sect 5.2
- QMUL Platform as a Service (PaaS) See Sect 5.3
- QMUL Infrastructure as a Service (IaaS) See Sect 5.4
- Software as a Service (SaaS) See Sect 5.5

ITS will always strive to deliver a Fully Managed service as the first and foremost offering, the other models are offered on an exception basis and where appropriate for all parties to do so. For all production services/applications ITS aims to provide reliable, responsive and secure services to its customers.

Reliability and availability is delivered, where appropriate and possible, by removing single points of failure and/or building in resilience all the way through from the application, system and server configuration and back to the datacentres. There are a number of factors that may be considered when building resilience into the configuration some of which are outlined below:

- Criticality of the application (Service classification)
 - Non-Critical,
 - Critical or
 - Highly-Critical
- Security
- Type of data
 - Regulated vs unregulated
 - Confidential
 - Restricted
 - Protect
 - Open (not protectively marked)
- Licensing costs
- Technology used/available
- Risk

Even though an application may be able to be offered in a fully resilient configuration the cost of doing so maybe prohibitive and when risk assessed may not represent value for money. Additionally, for applications that may require a test/development/pre-production environment etc. they will not be afforded the same levels of resilience as the production application.

ITS always aims to provide the right service offering, environment and support for the application in consultation with the customer.

3 Service Management

3.1 Service Classification

As part of the Service Level Agreement (SLA) process ITS will work with the customer and define the service classification. This service classification underpins some of the resiliency, recovery options and additional services that may be required/offered.

The service classification is defined in the Service Design Document (SDD) of the respective service/application. The classifications are:

- Non-Critical,
- Critical or
- Highly-Critical

Determining the service classification is achieved by discussing the service with the stakeholders/customers to understand the impact unavailability of the service would have on QMUL and its business. It is a business decision that will depend on the particular service being deployed. This activity will be led by the Faculty Relationship Manager working with the stakeholders, and will engage:

- The Business Service Owner and the ITS Service Owner
- Other key stakeholders which may include for example HR, IT Security, Finance, Admissions etc.

To apply a criticality, the business needs to consider the impact that service unavailability would have on QMUL. The impact will vary in the scale of effect on QMUL for each Service. Examples for consideration are shown below, and is not a definitive list.

- The potential for prosecution resulting from breaching legislative requirements.
- The possibility of reputational damage that could lead to various outcomes such as exposure through the media, loss of customers (student intake), damage to organisational peer relationships.
- Impact on our ability to function if the financial systems capability was impacted.
- Impact of loss of student systems during enrolment and clearing.

Understanding the threats and the scale of impact will help determine the service classification.

3.2 Service Level

ITS offers a “Business Standard” service level for all production services/applications. Arrangements can be made either temporarily or permanently for an enhanced service which may incur additional cost.

The Service will nominally be available 24 x 7 x 365 and fully supported between 8am and 6pm Monday to Friday on normal business days i.e. excluding bank holidays and college closure days. ‘Available’ means that the service will be accessible and operational to all users.

'Fully Supported' means that IT Services will work to resolve any issues with the service during these hours.

There are different levels of target response and resolution times depending on the impact during the fully supported hours; these can be found under Section 7: Service Level Targets. Where there is an issue with the service impacting the user ability to carry out their work ITS recommends they contact the ITS Help Desk immediately via phone as email is dealt with as a low priority.

3.3 Support Contact Details

All requests for support, or reporting of issues should be made via the QMUL ITS Help Desk in the first instance.

The Help Desk provides a full service during ITS business hours 8am to 6pm on business days and a reduced service out of hours **via phone only** 24 x 7 x 365.

The QMUL ITS Help Desk can be contacted via:

- Telephone on 8888 (020 7882 8888);
- Self Service at <https://helpdesk.qmul.ac.uk>.

Support via the QMUL Help Desk self-service portal will only be picked up during the business day unless exceptional support arrangements are in place and documented within the individual service/application SLA document.

4 Primary Contacts and Escalation

All initial contact and subsequent escalations should be via the IT Help Desk to ensure it is logged in the IT Service Management tool (LANDesk) which will provide a unique reference number. If customers are aware of their Faculty Relationship Manager (FRM) they can escalate via them, but must provide the unique reference number provided by the IT Help Desk. Contact and escalation details can be found on the ITS website on link below.

<http://www.its.qmul.ac.uk/support/helpdesk/escalation/150304.html>

Note: Unless otherwise stated, or where Major Incident requirements dictate, these contacts are only available for escalations during the business day.

5 Overview of IT Services Offerings

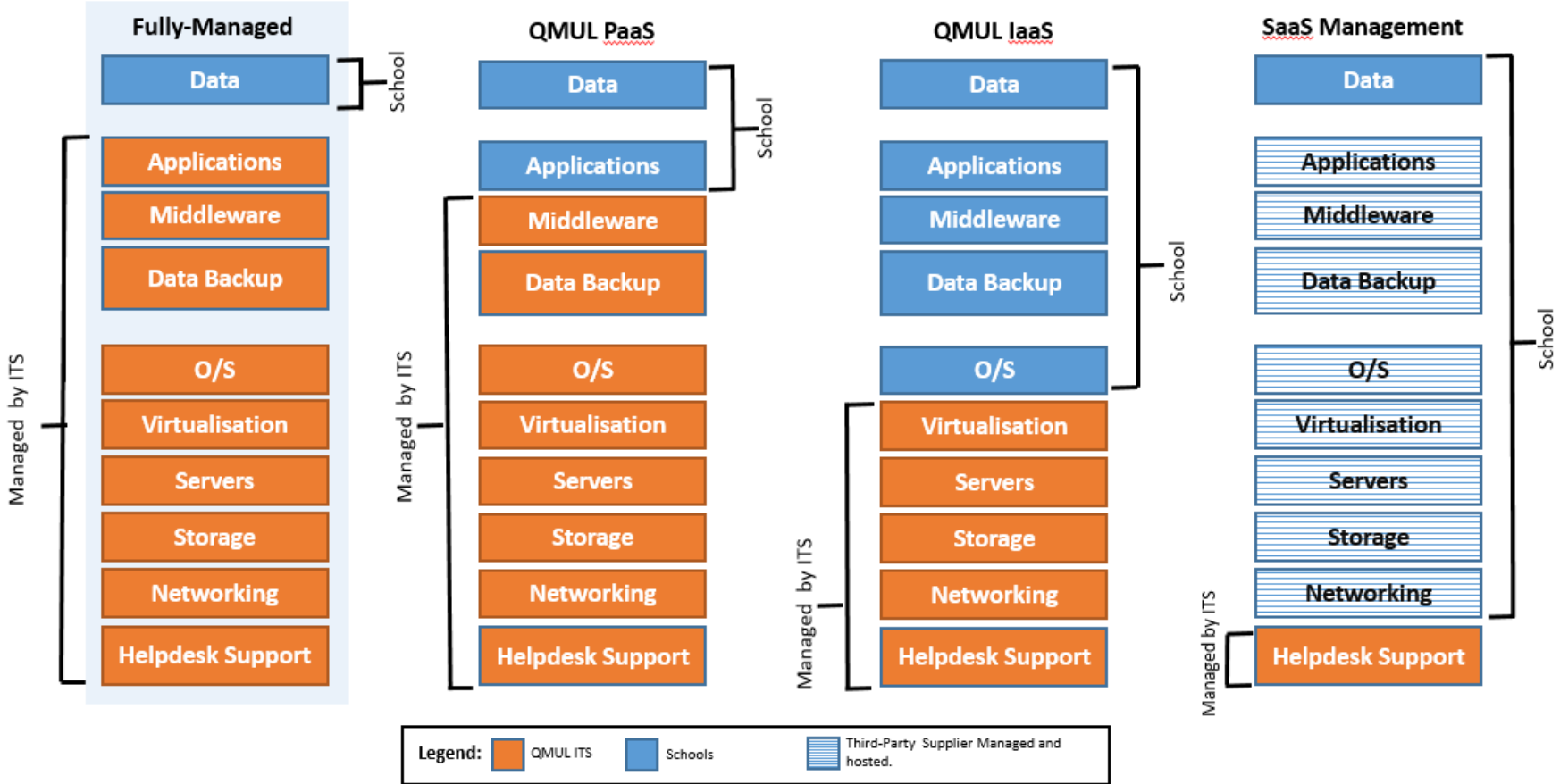
A high level view of the service offerings is shown below with a more detailed breakdown of the offerings shown later in Section 5.

The ITS service offerings are:

- Fully Managed See Sect 5.2
- QMUL Platform as a Service (PaaS) See Sect 5.3
- QMUL Infrastructure as a Service (IaaS) See Sect 5.4
- Software as a Service (SaaS) See Sect 5.5

ITS will always strive to offer the customer a Fully Managed service as the first and foremost offering, the other models are offered on an exception basis and where appropriate for all parties to do so. ITS will always work with the stakeholders to define the right service offering for each application/service or part thereof.

QMUL ITS Offerings

















5.1 Information Classification Matrix

The table below lists the standards for classifications of information assets. The information classification is made up of four categories:

- Confidential
- Restricted
- Protect
- Open (not protectively marked)

The four classes have been listed in the below table alongside how they fit into the different service offerings. The green ticks simply indicate data that is classed in that category can be hosted in the service offering.

	Service Offering			
	Fully managed	PaaS	IaaS	SaaS
Confidential				
Restricted				
Protect				
Open				

Criteria for each of the Information Categories can be found in the DG09 Information Classification pdf below.

<http://www.its.qmul.ac.uk/governance/policies/index.html>

Highly confidential data that is not standard needs to go through the Information Governance Group (IGG). The IGG will consider and advise on data classifications and data usage which are not clear or obvious, or falls within a highly confidential data classification.

	Service Offering			
	Fully managed	PaaS	IaaS	SaaS
ITS Managed OS	Yes	Yes	No	No
Antivirus	Yes	Yes	No	N/A
OS Patching	Yes	Yes	No	N/A
Unsupported OS	No	No	Yes	N/A
Backups	Yes	Yes	No	N/A
License Supplied	Yes	Yes	No	N/A
Confidential - internet access	No	N/A	N/A	Yes *
Restricted - internet access	No	N/A	N/A	Yes *
Protect - internet access	No	No	N/A	Yes
Open - internet access	Yes	Yes	Yes	Yes
Admin Access	No	No	Yes	N/A

*Subject to IGG approval

The table above lists the various high level options available for the service depending on the Service Offering it applies to. It is possible that some of these options can be negotiated to be supported locally by the customer, or centrally by ITS, but would need to be discussed with the FRM in the first instance.

5.2 Fully-Managed Service

With the ITS Fully-Managed service offering the infrastructure and application support is managed by ITS.

The data residing on the platform is managed by the School, and where appropriate and if the technology/skills allow, the data repository is managed by the ITS Database team.

Scope	Support / Owner
Data	Schools will manage the content their own data
Application	Application on Servers will be managed by ITS Application team, application support for End Users will be managed by ITS.
Middleware	Will be managed by ITS
Data Backup	Will be managed by ITS
Operating System	Will be managed by ITS
Virtualisation	Will be managed by ITS
Servers	Will be managed by ITS
Storage	Will be managed by ITS
Networking	Will be managed by ITS
Help Desk Support	Will be managed by ITS
Data Repository	Will be managed by ITS
Data Integration	ITS or 3 rd Party Support Partner
System Admin Access Applies to OS, Database, application and other privileged access to fully support the application and environment	<p>ITS and-or ITS approved Agents only. Approved ITS Agents will be defined in the SLA and are expected to follow ITS policies, and procedures. Failure to do so may result in removal of the privileged access.</p> <p>N.B. Agents can only be approved by the accountable service owner (i.e. Servers and Storage for OS, ITS Database Team for Db Sysadmin etc.)</p>
Change Control	All changes made by ITS will follow the IT Change Management process and require appropriate change approval
Budget Responsibilities	ITS will provide the budget for annual maintenance, support and hardware refresh. PAR bids may be required for consultancy for major changes, upgrades, capacity increases and migration to another platform(s) or other applications.

If a School requires higher spec/non-standard hardware or service, this will need to be discussed on an individual basis.

5.3 Platform as a Service (PaaS)

The PaaS offering provides the customer with a core hosted Operating System (OS) that allows the customer to run their own application(s) or third party application(s). All lower level elements of the infrastructure, network topology, security and back-up will be provided and managed by ITS.

Scope	Support / Owner
Data	Schools will manage their own data
Application	The Schools will manage the application residing on top of the OS. Application deployment/support to managed desktops will be supported by ITS.
Middleware	Will be managed by ITS
Data Backup	Will be managed by ITS
Operating System	Will be managed by ITS
Virtualisation	Will be managed by ITS
Servers	Will be managed by ITS
Storage	Will be managed by ITS
Networking	Will be managed by ITS
Help Desk Support	Will be managed by ITS
Data Repository	Will be managed by ITS
Data Integration	ITS or 3 rd Party Support Partner
System Admin Access Applies to OS, Database, application and other privileged access to fully support the application and environment	<p>ITS and-or ITS approved Agents only. Approved ITS Agents will be defined in the SLA and are expected to follow ITS policies, and procedures. Failure to do so may result in removal of the privileged access.</p> <p>N.B. Agents can only be approved by the accountable service owner (i.e. Servers and Storage for OS, ITS Database Team for Db Sysadmin etc.)</p>
Change Control	All changes made by ITS will follow the IT Change Management process and require appropriate change approval
Budget Responsibilities	ITS will provide the budget for annual maintenance, support and hardware refresh. PAR bids may be required for consultancy for major changes, upgrades, capacity increases and migration to another platform(s) or other applications.

If a School requires higher spec/non-standard hardware or service, this will need to be discussed on an individual basis.

5.4 Infrastructure as a Service (IaaS)

The IaaS offering provides the customer with core elements of infrastructure such as server (normally virtualised), storage and networking. The customer will be responsible for managing the Operating System (OS) image and related application software. It is the responsibility of the customer to patch/update and maintain the OS and any application software updates and security patches.

Scope	Support / Owner
Data	Schools will manage their own data
Application	The Schools will manage their own Application, the deployment of the application to managed desktops will be managed by ITS.
Middleware	The Schools will manage their middleware, where used
Data Backup	<p>The School will be required to take backups of the Servers / Application. ITS Services will take nightly backups of the full Virtual Machine so that it can be restored in the event of a hardware failure, this does not cover file level backups.</p> <p>All other levels of server and data backups are the responsibility of the School. Any other backup services performed by ITS will need to be explicitly added and agreed within the SLA.</p>
Operating System	The Schools will manage their own Operating System.
Virtualisation	Will be managed by ITS
Servers	Will be managed by ITS
Storage	Will be managed by ITS
Networking	Will be managed by ITS
Help Desk Support	Will be managed by ITS
Data Repository	Will be managed by ITS
Data Integration	School or 3 rd Party Support Partner
System Admin Access Applies to OS, Database, application and other privileged access to fully support the application and environment	<p>The School will have full administrative access to the Servers.</p> <p>N.B. it will NOT include access to underlying Network or VM infrastructure</p>
Change Control	All changes made by ITS will follow the IT Change Management process and require appropriate change approval.

	ITS recommend the customer follows a change process.
Budget Responsibilities	ITS will provide the budget for hardware refresh. Schools will provide budget for software, consultancy and 3 rd party support outside of the PAR process. PAR bids may be required for consultancy for major changes, upgrades, capacity increases and migration to another platform(s) or other applications.

If a School requires higher specification/non-standard hardware or service, this will need to be discussed on an individual basis.

5.5 Software as a Service (SaaS)

The SaaS offering has the application hosted by a third party running on their infrastructure with the majority of support being provided by the third party. ITS will mainly provide connectivity to the application and will normally be the primary interface to the supplier.

Scope	Support / Owner
Data	The Schools will manage their own data
Application	Application will be supported by the 3 rd Party vendor, the deployment of the app to managed desktops (if required and by prior agreement) can be managed by ITS.
Middleware	Middleware will be supported by the 3 rd Party vendor
Data Backup	Data Backup will be provided and supported by the 3 rd Party vendor
Operating System	Operating System will be managed by the 3 rd Party vendor
Virtualisation	VM platform will be supported by the 3 rd Party vendor
Servers	Server platform will be supported by the 3 rd Party vendor
Storage	Storage will be supported by the 3 rd Party vendor
Networking	All network related issues will be supported by the 3 rd Party vendor unless it is clearly an internal QMUL network issue.
Help Desk Support	Support will be provided by the ITS Help Desk team and then triaged over to the ITS Applications team who will deal with the 3 rd party vendor.
Data Repository	Data will be hosted on 3 rd party hardware.
Data Integration	School or 3 rd Party Support Partner
System Admin Access Applies to application privileges only as provided by the SAAS vendor	ITS and-or ITS approved Agents only. Approved ITS Agents will be defined in the SLA and are expected to follow ITS policies, and procedures. Failure to do so may result in removal of the privileged access.
Change Control	All changes made by ITS will follow the IT Change Management process and require appropriate change approval. ITS recommend the customer follows a change process.
Budget Responsibilities	Schools will provide funding for software, consultancy and 3 rd party support outside of the PAR process.

If a School requires higher spec/non-standard hardware or service, this will need to be discussed on an individual basis.

6 Service Environment, Technologies & Configuration

6.1 Description of the Service

Depending on the service offering, as described in Section 5, the support or “wrapper” provided by ITS will differ. This section provides a high level overview of some of the services available and the environment in which the application/services may run. This is background information only as all of these technologies are subject to change and ITS reserves the right to change them. Any change to the technologies will be subject to the appropriate change control process.

6.2 Datacentres

ITS is in the process of consolidating IT services from the various disparate locations across QMUL into 3 main datacentres, currently:

- Mile End (Primary)
- Enfield (Secondary)
- Slough (Research only)

All physical components of the systems (i.e. servers and/or storage) for service offering types of Fully-Managed, PaaS, IaaS are located in ITS approved/managed datacentres. These datacentres are purpose built, secure “lights out” rooms with restricted access, have full air conditioning with resiliency, protected by Uninterruptable Power Supply (UPS) and the environment and systems are controlled and monitored.

Where applications are hosted outside of ITS datacentres this will be explicit in the SLA.

ITS will be responsible for applying for University funding to ensure the infrastructure is fully supported, maintained and kept current. The technology used is industry standard enterprise class, best in breed and highly scalable. Currently the infrastructure utilises Lenovo servers, NetApp storage and Cisco networking.

6.2.1 Built in Resilience

Resiliency has been built into the datacentre, network, server and storage configuration design by default and configured appropriate for the service. In general, this means for production applications there should be no loss of service due to disk, network, or power supply failure.

Application level resilience needs to be designed, built and tested on a service by service basis. Application resilience can be increased but will depend on the ability of an application to leverage resilience technologies and there are other considerations as outlined below.

- Criticality of the application (Service classification)
 - Non-Critical,
 - Critical or
 - Highly-Critical
- Security
- Type of data
 - Regulated vs unregulated
 - Confidential

- Restricted
- Protect
- Open (not protectively marked)
- Licensing costs
- Technology used/available
- Risk

Additionally, for critical applications, data can be mirrored across datacentres allowing recovery time for applications to be kept to a minimum in the event of a failure.

The target SLA for the central infrastructure is 99.9% measured monthly on a 24 x 7 x 365 basis, excluding agreed in advance maintenance windows.

6.2.2 Security Management

ITS datacentres have security management standards in place, this is to ensure proper selection of adequate and proportionate security controls are in place to protect all information assets in the datacentres.

For network security ITS use class leading Cisco ASA firewalls providing security and firewalling in the core network and appropriate segmentation within the datacentre. These are complemented with other layers of security including Intrusion detection / prevention systems at the boundary of QMUL's network.

6.3 Virtualised infrastructure

ITS runs a virtualised server environment in its datacentres using the industry standard product VMWare. Virtualization uses software to simulate the existence of hardware and create a virtual computer system. This allows ITS to run more than one virtual system and multiple operating systems and applications on a single server, providing economies of scale and greater efficiency. The physical and virtual servers are managed via system administration tools and depending on the criticality of the service resiliency can be built into the physical and-or virtual environment.

ITS has adopted virtualisation across all platforms and service where possible. Although ITS anticipate that system performance will increase when run from a modern data centre this is not always the case as some software is not optimised to leverage advanced virtualisation technologies and may not perform as expected; although this will be the exception rather than the rule. In these cases ITS will consider the use of dedicated physical hardware within the datacentres and will agree the necessary changes to the service levels as appropriate.

6.3.1 Virtual Machine

ITS will work with the customer to ensure the virtual server provisioned is able to cope with the demand and load with no degradation of performance, unless it is a conscious decision to do so (e.g. for test or development servers). Changes may be required to the configuration to optimise it for its intended use and this will be subject to change control.

ITS will provision a standard service for each of the service offerings which will include various files, software packages and services that are managed by ITS for the customer. These will all be on the initial image provided. The customer is prohibited from removing or disabling any of the packages or services that were supplied in the initial image as it may impair the functioning of the server and the ability for ITS to manage it.

6.4 Network

ITS has deployed Cisco network solutions who are one of the leading network solution providers. The solution deployed at QMUL is best of breed, enterprise grade that is fully redundant; high availability; high performance; secure and scalable with appropriate service backup to underpin the required SLA.

The Wide Area Network (WAN) between the three main QMUL campuses are connected via technology providing a resilient, flexible and scalable solution for the future. ITS have also deployed data network traffic management solutions for both, inter and intra datacentre connectivity.

6.4.1 Global Traffic Manager

ITS have deployed Global Traffic Manager (GTM) to monitor and direct Domain Name System (DNS) traffic to the best available resource in either of the two datacentres including any system failures and service recovery scenarios. The GTM's service deployed is fully redundant.

6.4.2 Local Traffic Manager

ITS have deployed two Local Traffic Managers (LTM) in each datacentre in a fully redundant configuration. These LTM's monitor and poll the health check and integrity of the application while offering an Application Load Balancing service that helps deliver to the users a reliable, secure, and optimized access to the application(s). Additionally LTM's also offer Secure Sockets Layer (SSL) security certificate management and encryption service.

6.5 System & Data Backups

Where ITS is responsible for backups they are taken as a matter of course. There are different backup, archiving and replications options deployed and available. ITS will work with the customer to provide the right solution to meet their need.

Full backups are started on Saturday morning and additional incremental updates occur nightly during the week.

For these servers, ITS will also take file level backups of the entire VM filesystem via a backup agent installed and configured on the machine. The customer must not to interfere with its operation.

Recoveries can be requested via the Help Desk. Or alternatively, ITS will provide advice on how recovery can be performed by the customer. Again, the normal request channel for that advice is via the Help Desk.

6.5.1 Definition of Data Recovery Times RTO/RPO.

Recovery expectation times are normally quoted in terms of the “Recovery Time Objective” (RTO) and “Recovery Point Objective” (RPO).

The RTO refers to the maximum targeted time taken within normal operational support hours for data to be recovered or restored measured from the point at which an Incident or Service Request is logged in the IT Service Management tool during business hours.

The RPO refers to the maximum targeted period for which data may be lost due, for example, from having to revert back to the previous night’s backup.

Where ITS are responsible for backups and restore, estimated times regarding RTO and RPO can be provided to the customer and will be part of the SLA.

6.5.2 Backup and Data Retention Time.

Detailed information on the backup and data retention times are contained with the TSM Backup and Recovery document. Currently backup of information is taken on a 24 hour rolling basis. Each backup is retained for a maximum of 90 calendar days and then deleted. Restoration of data can be requested from any of the retained backups within the 90 day period, should restoration to a specific point in time be required.

It is the responsibility of the data owner to ensure that data retention is aligned with the QMUL data retention policies to maintain legal and ethical compliance and are in line with policy QMUL Records Retention Schedule. Normally this involves the data owner ensuring the data remains on-line for the required retention period. ITS are available to discuss possible solutions for specific data archiving requirements if required

http://www.arcs.qmul.ac.uk/information_governance/records_management/records_retention_schedule.html

<http://www.arcs.qmul.ac.uk/policy/index.html>

6.5.3 Backup Restoration and Recovery Testing

Full backup restoration testing will be carried out during the process of service design and implementation to ensure that services, data and files can be restored within the Service Level Agreement (SLA) target times during business as usual operation.

6.6 System Recovery Targets

6.6.1 Server Hardware Recovery

Recovery following a Physical Blade Server or Virtual Machine Host failure.

The RTO is 10 minutes maximum with a maximum RPO of 60 seconds.

ITS uses “High Availability” technology to provide the support which is carried out automatically with no manual intervention. Due to the automatic enablement of service recovery the actual service availability is 24 x 7 x 365.

From time to time, to optimize performance, ITS may use the above mechanism during normal operation to move the service to another blade.

6.6.2 Server Image Recovery

Virtual Machine Restoration following corruption of server operating system image

The RTO is 8 hours maximum with a maximum RPO of 24 hours.

Following an event where there may be a corruption of the operating system data, the corrupted information will be restored to the last known good backup point. Restoration requires manual intervention from the support team and as such the service availability is aligned with the standard business day support hours of the appropriate team(s).

6.6.3 Application Data Recovery

File store restoration following corruption of data

The RTO is 8 hours maximum with a maximum RPO of 24 hours.

Following an event where there has been a corruption of data, the corrupted files will be restored to the last known good backup point. Snapshot mirrors of the data are taken from the ITS N series network attached storage arrays on a rotating 8 hourly basis. Restores require manual intervention from the support team and as such the data availability is aligned with the standard business day support hours of the appropriate team(s).

6.6.4 Service Restoration and Recovery Testing

Full restoration testing will be carried out during the process of service design and implementation to ensure that services, data and files can be restored within the Service Level Agreement (SLA) target times during business as usual operation.

6.6.5 Recovery in the Event of the Loss of Datacentre (DC)

For Applications defined as “Highly critical” and “Critical” and where the application can support it, the application and data is available in both datacentres, expediting or eliminating the need for recovery of the application. Depending on the nature and the scale of the DC failure ITS may need to prioritize the recovery of services by impact on the college as a whole, and so no recovery times will be given.

6.7 Monitoring and System Access.

Authorised ITS staff require privileged (admin/root or supervisor) access to systems they are required to support to ensure they are functioning correctly. The customer must not take any action to exclude ITS staff from access, and must be members of the “install” local system group.

Irrespective of the service offering, ITS reserves the right to withdraw support if it feels its ability to support the environment is being compromised.

The customer is not permitted to give privileged (admin/root or supervisor) access to any other person (be they members of the college or not) without prior consent from ITS requested via the Help Desk. Any occurrence of this will lead to a suspension of the customer's access to the machine and a possible suspension of the service at ITS discretion. Any request for additional access should be requested via the ITS Help Desk.

ITS reserve the right to monitor the system for performance, system malfunctioning, security auditing and auditing of data and processes on the system. ITS also reserves the right to perform security scans against the system at any time and without prior notice. When notified of the source of those security scans the customer must not take any explicit and deliberate actions to bypass these checks.

6.8 System Performance

Any concerns or issues with performance of the system/application are to be initially raised via the Help Desk. Where an issue is identified ITS will work with the customer to provide a satisfactory resolution. Please note: ITS also reserve the right NOT to increase system resources if it will have, or is suspected to have, a detrimental effect on other systems and or services.

ITS will work with the customer to find an appropriate solution.

7 Service Level Targets

ITS establishes priorities for the restoration of a service or application broadly based on the impact of the service outage. ITS recognises that at different times of the year normal non-critical applications or services may become business critical and the Service Level classification is flexible to deal with these circumstances. The Service Level Targets for both incidents and requests can be found on the ITS website via the link below.

<http://www.its.qmul.ac.uk/support/helpdesk/serviceleveltargets/index.html>

8 Service Maintenance and Change Freezes

All changes made by ITS will follow the IT Change Management process and require appropriate change approval. This includes all changes to integrated systems and plug-ins.

For scheduled changes requiring a Planned Service Interruption (PSO), a minimum of 5 business days' notice will be given to customers. For emergency changes ITS will give as much notice as possible. For unscheduled outages by their nature ITS are unable to provide any prior warning.

8.1 Change Freezes

ITS have implemented application and infrastructure change freeze periods during business critical times of the year for example clearing and enrolment. Standard agreed pre-approved changes can still be undertaken during change freeze periods. However, ITS would not carry out for example a major network upgrade during a change period. More information on change freezes can be found below.

<http://www.its.qmul.ac.uk/support/freeze/145779.html>

9 Service Performance Reports and Reviews

IT Services will report service delivered, against the service required in the agreed SLA every month. The report will detail all issues experienced, the time taken to respond to each reported issue and the time taken to resolve. ITS will have successfully supported the service if 95% of the issues reported were dealt with according to the agreed service level targets. Where failures to resolve issues are due to circumstances outside the control of ITS (such as a power cut across the local area) it will be included in the report, however, the failure to meet the target will not be included in the measurement of the 95% target.

If ITS misses the 95% target for resolving issues with the service in one monthly reporting period, a comprehensive and clear explanation for this failure will be given.

Where ITS misses the 95% target for resolving issues with the service in three consecutive monthly reporting periods, IT Services will provide a service improvement plan detailing what actions are being planned to bring the level of service being provided back to within the agreed target level.

Regular Service Review meetings will be arranged by the FRM, described in the Service Management policy document which can be found here:

<http://www.its.qmul.ac.uk/governance/policies/index.html>:

10 Glossary

Acronym/Definition	Meaning
Agent(s)	Is an individual(s), team(s), group(s), organisation(s) or supplier(s) involved in the support and maintenance of a service offering who are not part of IT Services.
Application Owner	An application owner is the individual or group with the responsibility to ensure that the program or programs, which make up the application, accomplish the specified objective or set of user requirements established for that application, including appropriate security safeguards.
Business Day	Monday-Friday 8AM - 6PM excluding bank holidays and college closure days.
Change	The addition, modification or removal of anything that could have an effect on an IT service.
FRM	The Faculty Relationship Manager is responsible for maintaining the relationship between QMUL ITS and with one or more Faculties, they also carry out the Service Level Manager role.
Incident	An unplanned interruption to an IT Service or reduction in the quality of an IT service. Failure of an IT Asset that has not yet affected a service is also an incident – for example, failure of one disk from a resilient mirrored set.
ITS	IT Services Department
ITIL®/ITSM	Information Technology Infrastructure Library /IT Service Management https://www.axelos.com/best-practice-solutions/itil/what-is-itil
Problem Management	The process responsible for managing the lifecycle of all problems. Problem management proactively prevents incidents from happening and minimizes the impact of incidents that cannot be prevented.
Service Owner	A role responsible for managing one or more services throughout their entire lifecycle.
Service Provider	An organisation supplying services to one or more internal or external customers. An application service provider (often abbreviated as an ASP) is “a third-party that manages and distributes software-based services and solutions to customers across a wide area network (e.g., the Internet) from a central datacentre”.
Service Request (Request)	A formal request from a user for something to be provided – for example, a request for information or advice; to reset a password; or to install a workstation for a new user. Service requests are managed by the request fulfillment process. Service requests may be linked to a change as part of fulfilling the request.

SLA	Service Level Agreement
-----	-------------------------