Appendix A

Risk Number	RM010	**Date of update**	22 September 2017
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: reduce.

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**	Mar-18	**Amber**

Tasks to mitigate the risk

1) Full power down completed periodically.
2) Voice and Data reprocurement.
3) Commission Independent Data centre and power audit
4) Reproduce 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.
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 centre / 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 arrangements to protect against possible cyber / ransomware 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: reduce

Progress update

Progress update

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 Independent Data Centre and Power audit, which completed in August 2017. The audit recommended separate diverse power supply and new data centres. Costing additional power and plan (subject to approval) of new data centre's.
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 September 2017, implementation due by January 2018 providing additional resilience and necessary DR capability once full DR site is implemented.
6) Replacement New Local Area Network (LAN) to be procured in Nov/Dec 2017 to reduce risk of network failure.
7) New potential DR site identified, and work has started to cost and seek relevant permission to implement. Once complete server, network and storage DR equipment will be moved into the new site providing full failover facilities in the event of loss of County Hall. Estimated timescale for completion; by Summer 2018.
8) The Core Infr-
astructure Services (DHCP, DNS, Active directory) will be reviewed and reconfigured to enable access to systems and services in the event of the loss of County Hall and/or the DR site January 2018; implementation Summer 2018.
9) Cloud-based highways management system has been implemented; Liquid Logic replacement is remotely hosted and due live by April 2018 with resilient network connections ordered; review of Oracle hosting has commenced.
10) Replacement of contact centre system to a cloud based service due to begin migration to the cloud service Q4 2017, with full completion by Q1 2018 and replacement of the desktop telephony with Skype for business initial pilot late 2017.
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) has been 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 ongoing task). A simulated phishing attack has been run and the results are being analysed.

Appendix A

Risk Number	RM14223	**Date of update**	14 September 2017
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**	Nov-17	**Amber**

Tasks to mitigate the risk

New call monitoring capability will be brought in from November 2017.

Progress update

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

Implementation has been rolled back from April 2017 to November 17.

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