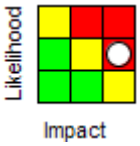
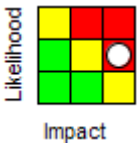
IT Risk Register Entries

Generated on: 28 February 2020

Risk Code	CR62	Risk Title	Cyber Risks
Risk Owner	Howard Crompton	Updated By	Vic Godfrey
Year Identified	2014	Corporate Priority	Responsive and Efficient
Risk Description	**As a result of:** - Computer virus - Malware - Ransomware - Computer hacking - Action by Staff/Member (e.g. opening a malicious link) - Malicious tampering of computer records - Information being sent to the wrong recipient - Loss or damage to server room **There is a risk of:** - Systems being interrupted or damaged - Data being corrupted or erased - Personal data being stolen - Breach of the Data Protection Act 2018		
Opportunities	- Safe and effective use of Information Technology		
Consequences	The consequences of these risks include: - Loss of reputation - Ability to provide services is disrupted - Revenue streams are reduced - Additional costs to investigate and test following repair/restoration - Claims for compensation if a third party suffers a financial loss - Fines from the Information Commissioner		
Work Completed	- Information Security policy in place, which applies to staff and Members use of IT systems - Email encryption software (EGress) implemented - Introduced new software (Clearswift and Bloggs) to enhance the checking of threats attempting to attack via the firewall - All data centres have fire suppressing systems and are located in secure areas - Disaster recovery in place at a remote site (Unit 3) - Basic computer insurance provides limited cover for damage to equipment and reinstatement of data (although it does not cover payment of any fines or compensation to third parties) - Business Continuity Plans in place - Ransomware attack resulting in the write-off of IT hardware and infrastructure identified as a financial risk for 2019/20 (Low/£200k) - Data Protection/FOI SIAS internal audit - Controls in place to ensure any third party providers adhere to NHDC security requirements - Annual PEN Test completed autumn 2018 and PSN Accreditation renewed January 2019 - SIAS audit of Cyber Security (March 2018) provided Moderate overall assurance - Implemented specific cyber roles/responsibilities within the ICT team to strengthen resources and approach (September 2018) - Implemented the recommendations from the SIAS audit of Cyber Security - Reviewed findings of the 2018 penetration test and worked through the minor improvements identified - In 2019, the requirement for Members to be registered as Data Controllers with the ICO was removed - SIAS audit of Cyber Security (August 2019) provided Satisfactory overall assurance and the report made five recommendations (four medium priority and one low priority)		

Ongoing Work	- Anti-virus/malware software in place and automatic updates are performed to servers and all PCs/laptops/tablets - Email Filter monitoring - Web Filter monitoring - Firewalls continually reviewed and updated - Reviewing firewall log files - Microsoft patches kept up to date - Annual PEN Test will be undertaken in December 2019 and PSN Accreditation will be renewed January 2020 (Annual PEN Test to commence following the relevant tender process) - Regular advice and reminders issued to users - LMS training available (e.g. annual DPA 2018) - Control/security systems enable potential threats to be identified, investigated and managed accordingly - Regular reminders to all staff and Members are sent by the Service Director - Customers about the need to be vigilant about opening emails from unknown sources - Attending MHCLG Cyber Pathfinder Training Scheme events (next one due in late 2019 in Cambridge) - Implementing the recommendations from the SIAS audit of Cyber Security (August 2019), including the forthcoming release of a new Cyber Security mandatory training package		
Current Impact Score	3	**Current Likelihood Score**	2
Overall Risk Score	8	**Current Risk Matrix**	
Date Reviewed	30-Sep-2019	**Next Review Date**	30-Mar-2020
Latest Note	01-Oct-2019 Risk reviewed and updated by Vic Godfrey on 30 September 2019. NHDC continues to assess and improve its cyber security arrangements, although this remains a challenging and evolving process. The requirement for Members to be registered as Data Controllers with the ICO was removed in 2019 and the Risk Description has been amended accordingly. No change made to the overall risk score.		

Risk Code	RR304	Risk Title	Data Protection Act 2018
Risk Owner	Howard Crompton	Updated By	Vic Godfrey
Year Identified	2005	Corporate Priority	Responsive and Efficient
Risk Description	As a result of: - Action by individuals (e.g. use of the email system is the predominant cause of breaches) - CCTV systems not being fully compliant - Retention of out of date information on IT systems and in hard copy - Inappropriate use/disclosure of personal information - Fraudulent use of data - Loss or theft of portable devices There is a risk that: - There could be breaches of the Data Protection Act 2018 (the UK's implementation of the General Data Protection Regulation)		
Opportunities	- Ensuring compliance with legislation and appropriate handling of personal data - Reduced disk storage requirements, leading to reduced costs		
Consequences	- Inappropriate use/disclosure of personal information - Fraudulent use of data - Enforcement/Information Notice being served by the Information Commissioner - Penalties under the General Data Protection Regulation, i.e. 4% of annual global turnover or €20 million, whichever is greater - Loss of reputation and customer confidence/trust		
Work Completed	- Information Security and Internet/Email user policy prevents staff sending emails to their home address - Incident Register in place - Data protection policy in place - NHDC creates its own data sharing protocols on a case-by-case basis; data sharing agreements are in place with all relevant external organisations - Information security policy adopted on the 02 February 2011 and it is reviewed on a regular basis - Purchased Active Navigation software, which highlights duplicate records and out of date information/documentation held on the network and recommends appropriate filing systems for stored information - EGress email encryption software replaced with Clearswift Email Encryption for the corporate wide encrypted and secure sending of personal, confidential and sensitive information outside of the authority - USB encrypted pens are monitored by GIF Software - All NHDC CCTV systems are fully data compliant - ICT has ownership of all CCTV devices within the authority buildings, which also includes displayed signage and extraction of data when requested via a Subject Access Request (SAR) - Software in place to redact images if there is a request for CCTV images (the amount of time required to redact images manually was lengthy/costly) - Network log-in screens detail terms/conditions of use - NHDC data protected on portable devices - Financial risk identified for 2019/20: -- Fines for breaches of the EU General Data Protection Regulation by the Council or by NHDC outsourced providers when handling and storing data originally collected by NHDC (Low/£500K) - SIAS audit of Data Protection and Freedom of Information (December 2016) provided moderate overall assurance - Officer seconded to the Information Team to help with preparations for the General Data Protection Regulation - Auto-forwarding of emails was switched off on 26 June 2017, in line with the high priority SIAS audit recommendation - Presentation to Senior Managers Group (November 2017) - Implemented the recommendations from the SIAS audit of Data Protection and Freedom of Information (December 2016)		

	- Full information audit completed, including gap analysis and review of processes/procedures, and agreed actions implemented to ensure compliance with the General Data Protection Regulation - Member information/training sessions - SIAS audit of General Data Protection Regulations (July 2018) provided Satisfactory overall assurance - Designated Data Protection Officer in place - Information Security Policy published - Developed strategy for officers/Members to use BlackBerry Apps to deliver better services at reduced cost across the authority - Completed required changes to documentation, e.g. fair processing notices - Implemented the recommendations from the SIAS audit of General Data Protection Regulations (July 2018) - Requirement for Members to register as a Data Controller with the ICO removed in 2019 (previously, if requested by Members, officers did this on their behalf, including payment of the fee)		
Ongoing Work	- Mandatory annual training via e-learning; completion by staff monitored and escalation processes in place - Regular reminders to staff and Members on the use of email - The use of email quotas forces individuals to review the data they are keeping - Continue to implement/monitor the Active Navigation tool - Information Team works with service areas to ensure all departments are keeping documents in line with their retention schedules - Annual review of CCTV in Operation notices to ensure they are up to date and fully displayed (all areas covered by cameras, including meeting rooms) - Monthly tests of all CCTV data extraction processes are carried out - ICT control and monitor regularly data storage and retention in off site facility - Identified DPA breaches reported to the ICO if required; so far, the ICO has not instigated any formal action - Ongoing communication with officers and Members to raise awareness - Regular officer meetings to review/discuss DPA 2018 issues - Implementation of new systems/databases require the completion of Privacy Impact Assessments and if required, Data Processing Agreements - Draft "GDPR Operational" SIAS audit report received, which provides Satisfactory overall assurance; awaiting publication of the final report		
Current Impact Score	3	**Current Likelihood Score**	2
Overall Risk Score	8	**Current Risk Matrix**	
Date Reviewed	30-Sep-2019	**Next Review Date**	30-Mar-2020
Latest Note	03-Oct-2019 Risk reviewed and updated by Vic Godfrey on 30 September 2019. The recently received draft "GDPR Operational" SIAS audit report provided Satisfactory overall assurance and it did not highlight any significant findings (two Medium and two Low priority recommendations). No change made to the overall risk score.		

Risk Code	RR493	Risk Title	IT Disaster Recovery
Risk Owner	Howard Crompton	Updated By	Vic Godfrey
Year Identified	2013	Corporate Priority	Responsive and Efficient
Risk Description	As a result of a: - Cyber attack - Power failure in Letchworth - Problem with the broadband service provider There is a risk that: - There is a total loss of IT network services NHDC has now developed an in-house fully functional Disaster Recovery solution, which enables IT to be able to bring services back online within 4 hours.		
Opportunities	- Effective DR arrangements ensure the ongoing provision of IT network services		
Consequences	- Business continuity arrangements become ineffective - Increased time required to recover from events - NHDC unable to deliver its services		
Work Completed	- In 2014/15, the in-house IT Technical Team built a fully functional DR solution, which enables them to bring back online core services within 4 hours instead of the 4 days with the HP DR Service in London - Within the 2015/16 IT Service Plan, IT carried out two rehearsals to recover data, which tested positively and well within the 4 hours - To compliment the new DR service, IT have installed an additional 100Meg Broadband Service, which is provided by BT, to ensure there is also resilience in the event of any issues with the Virgin Media Broadband Services; this will ensure there is connectivity available to home workers - The new DR Site at Unit 3 is now fully functional with its own Data Centre, BT Broadband DR link and a 12-hour UPS system - The Data Centre has been built in accordance with PSN security requirements, which means it has FM200 Gas Protection, CCTV, Building Alarm and Heat Monitoring and alerts systems provided by Trend - Careline DR now relocated to Unit 3 - Diesel generator relocated to the DCO - Implemented and tested relevant infrastructure required for Careline's move to the refurbished DCO		
Ongoing Work	- IT continue to be responsible for disaster recovery of corporate systems relating to infrastructure failures resulting from general failures or any environmental interventions such as fire, flooding etc. - Depending on the nature of the failure, users will continue to be responsible, as the system owners, for working with their suppliers where systems are down for other reasons, such as software failures due to bugs, upgrade failures etc. - Rehearsals are carried out quarterly, which are documented in accordance with the SIAS Audit - There are six IT staff who receive alerts and Property Services, which is a 24x7 service - The latest rehearsal identified the need to enhance our current disaster recovery arrangements, which requires establishing a disaster recovery loop (by adding further back-up at one further site, i.e. Hitchin Town Hall) - Following Brexit considerations, increasing the diesel generator run time at the DCO from two to 12 days, in order to improve the resilience of the IT network (using available Brexit funding)		
Current Impact Score	2	Current Likelihood Score	1
Overall Risk Score	3	Current Risk Matrix	
Date Reviewed	05-Feb-2020	Next Review Date	29-Jan-2021

Latest Note	05-Feb-2020 Risk reviewed by Vic Godfrey on 5 February 2020. In view of the effective DR arrangements that the Council has implemented over a number of years, Vic agreed to reduce the Impact score to Medium. The risk entry will remain active in view of the plans to increase the diesel generator run time at the DCO and to establish a disaster recovery loop (by using three sites), which will enhance our arrangements further.