# CTM UHB

Digital Business Continuity update – March 2021

# Digital Business Continuity – Definition & Scope



Definition: Plans and activities that support the ongoing delivery of digital services to the organisation in the event of a failure or compromise to a critical component or interrelated group of components.

Scope: CTM Hosted and managed digital services infrastructure- networks, servers, storage, telephony, systems and staff. This excludes:

- **Nationally hosted systems** - under NWIS SLA
- **Cloud hosted systems** - per system SLA arrangement
- **Systems provided to the Bridgend area** - under SLA with SBUHB

Where SLA's are in place, these are assured through SLA management meetings, risk reviews and Welsh internal audit reviews.

# CTM Hosting

The DGH's at both **PCH** and **RGH** provide a central setting for the hosting of digital services:

**PCH** is the primary hosting location for most systems used across the UHB. A server room provides a robust housing for high end server, storage and network infrastructure. The room requires specialised arrangements to ensure stability of electrical supply, cooling, fire suppression and physical security.

A second, less equipped room within **PCH** is utilised to allow certain systems to continue to operate in the event of a partial or complete loss of the primary room. Other rooms are used across the site, specifically for telephony and network hosting.

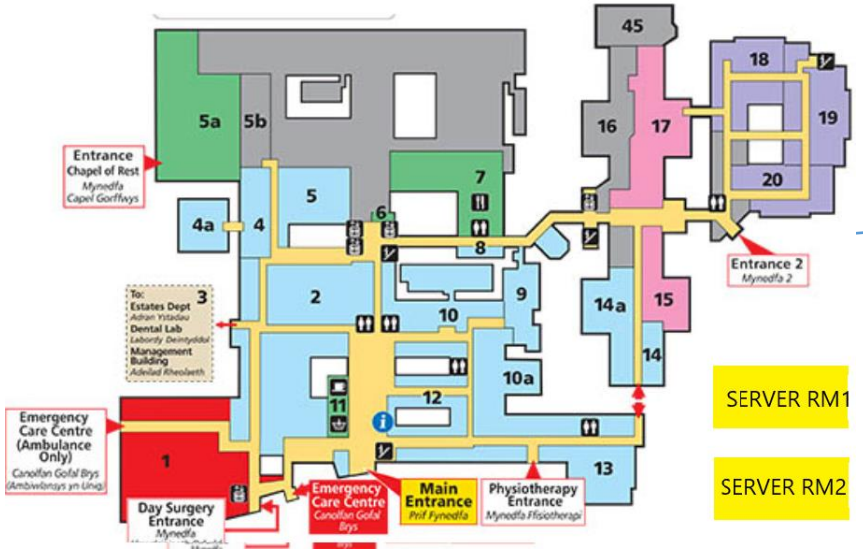
**RGH** houses a similar room, although this is typically utilised for systems that are required to be within the locality of **RGH** (e.g. due to network links). There are also other rooms used across the site, specifically for telephony and network hosting.

***The Digital services hosted as above are used for Secondary and Community care systems.***

# CTM Hosting cont.

DBC March 2021

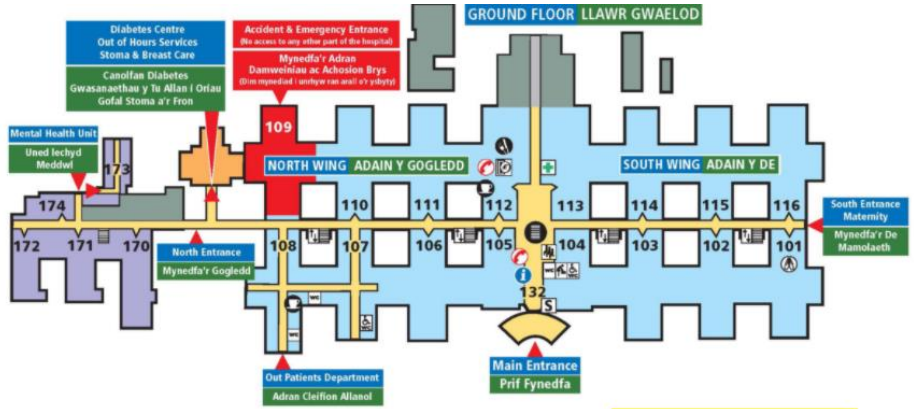
PCH




SERVER RM1

SERVER RM2

RGH



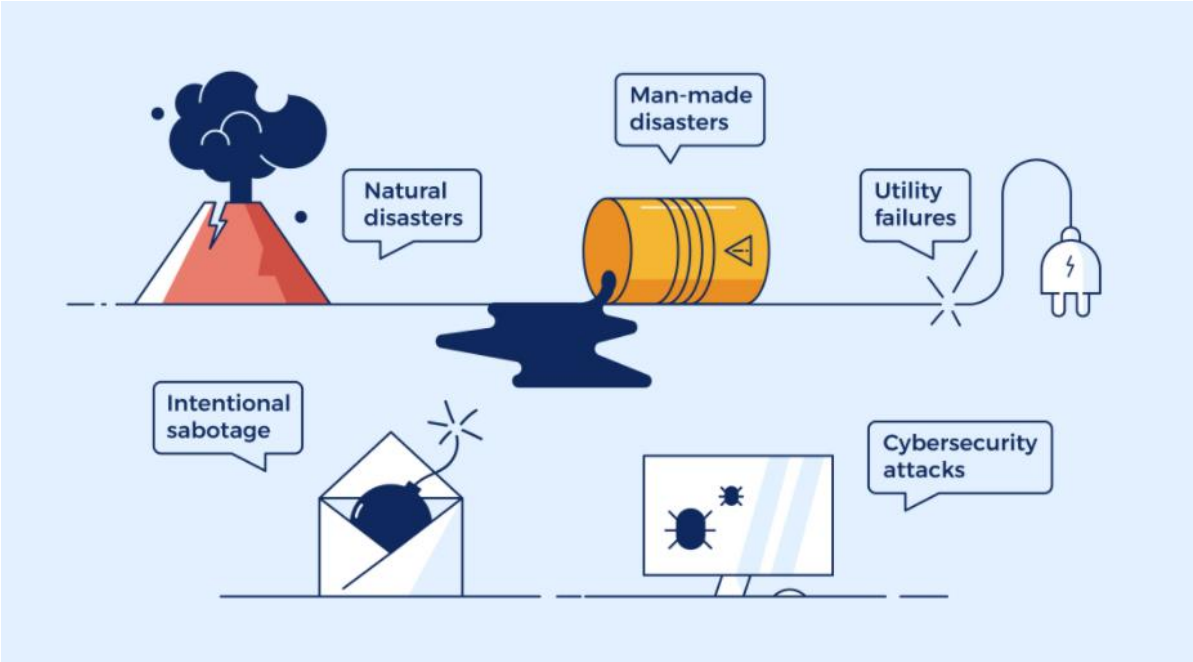

SERVER RM 3


# Risks



The risks that relate to digital business are derived from a variety of sources –

- Natural disasters
- Man-made disasters
- Utility failures
- Sabotage
- Cyber attacks




- Staff availability

# Risks (cont)

A high level assessment is provided here - the likelihood of these risks impacting the UHB needs to be considered and localised, proportionate approaches need to be applied.

| Risk | Assessment | Example(s) |
|---|---|---|
| Natural disasters | Low | Storm Damage, Localised flooding, Long term utilility disruption |
| Man made disasters | High | Site refurbishment, Buildings, Upgrades |
| Utility failures | Medium | Electrical arrangements, UPS, Cooling |
| Sabotage | Low | Vandalism, Targeted attack |
| Cyber Attacks | High | Viruses, Targeted attack |
| Staff availability | Medium | Sickness, Recruitment, other absence, Skill sharing |

# Systems and availability



To design and deliver digital services, there is a requirement to ensure that they are architected to the relevant standards which consider:

Performance | Availability | Frequency of use | Growth | Costs | Application architecture | Physical constraints| ICT skills and availability

These determine how a system is designed and implemented and typically lead to a tiered arrangement for digital services – *"consider a long term archive maintained for compliance purposes VS a critical care monitoring system".*

Where the expectation may be that a system should be designed and implemented to the highest standards at all times, this in practice is likely to introduce waste.

The development of digital business continuity should follow a similar 'proportional effort' approach – some key factors can influence this –

- Availability of effective departmental BC procedures
- Highly Available ICT Architecture (spanning across hardware, rooms and sites)
- Service needs

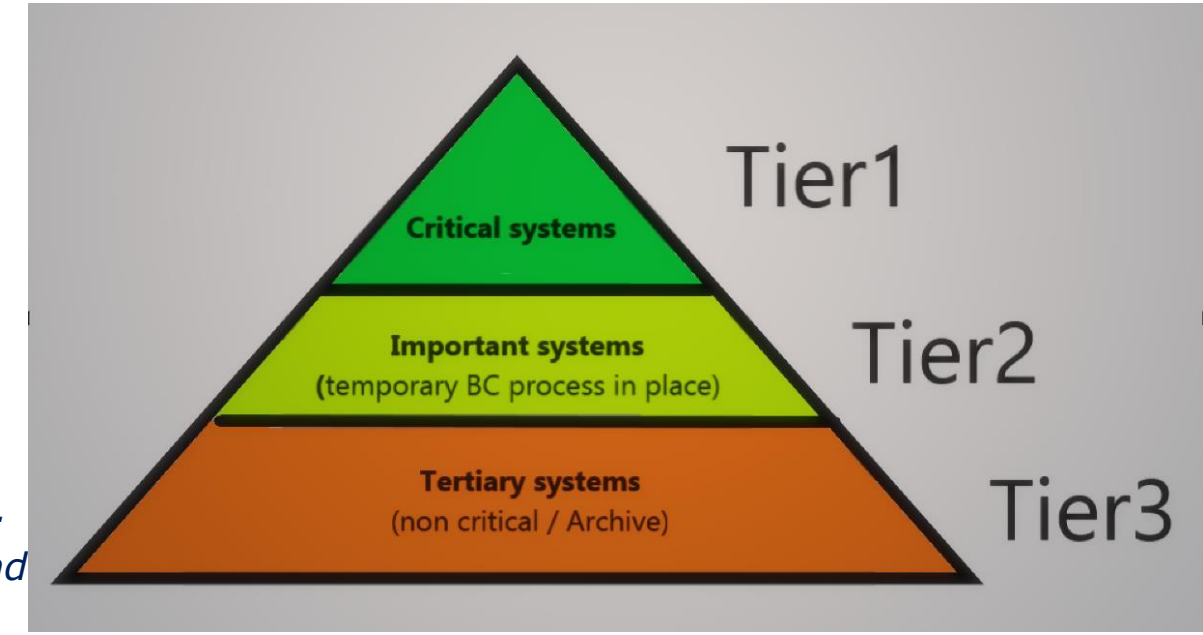
# Approach to Digital Business prioritisation

The approach is to categorise systems based on their criticality to digital business provision. This leads to proportionate effort being made to maintain services and influences continuity planning, this also directs and prioritisation should a multi system outage occur. The tiering of any system will be derived from requirements from the users of the system and the team/supplier supporting the system

The agreed tier for any system should influence the following :

- **Location** – single room, multi room, multi site, cloud
- **Hardware** – single server, multi server (cluster), multi server (cross location cluster)
- **Backup\restore capabilities** – Standard backup, Enhanced backup (with quick restore options)

*(note – configuration of a system can be constrained by its design. e.g. An older system may have been designed as single server, and not capable of being setup on multiple servers)*



# Approach to planning for B.C.



**Stage 1 – Prevent**

Deploy systems in a resilient manner, allowing tolerance to failure of as many components as possible.

Make component replacement transparent to the operation of the system.

**Stage 2 – Failover**

Deploy systems with High Availability (HA), allowing tolerance to failure at as many levels as possible – spanning servers and rooms. Where possible make the HA seamless and practice this within normal operations.

**Stage 3 – Recover**

Should a major failure occur, recovery should be made from system backups and service returned within temporary arrangements, possibly at the second site, until the primary hardware\room\site is available again. This will be disruptive to service. Some recovery tests can be done to validate this.

**Stage 4 – Restore and review**

Return systems back to original location providing full performance capacity.

Conduct a review of the incident and how the technical aspects of the recovery worked.

# Status, plans and compliance

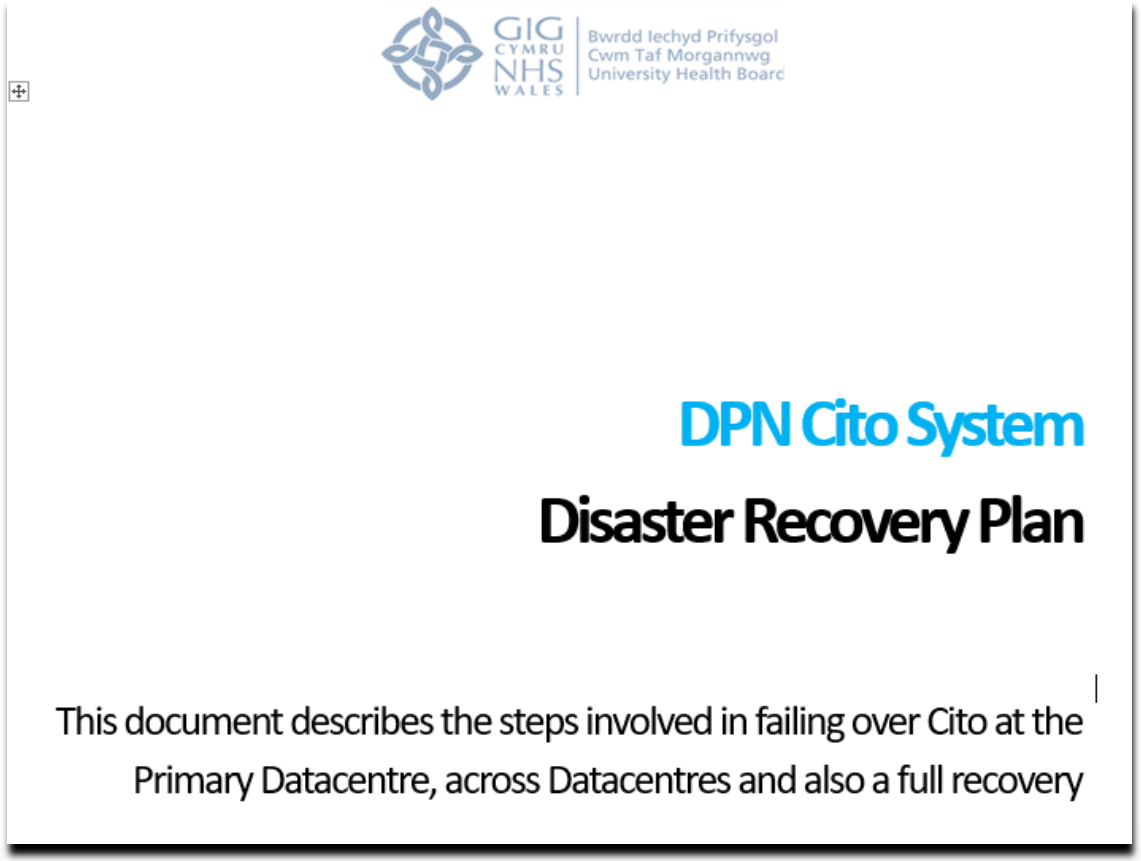


Although plans have existed for systems historically, it is considered within the department that the document set is incomplete and out of date. Since September ’20, a dedicated resource has been allocated to reviewing and driving the creation of a full document set which will be written to a newly agreed standard – and in line with industry best practice.

A tracker has been established to ensure that assessments and documentation are in place for the areas deemed **Critical** to digital business services.

# Status, plans and compliance (cont)

## Sample of new document format

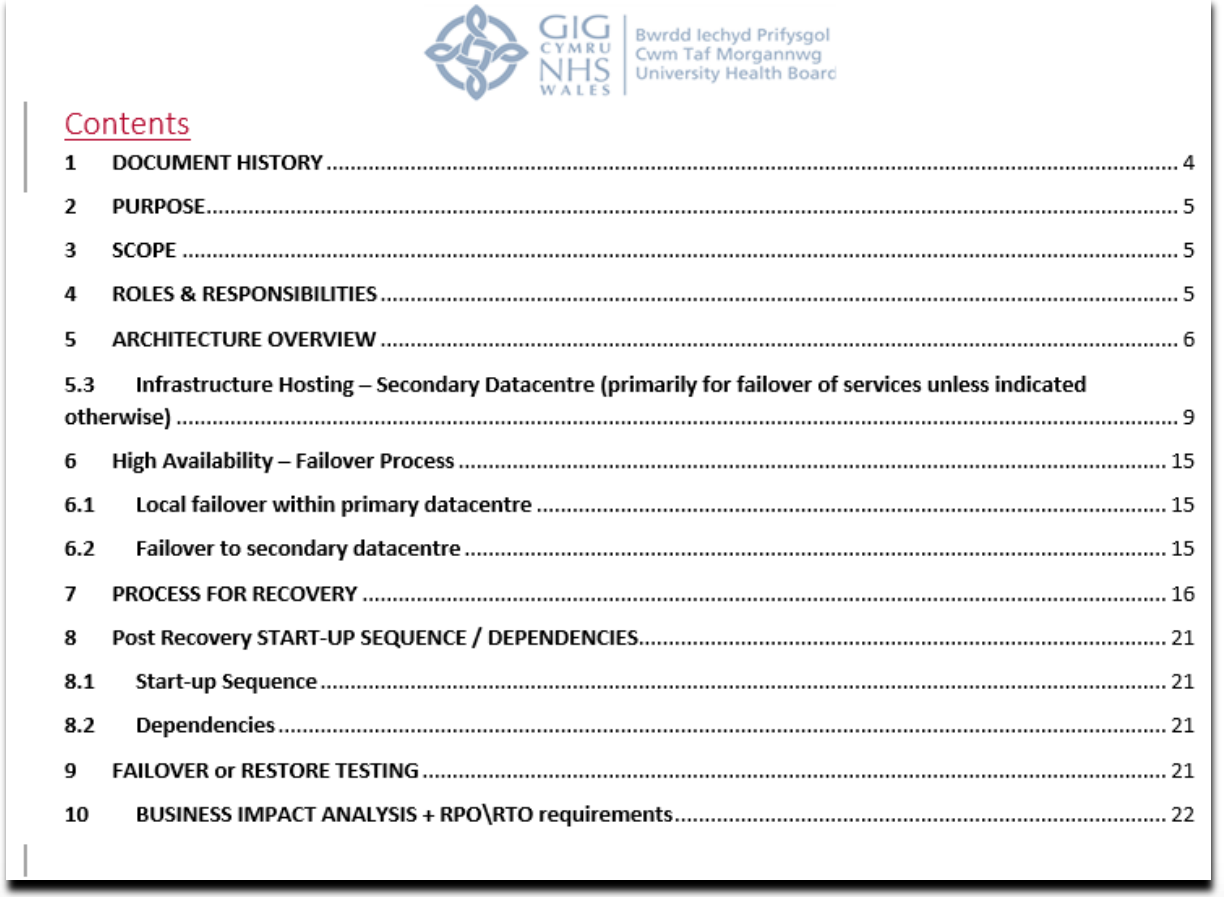


GIG CYMRU NHS WALES
Bwrdd Iechyd Prifysgol
Cwm Taf Morgannwg
University Health Board

**DPN Cito System**

**Disaster Recovery Plan**

This document describes the steps involved in failing over Cito at the Primary Datacentre, across Datacentres and also a full recovery

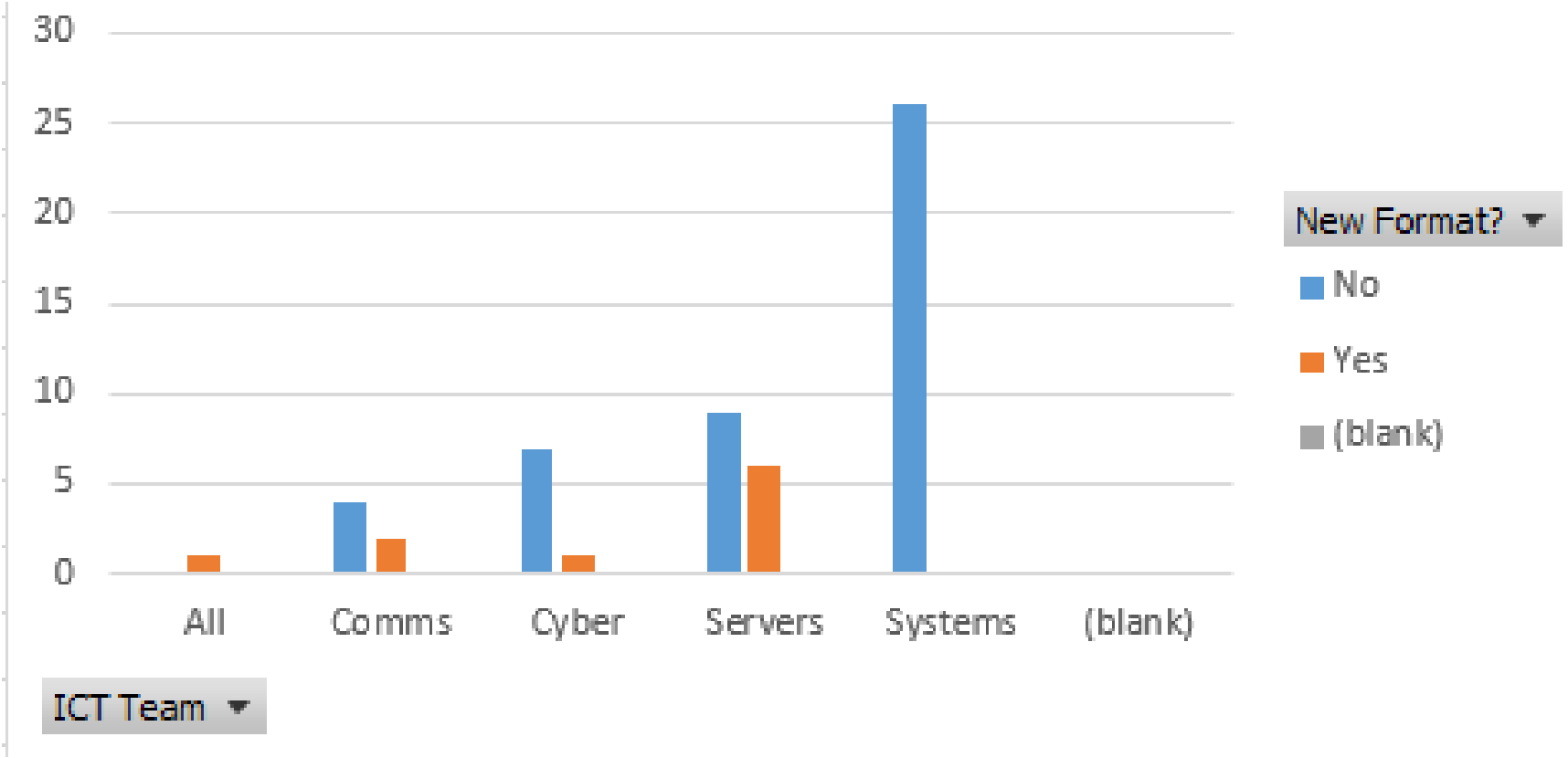


GIG CYMRU NHS WALES
Bwrdd Iechyd Prifysgol
Cwm Taf Morgannwg
University Health Board

Contents

# Status, plans and compliance (cont)

## Current tracker status



# Ongoing actions

To provide a comprehensive set of documents and to carry out the assessment required to complete each document, the concerted efforts around this will continue. It is anticipated that the completing of the core document set is prioritised and commitment is made by all staff to provide this be July ’21

- There will be a requirement to continually assess the document set, the list of critical applications and keep the documents in line with any changes made to either Infrastructure of systems configuration
- A commitment to a full review of related Risks will also need to be completed to inform some of the documentation and plans
- Internal and External compliance standards review will also need to capture the standards required – e.g. NIS, Cyber Essentials, Internal Audit, Electrical Safety

**Complete document set for Critical Systems by - July ‘21**

**Risks review – underway due to complete by - May ‘21**

**Compliance review – Formal review by - July ‘21**

# Ongoing actions and Conclusion



In order to improve the ability to failover systems from room to room, and site to site, a number of infrastructure development workstreams are underway:

- Provision of network capacity to allow site to site replication for High Availability
- Network design changes to allow sites to share server networks
- Build of a new server room within PCH to allow active / active running and increased failover capacity
- Local network redesign at PCH and RGH to introduce further resilience for Server Rooms and general connectivity
- Assessment of Cloud services to support DR arrangements (i.e. Burst capacity)
- Inform and assure future procurement standards to ensure system meet the requires standards