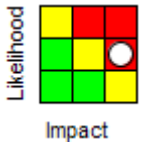
IT risks

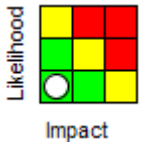
Report Author: Fiona Timms
Generated on: 23 April 2015

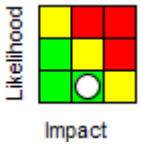
Risk Code	RR304	Risk Title	Data Protection Act
Risk Owner	Howard Crompton	Updated By	Vic Godfrey
Year Identified	2005	Corporate Priority	
Risk Description	- Breaches of the Data Protection Act by individuals (use of email system is the predominant cause) - CCTV systems may not be fully compliant - Retention of out of date information on IT systems and in hard copy - Inappropriate use/disclosure of personal information - Fraudulent use of data		
Opportunities	- Ensuring compliance with legislation and appropriate handling of personal data - Reduced disk storage requirements (which are currently escalating - December 2011), leading to reduced costs		
Consequences	- Any breach of the DPA can lead to a fine of up to £500k (per breach) from the Information Commissioner: -- inappropriate use/disclosure of personal information -- fraudulent use of data - Notice being served by the Information Commissioner - Loss of reputation and customer confidence		
Work Completed	- Internet and email policy prevents staff sending emails to their home address. - Incident Register procedures reviewed and approved by Legal in 2009 - Training via e-learning - Data protection policy released - Monitoring Officer review of data protection conducted - All staff trained within the Gov Connect guidelines for the use of data - The County Information Group proposed a countywide information data sharing protocol, but this was not practical. NHDC creates its own protocols on a case-by-case basis and has a number of agreed protocols in place. - Information security policy adopted on the 02 February 2011 next review scheduled for January 2016 - Identified a tool that will highlight duplicate records and out of date information / documentation held on the network and will recommend appropriate filing systems for stored information - software (Active Navigation) now purchased - Property Services now responsible for the maintenance of the CCTV system and for extracting data from it - Property Services staff have been trained on the extraction process - refresher training required every six months (next due May 2013) - Email encryption software (EGress) used corporate wide for sending personal, confidential and sensitive information outside of the authority - training took place in February 2013 followed by a roll-out across the authority - USB encrypted pens – a small number of authorised users have been issued with USB pen devices, which are monitored by GIF Software - Reminder to staff and Members on the use of email sent on the 25/02/2013 - Email quotas are forcing individuals to review data they are keeping		
Ongoing Work	- Property Services to check the CCTV system whenever Quadrant performs its maintenance checks - Implement the tool (Active Navigation) to highlight duplicate records and out of date information / documentation held on the network and recommend appropriate filing systems for stored information - the project team are working with service areas to highlight duplicate records, records not		

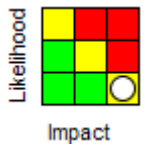
	complying within the data retention schedules etc. The Information Team have now meet all departments to firstly help them to identify and remove duplicate records and secondly to review large files stored. Work continues within this area to ensure departments are keeping documents in line with their retention periods. - As part of the Office Accommodation project, - Review CCTV in Operation notices to ensure up to date and fully displayed – all areas covered by cameras, including meeting rooms - Investigate software options for redacting images if there is a request for CCTV images - the amount of time required to redact images manually is lengthy/costly - To review data storage in boxes held at Royston. Some have a do not destroy sticker on them - but need to have an end date. Work continues on a month by month basis to review the Royston store and any soft media that has passed its retention period is scheduled for destruction and shredding which is organised by Property Services - Mandatory training on data protection is an annual requirement for managers and every 3 years for other members of staff - Members encouraged to use North Herts email address rather than auto forwarding. Good App is available for members to use. To date we now have 16 Members actively using the Good App to read and reply to emails and I have another 8 who are partially setup and I'm waiting for the User Agreement to come back to IT. - We currently have 2 x Dell Tablets out with Cllrs Clare Billing and Cllr Faye Frost who are Pilot testing as part of a bigger project to reduce paper copies of committee reports with the added benefit of NHDC providing them with a Tablet with the Good App to receive emails. -Currently the ICT Manager and HOS are reviewing the strategy of using the Good App Tools to deliver better services at reduced cost across the authority. - Members advocating for a constituent should be registered as a Data Controller with the ICO This is an area of concern albeit not a direct responsibility of the NHDC Data Controller. In 2013/14 6 Members claimed the £35.00 back which was the registration fee for them to become a Data Control and in 2014/15 on 4 Members have claimed the £35.00 back. However, it might be that other Members have registered but just not claimed the Data Registration back via expenses

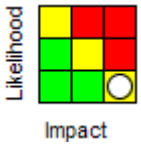
Current Impact Score	3	**Current Likelihood Score**	2
Current Risk Matrix			
Date Reviewed	11-Feb-2015	**Next Review Date**	01-Feb-2016
	FINANCIAL		
	INFORMATION		
	REGULATORY		
	REPUTATION		

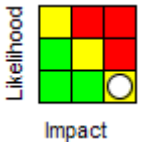
Linked Action Status	Linked Action Title	Linked Action Due Date	Responsible Officer

Risk Code	RR434	**Risk Title**	Compliance with Freedom of Information Act, Environmental Information Regulations and Local Government Transparency Code
Risk Owner	Howard Crompton	**Updated By**	Vic Godfrey
Year Identified	2009	**Corporate Priority**	
Risk Description	As a result of the requirements to provide information under various legislative requirements to promote openness and transparency there is a risk that NHDC fails to provide information requested under the FOI Act 2005 and EIR Regulations 2004 within 20 days and to comply with the Transparency Code 2014. Failure to provide requested information may result in a complaint to the Information Commissioner.		
Opportunities	- Full compliance with the Freedom of Information Act 2005, Environmental Information Regulations 2004and Transparency Act		
Consequences	- Complaints made re response time/non-compliance with Transparency Code - Investigation by the Information Commissioner - Recommendations made if the authority is not working within the Act - Non-compliance with the FOI Act and EIR may result in the authority being fined - Loss of reputation		
Work Completed	- There are two admin support staff and two fully trained FOI staff. This allows for sickness and annual leave to be covered - Service areas are given timescales to work to by Information Management, which keeps a record of requests and status of replies - There are now 3 Officers who deal with FOI, EIR and Data Protection following a restructure within IT which was completed in December 2014.		
Ongoing Work	- Staff training on FOI and EIR via online e-learning module - Implementing the internal audit recommendations on Open Data may prevent a few FOI enquiries - There has been a massive increase in FOI and DP requests over the past 2 years: 2013/14 – FOI 563 with 95% completed within the 20 day timescale, DP 4 with 100% completed within the 40 days. 2014/15 – FOI 554 with 98.19% completed within the 20 days, DP 48 with 97.02% completed within the 40 days. These figures are as of the 9th Feb 15. - Staff Training – The LMS and dates last completed need to be reviewed to ensure staff and Managers are still complaint. - Information Team to review compliance with Transparency Code		
Current Impact Score	1	**Current Likelihood Score**	1
Current Risk Matrix			
Date Reviewed	11-Feb-2015	**Next Review Date**	01-Feb-2016
	FINANCIAL		
	INFORMATION		
	REGULATORY		
	REPUTATION		

Risk Code	RR492	**Risk Title**	Software Patch Management
Risk Owner	Howard Crompton	**Updated By**	Vic Godfrey
Year Identified	2013	**Corporate Priority**	Living within our means
Risk Description	Due to changes in working practices (e.g. home working effectively allowing officers to work seven days a week) and reduced resources within IT there is a risk that software patch management will not be delivered effectively without an agreed policy/schedule in place. This may lead to: - Required software patch management not being completed - Increased unplanned system down time - Adverse impact on the delivery of NHDC services, e.g. Careline - Pressure on IT resources to deal with associated issues		
Opportunities	NHDC's systems remain up to date and secure without any unplanned down time.		
Consequences	- Required software patch management not being completed - Increased unplanned system down time - Adverse impact on the delivery of NHDC services, particularly Careline - Pressure on IT resources to deal with associated issues		
Work Completed	Schedule now in place for quarterly updates. Reminder sent to staff two weeks before this happens.		
Ongoing Work	IT to develop a policy relating to software patch management, including scheduling required works on a regular basis (e.g. one weekend per month). IT restructure to take place which will align duties and skills to better manage the network & infrastructure. Notice given to users when systems are likely to be down Essential maintenance takes place over the weekend every few months. Systems taken down immediately if there is a security issue There are now Planned Maintenance Days booked within IT diaries to ensure that in the need of any none urgent patches being required to be installed can be properly programmed in. All Microsoft Patches are pushed out to Desktops/Laptops fortnightly vi Microsoft's SCCM and all Anti Virus updates are electronically reviewed and installed automatically every hour.		
Current Impact Score	2	**Current Likelihood Score**	1
Current Risk Matrix			
Date Reviewed	11-Feb-2015	**Next Review Date**	01-Feb-2016
	OPERATIONAL		
	PEOPLE		
	REPUTATION		

Risk Code	RR493	**Risk Title**	IT Disaster Recovery
Risk Owner	Howard Crompton	**Updated By**	Vic Godfrey
Year Identified	2013	**Corporate Priority**	Living within our means
Risk Description	NHDC currently has a contract with HP for provision of hardware to enable system restoration. Due to an increased demand on IT resources, there is a risk that IT officers will not be able to complete the two rehearsal periods each year for restoring systems offsite. This may lead to: - Business continuity arrangements becoming ineffective - Increased time required to recover from events - NHDC being unable to deliver its services		
Opportunities	IT prepared fully for implementing its disaster recovery plans effectively.		
Consequences	- Business continuity arrangements become ineffective - Increased time required to recover from events - NHDC unable to deliver its services		
Work Completed	- Action included in the service plan for 2014/15. - NHDC IT staff attended the HP Disaster Recovery Centre at Kings Cross between the 11th and 13th March 2014 to perform the annual rehearsal on recovering systems and data as per the HP Contract. This also gave officers the opportunity to review relevant documentation and procedures to ensure they were still compliant and relevant. This year, one of the other Senior Technical Staff attended, providing a fresh pair of eyes to look over the arrangements. The restore of systems was successful, with full complete restore completed by 13:00 on Day 3. However, there would be the need for full user testing of applications, which needs to be considered. HP provided a certificate to confirm NHDC's successful recovery process.		
Ongoing Work	- IT will 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, this may require full use of the contractual arrangements with HP for use of their Disaster Recovery Centre. 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 -IT have just finished building an in-house DR solution which is hosted within another building in Letchworth. Full Testing Rehearsals are still taking place prior to this going LIVE on the 31st March 2015. 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. In the 2015/16 Capital programme there is a bid for a generator to be installed in the car park of the DCO which again will compliment the 6hr UPS System that is already in place.		
Current Impact Score	3	**Current Likelihood Score**	1
Current Risk Matrix			
Date Reviewed	05-Feb-2014	**Next Review Date**	01-Feb-2016
	OPERATIONAL		
	PEOPLE		
	REPUTATION		

Risk Code	RR498	**Risk Title**	Public Services Network (PSN)
Risk Owner	Howard Crompton	**Updated By**	Vic Godfrey
Year Identified		**Corporate Priority**	Living within our means to deliver cost-effective services
Risk Description	As a result of the absolute deadline to be re-accredited with the Code of Connection (CoCo), there is a risk that NHDC will fail to be compliant by the deadline (August annually) leading to the loss of the connection with government services.		
Opportunities	PSN provides an assured network over which NHDC can safely share services with government , including many G-Cloud services, to collaborate in new ways, more effectively and efficiently.		
Consequences	The consequences of this risk include - loss of link to DWP which would mean benefit claims are unable to be checked - benefit claimants could loose benefit causing extreme financial hardship - loss of ability to share data with other government departments - impact on homelessness service		
Work Completed	Previously re accredited for CoCo. Robust security measures already in place in order to prevent loss of data by security breaches. Re accreditation obtained for 2013/14 at a cost of £35,000 for hardware plus manpower costs Penetration tests completed Critical and High level recommendations adhered to		
Ongoing Work	To raise with the Cabinet office due to costs and resources involved. PSN Compliance was awarded in August for 2014. Work commences in April on the 2015 PSN Accreditation which has been captured in the IT Service Plan: April – Review suppliers and award the contract for the annual PEN Test May – PEN Test carried out June-July – Action plan put together on any outcomes found from the PEN Test August – Submission to the Cabinet Office for the PSN Accreditation. This is due on the 25th August 15.		
Current Impact Score	3	**Current Likelihood Score**	1
Current Risk Matrix			
Date Reviewed	11-Feb-2015	**Next Review Date**	01-Feb-2016
	FINANCIAL		
	INFORMATION		
	OPERATIONAL		
	PEOPLE		
	REPUTATION		

Risk Code	RR522	**Risk Title**	Cyber Risks
Risk Owner	Howard Crompton	**Updated By**	Vic Godfrey
Year Identified	2014	**Corporate Priority**	Living within our means
Risk Description	As a result of: - Computer virus - Malware - Computer hacking - Malicious tampering of computer records - Information being sent to the wrong recipient - Loss or damage to server room There is a risk of: - Data being corrupted or erased - Personal data being stolen - Breach of the Data Protection Act		
Opportunities	Safe and effective use of Information Technology		
Consequences	The consequences of these risks include: - Ability to provide services is disrupted - Revenue streams are reduced - Additional costs to investigate and test following repair/restoration - Loss of reputation - Claims for compensation if a third party suffers a financial loss - Fines from the Information Commissioner		
Work Completed	- Anti virus/malware software is in place and automatic updates are performed to Servers and all PCs/Laptops - Email Filtering Monitoring - Web Filter Monitoring - An annual Penetration test is carried out in line with Cabinet Office (PSN) requirements, which was undertaken in June 2014 with NO Risk Identified to Security - Information Security policy applies to staff and Members use of IT systems - Annual PSN accreditation - Email encryption software - Server room has fire suppressing system and is in a secure area - Disaster recovery contract in place at a remote site - Computer insurance covers reinstatement of data and increased cost of working in the event of physical loss or damage (but not from hacking/viruses)		
Ongoing Work	Annual PEN Test and PSN Accreditation. The introduction of new software called Clearswift and Bloggs this year has enhanced the checking of threats trying to attack via the Firewall. IT have also recently installed 2 new Firewalls which contain modern and improved threat software.		
Current Impact Score	3	**Current Likelihood Score**	1
Current Risk Matrix			
Date Reviewed	11-Feb-2015	**Next Review Date**	01-Feb-2016
	FINANCIAL		
	INFORMATION		
	OPERATIONAL		

	PEOPLE
	REGULATORY
	REPUTATION