Appendix A

Risk Number	RM010	**Date of update**	20 June 2018
Risk Name	The risk of the loss of key ICT systems including: - internet connection; - telephony; - communications with cloud-provided services; or - the Windows and Solaris hosting platforms.		
Risk Owner	Simon George	**Date entered on risk register**	02 September 2015

Risk Description

Loss of core / key ICT systems, communications or utilities for a significant period - as a result of loss of power, physical failure, fire or flood, supplier failure or cyber attack - would result in a failure to deliver IT based services leading to disruption to critical service delivery, a loss of reputation, and additional costs.
Overall risk treatment: treat.

Original			**Current**			**Tolerance Target**				
Likelihood	Impact	Risk score	Likelihood	Impact	Risk score	Likelihood	Impact	Risk score	Target Date	Prospects of meeting Target Risk Score by Target Date
3	4	**12**	3	4	**12**	1	3	**3**	Sep-18	**Amber**

Tasks to mitigate the risk

'1) Full power down completed periodically.

2) Voice and Data reprocurement.

3) Commision Independant Data centre and power audit

4) Reprocure storage with suitable resilience and Disaster Recovery (DR)

5) Reprocure Microsoft Server Infrastructure with suitable resilience and DR

6) Replace ageing Local Area Network (LAN) equipment

7) Identify a suitable DR site to replace Carrow House

8) Ensure access to services if county hall lost by reconfiguring Core Infrastructure Services (DHCP, DNS, Active directory)

9) Implement Cloud-based business systems with resilient links for key areas

10) Replace voice services (contact center / desk phones) with resilient cloud based service including

Relocate resilient Network Routing Server to allow call routing to continue for other sites if County Hall failed

Reconfigure sites to point to an active Survivable Media Gateway (one of the 4 ISDN sites) so if Avaya fails a reduced fall back service is available

11) Review and Implement suitable arrangments to protect against possible cyber / ransonware attacks including

- Carry out recommendations from Cyber Security Audit
- Carry out recommendations from Phishing Simulation exercise, and repeat
- Retire Windows 2003
- Implement new client service security for Windows 10 build
- Independent IT Health Check for PSN accreditation (Oct 2017)

Overall risk treatment: Treat

Progress update

Progress update

Progress completed to date

1) Full power down completed and procedures updated from lessons learned.

2) Voice and Data reprocurement complete and implemented significantly increasing resilience for the Wide Area Network and internet.

3) Commissioned Independant Data centre and power audit, complete August 2017, recommended separate diverse power supply and new data centre's, costing additional power and plan (subject to approval) new data centre's as part of basement / lower ground refurbishment.

4) New storage procured, implemented in July 2017, providing additional resilience and necessary DR capability once a full DR site is implemented

5) New Microsoft Server Infrastructure procured implementation complete ready for migration when ready to test full DR capability.

8)All core infrastructure services (DNS, AD, ADFS, NPS, AlwaysOn VPN) are now clustered across to the Secondary site ;

- All production Wintel servers (380) are now replicated to the Secondary site;
- Email system is now able to operate independent of County Hall campus. This includes user’s access to mailbox as well as ability to send/receive internal and external emails.

9) Cloud-based highways management system has been implemented; Liquid Logic replacement is remotely hosted with resilient network connections ordered; review of Oracle hosting has commenced.

11) To mitigate against a cyber attack Network segregation has been improved over the Wide Area Network (WAN), ensuring all partners that use the NCC network are fully segregated. Denial of Service (DDOS) and Intrusion Prevention system (IPS) implemented on our internet gateways and robust patching and host based protection implemented on all NCC devices that attach to the network (This is a pre-requisite of PSN accreditation, and is an on-going task). A simulated phishing attack has been run (we are one of few Councils to have undertaken such an exercise) and results are being analysed. New client service security for Windows 10 has been successfully implemented and is being enforced as the new build rolls out.

Actions to be completed

6) Replacement New Local Area Network (LAN) to be procured to reduce risk of network failure.

7) New DR site work permissions approved, building work complete. The server, network and storage DR equipment will be moved into the identified site providing full failover facilities in the event of loss of County Hall. This is still on target to be complete by late Summer 2018.

8)All core infrastructure services (DNS, AD, ADFS, NPS, AlwaysOn VPN) to be moved Q3 2018 to the new DR site;

- Work started on the new Solaris EBS platform which by design is replicated to the Secondary site (go live Q4 2018);
- Network layer resilience main concepts agreed, design work initiated. This will be enhanced by the LAN refresh (Q4 2018);
- Works have started to reorganise/improve the site's Comms Room which will become ready as Secondary site Q3 2018;

10) Replacement of contact centre system to a cloud based service taking longer than expected. Skype for business project being reset and replanned to improve resilience and reduce dependencies on onsite infrastructure.

11) Work to complete recommendations from Cyber Security Audit is ongoing 5 out of 25 actions now complete with a target of December 2018, the work to retire Windows 2003 servers 26 remain 16 due to be complete by Jun 2018 leaving 10 including Oracle UCM, SMIS, call pilot which are all dependant on other projects but will be patched with security patches provided by the NHS, the recommendations from the Independent IT Health Check for PSN accreditation are 69% complete. We are working through the recommendation/actions from the phishing exercise and have completed 1 of the 12 we will complete all actions by October 2018.

Appendix A

Risk Number	RM14223	**Date of update**	19 June 2018
Risk Name	Payment Card Industry compliance of call monitoring system		
Risk Owner	Andrew Blaxter	**Date entered on risk register**	10 March 2015

Risk Description

The current call monitoring system is not up to current PCI compliance standards, potentially leaving the organisation exposed from a compliance perspective.

Original			**Current**			**Tolerance Target**				
Likelihood	Impact	Risk score	Likelihood	Impact	Risk score	Likelihood	Impact	Risk score	Target Date	Prospects of meeting Target Risk Score by Target Date
3	5	**15**	2	3	**6**	1	3	**3**	Oct-18	**Amber**

Tasks to mitigate the risk

New call monitoring capability will be brought in. Implementation date to be confirmed.

Progress update

Voice and data contract awarded. Updata have produced a Project Initiation Document (PID) and solution.

Implementation has been rolled back.

Finance are looking at new payment system, where calls are transferred to an automated service, removing all PCI risk of card data.

New call recording from Updata was available for release to NCC in May but no confirmed date for NCC implementation to the Customer Service Centre. New pay.net system is scheduled to go live in September 2018, where the Customer Service Centre will transfer calls to a payment line, removing the need to take credit card details.