Public Document Pack

Information Technology Sub (Finance) Committee

Date: **THURSDAY, 31 MAY 2018**

Time: **1.45 pm**

Venue: **COMMITTEE ROOMS - WEST WING, GUILDHALL**

Members:
Deputy Jamie Ingham Clark (Chairman)
Randall Anderson (Deputy Chairman)
Deputy Keith Bottomley
John Chapman
Tim Levene
Jeremy Mayhew
Deputy Robert Merrett
Sylvia Moys
Alderman Andrew Parmley
James Tumbridge

Enquiries: **Paige Upchurch**
paige.upchurch@cityoflondon.gov.uk

Lunch will be served in the Guildhall Club at 1pm

John Barradell
Town Clerk and Chief Executive

AGENDA

Part 1 - Public Agenda

1. **APOLOGIES**

2. **MEMBERS' DECLARATIONS UNDER THE CODE OF CONDUCT IN RESPECT OF ITEMS ON THE AGENDA**

3. **MINUTES OF THE PREVIOUS MEETING**
To agree the public minutes and non-public summary of the meeting held on 26 March 2018.

For Decision
(Pages 1 - 8)

4. **OUTSTANDING ACTIONS FROM PREVIOUS MEETINGS**
Report of the Town Clerk.

For Information
(Pages 9 - 10)

5. **WORK PROGRAMME FOR FUTURE MEETINGS**
Joint report of the Town Clerk and Chamberlain.

For Information
(Pages 11 - 12)

6. **INTERACTIVE DIGITAL SESSION - DEMO OF THE SURFACE HUB AND OFFICE.COM AND INTEGRATING DIARIES**
Verbal report of the Chamberlain

For Information

7. **IT DIRECTOR SUMMARY**
Report of the Chamberlain

For Information
(Pages 13 - 16)

8. **IT DIVISION RISK UPDATE**
Report of the Chamberlain

For Information
(Pages 17 - 20)

9. **GENERAL DATA PROTECTION REGULATION (GDPR) UPDATE REPORT**
Report of the Comptroller

For Information
(Pages 21 - 26)

10. **CHANGE AND ENGAGEMENT APPROACH**
Report of the Chamberlain

For Information
(Pages 27 - 30)

11. **DESIGN, BUILD, SUPPORT AND HOSTING FOR NEW WEBSITE**
Report of the Town Clerk (Director of Communications)

For Information
(Pages 31 - 34)

12. **QUESTIONS ON MATTERS RELATING TO THE WORK OF THE SUB COMMITTEE**

13. **ANY OTHER BUSINESS THAT THE CHAIRMAN CONSIDERS URGENT**

14. **EXCLUSION OF THE PUBLIC**
MOTION - That under Section 100(A) of the Local Government Act 1972, the public be excluded from the meeting for the following items on the grounds that they involve the likely disclosure of exempt information as defined in Part I of Schedule 12A of the Local Government Act.

For Decision

Part 2 - Non-Public Agenda

15. **NON-PUBLIC MINUTES OF THE PREVIOUS MEETING**
To agree the non-public minutes of the meeting held on 26 March 2018

For Decision
(Pages 35 - 38)

16. **OUTSTANDING ACTIONS FROM NON-PUBLIC MINUTES OF PREVIOUS MEETINGS**
Report of the Town Clerk

For Information
(Pages 39 - 40)

17. **CR 16 INFORMATION SECURITY RISK**
Report of the Chamberlain

For Information
(Pages 41 - 54)

18. **DRAFT PERSONAL ACCESS DEVICE POLICY**
Report of the Chamberlain

For Decision
(Pages 55 - 60)

19. **IT TRANSFORMATION PROGRAMME - UPDATE REPORT**
Report of the Chamberlain

For Information
(Pages 61 - 66)

20. **FILE SHARES/ONEDRIVE PERMISSIONS BREACH**
Report of the Chamberlain

For Information
(Pages 67 - 70)

21. **MEMBERS' SURVEY RESULTS AND ACTION PLAN**
Report of the IT Director

For Information
(Pages 71 - 78)

22. **CITY OF LONDON POLICE IP TELEPHONY UPGRADE**
Report of the Chamberlain

For Information
(Pages 79 - 92)

23. **CITY OF LONDON CORPORATION & CITY OF LONDON POLICE IT STRATEGY UPDATE**
Report of the Chamberlain

For Information
(Pages 93 - 124)

24. **POLICE IT PROJECTS - UPDATE REPORT**
Report of the Head of Police IT

For Information
(Pages 125 - 130)

25. **NON-PUBLIC QUESTIONS ON MATTERS RELATING TO THE WORK OF THE SUB COMMITTEE**

26. **ANY OTHER BUSINESS THAT THE CHAIRMAN CONSIDERS URGENT AND WHICH THE SUB COMMITTEE AGREE SHOULD BE CONSIDERED WHILST THE PUBLIC ARE EXCLUDED**

INFORMATION TECHNOLOGY SUB (FINANCE) COMMITTEE

Monday, 26 March 2018

Minutes of the meeting of the Information Technology Sub (Finance) Committee held at Guildhall, EC2 on Monday, 26 March 2018 at 2.15 pm

Present

Members:

Deputy Jamie Ingham Clark (Chairman)
Hugh Morris (Deputy Chairman)
Rehana Ameer
Deputy Keith Bottomley
John Chapman
Jeremy Mayhew
Deputy Robert Merrett
Sylvia Moys

Officers:

John Cater	-	Town Clerk's Department
Paige Upchurch	-	Town Clerk's Department
Bob Roberts	-	Town Clerk's Department
Peter Kane	-	Chamberlain's Department
Sam Collins	-	Chamberlain's Department
Kevin Mulcahy	-	Chamberlain's Department
Sean Green	-	IT Department
Sam Kay	-	IT Department
Matt Gosden	-	IT Department
Gary Brailsford-Hart	-	City of London Police
Andrew Bishop	-	City of London Police
Michael Cogher	-	Comptroller

Present from Agilisys:
Adrian Davey
Eugene O'Driscoll
Sean Grimes
Andrew Mindenhall

1. **APOLOGIES**
   Apologies were received from Randall Anderson and James Tumbridge.

2. **MEMBERS' DECLARATIONS UNDER THE CODE OF CONDUCT IN RESPECT OF ITEMS ON THE AGENDA**
   There were no declarations.

3. **MINUTES OF THE PREVIOUS MEETING**

RESOLVED: That the public minutes of the meeting held on 09 February 2019 be approved as an accurate record.

4. **OUTSTANDING ACTIONS FROM PREVIOUS MEETINGS**

The Sub-Committee considered a joint report of the Town Clerk and the Chamberlain which provided updates of outstanding actions from previous meetings:

- The Chairman reminded the Members to complete the Member Survey.

RESOLVED: That the Sub-Committee noted the report.

5. **WORK PROGRAMME FOR FUTURE MEETINGS**

The Sub-Committee received a report of the Chamberlain regarding the Work Programme for future meetings and the following points were made:

- The Chairman commented that the roll out date for the report on GDPR was July, not June as mentioned in the report.

- The Chairman commented that future reports would take a greater look forward, looking further than the next two months.

RESOLVED: That Members noted the report.

6. **INTRODUCTIONS - NEW IT SENIOR MANAGEMENT TEAM**

The IT Director provided a verbal update to the Sub-Committee introducing Sam Collins; the new Head of Change and Engagement, and Andrew Bishop; the new Police Head of IT.

RESOLVED: That Members noted the new additions to the IT senior management team.

7. **INTERACTIVE DIGITAL SESSION - IPAD DEMO FROM IT ON HOW TO ACCESS EMAIL, CALENDAR AND ONEDRIVE AND USE OF SHAREPOINT FOR COLLABORATION**

Modern.Gov Demonstration

The IT Director provided the Sub-Committee with a demonstration on the Modern.Gov app and the following points were made:

- The IT Director informed Members that the app only provided public access when it is first downloaded, and private access could be obtained by contacting the Committee and Member Services team.

- The IT Director commented on the benefits of using the app including the ability to annotate and highlight sections of the papers and switching between the original and annotated agenda pack at the click of a button.

- The Chairman commented that the app allowed Members to have easy access to the papers that are only relevant to the Committees that each Member serves on. Also, that the app provided added security measures as information is kept in a separate secure app, rather than stored on the device.

- The IT Director informed Members that 'blue papers' could not be accessed via the Modern.Gov app.

One Drive Demonstration

The IT Director also provided the Sub-Committee with a demonstration on using One Drive and the following points were made:

- The IT Director informed Members that One Drive was a cloud based service which was secure and remote and users could share documents by inviting them into the document and editing the documents from different devises, rather than having multiple versions of the same document.

- The Chairman commented that the document author could decide who to share the document with, whereas with Share Drive an IT Officer decided access rights. It was further commented that One Drive was useful for Chairman and Deputy Chairman, particularly when dealing with urgencies.

- In response to a question the Chamberlain confirmed that One Drive could be used via outlook by way of document link, but this does not allow shared access.

- The IT Director commented that Blue Papers are likely to run off of One Drive in the future.

RESOLVED: That Members noted the demonstrations and agreed that demonstrations on new technology are a useful addition to the Sub-Committee meetings.

8. **IT DIVISION UPDATE**

The Sub-Committee received a report of the Chamberlain regarding the IT Division update and the following points were made:

- The IT Director informed Members that throughout the "Beast is East" snow storm the Corporation experienced no issues and very few calls to the IT Desk whilst many employees were working from home with their laptops. The Chairman commented that the corporation was now able to consider how agile working might be implemented.

- The IT Director commented on a hardware failure with the planning portal in January and that the hardware needed replacing and to be placed on the

same Agilisys platform as other systems. The Chairman requested that the IT Director come back to the Sub-Committee with further report on this issue.

- Members were informed that the Corporation had received its PCN licence and it would remain valid until the end of March 2018.

RESOLVED: That Members noted the update and that The IT Director look into replacing the planning portal and report back to the Committee.

9. **IT RISKS UPDATE**

The Sub-Committee received a report of the Chamberlain regarding an update on IT Risks and the following points were made:

- The IT Director informed Members that the Department has incurred one new risk and that the resilience power infrastructure risk has reduced. The three risk categories were confirmed as IT service, IT security and GDPR.

- The Chairman commented that the department are in strong position with a clear picture on risks.

RESOLVED: That Members noted the update.

10. **GDPR UPDATE**

The Sub-Committee received a report of the Comptroller and the City Solicitor regarding an update on GDPR and the following points were made:

- The Comptroller commented that the Corporation is in a good position in preparation for the new legislation regarding IT and policies and that the aim is to have compliance by 25th May 2018. It was further commented that in preparing for the GDPR the Comptroller has learnt that not all departments are fully compliant, but that breaches tend to be low level.

- The IT Director commented that the main changes in the department would be e-forms and considering the right to be forgotten. It was added that the department has been looking at where data has been stored in different systems and has been working with other regulators to ensure best practise.

- The Chairman commented that the 6 principles of data protection need to be known corporation wide and embedded into its culture.

RESOLVED: That Members noted the update.

11. **DATA PROTECTION POLICY**

Members considered a report of the Comptroller and City Solicitor regarding the Data Protection Policy and the following points were made:

- The Comptroller commented that the policy is a straight forward one and that it should be reviewed annually. The Chairman commented that the policy

should be reviewed at Member level in order to ensure openness and transparency and a Member commented that the reviews should be fazed by section to ensure that the policy is considered closely.

- A Member questioned whether the policy should be included in the Members Code of Conduct. The Comptroller commented that this could bring about floodgates as all legal requirements could then be included and the code of conduct could become exhaustive. The Chairman added that the Code of Conduct should remain about principles and simple.

RESOLVED: That Members Approved and agreed to adopt the revised Data Protection Policy set out in Appendix 1 with effect from 25 May 2018.

12. **MEMBER SURVEY**

The Sub-Committee received a verbal report from the Chamberlain regarding the Member Survey and the following points were made:

- There have been 36 responses so far and from these it has been found that:
    - 80% of Members use City of London equipment;
    - 16% use Modern.Gov;
    - Members provided good feedback on room equipment;
    - Members felt they had a good awareness of GDPR but wanted to know how it affects different roles;
    - Members did not take well to the suggestion of a secure email, as the city email address is sufficient;
    - Members commented on Wi-Fi issues, the department has worked with O2 to fix this problem.

- The Chairman commented that work should go into increasing the number of Members that use Modern.Gov in order to get full use out of the software and requested that a report is submitted to the next meeting detailing the findings.

RESOLVED: That the Members noted the update.

13. **WEBSITE PROJECT UPDATE**

The Sub-Committee received a report of the Chamberlain and the Town Clerk regarding an update on the website project and the following points were made:

- The Chamberlain informed Members that the project went to the Project Sub-Committee and received approval to go out to tender and the next stage is to consult about what the website should do and feature. It was added that the aim is to start building the website in 2019.

- The Chairman commented that other areas of the Corporation might want to 'piggyback' on the web design project, the Barbican was mentioned as an example. The Chamberlain confirmed that there is a meeting planned to establish this.

- In response to a question the Chamberlain confirmed that the whole project will cost £213,000 and the ongoing annual cost will amount to £80,000-£150,000.

RESOLVED: That Members noted the update.

14. **QUESTIONS ON MATTERS RELATING TO THE WORK OF THE SUB COMMITTEE**

Enhanced Wi-fi
In response to a question the IT Director confirmed that there have been no problems regarding enhancing the Wi-fi within the Guildhall complex.

15. **ANY OTHER BUSINESS THAT THE CHAIRMAN CONSIDERS URGENT**

Chairman's Thanks

- The Chairman thanked Adrian Davey who is leaving his role and commented that he has been the driver of the transportation project which has been a huge success.

- The Chairman also expressed his thanks to John Cater, the Committee Clerk who is stepping down from this role and welcomed Paige Upchurch who is taking over.

- The Chairman thanked The Members and Officers of the Committee for their work this year as it is the last meeting of the Common Council year.

16. **EXCLUSION OF THE PUBLIC**

RESOLVED: That under Section 100(A) of the Local Government Act 1972, the public be excluded from the meeting for the following items on the grounds that they involve the likely disclosure of exempt information as defined in Part I of the Schedule 12A of the Local Government Act.

17. **NON-PUBLIC MINUTES OF THE PREVIOUS MEETING**

RESOLVED: That the non-public minutes of the meeting held on 09 February 2019 be approved as an accurate record.

18. **OUTSTANDING ACTIONS FROM NON-PUBLIC MINUTES OF PREVIOUS MEETINGS**

The Sub-Committee considered a joint report of the Town Clerk and the Chamberlain which provided updates of outstanding actions from previous meetings that arose from the non-public minutes.

19. **IT SECURITY UPDATE CR16**
The Sub-Committee considered a report of the Chamberlain regarding an update on CR 16 Information Security Risk.

20. **POLICE IT PROJECTS - UPDATE REPORT**
The Sub-Committee received a report of the Chamberlain regarding Police IT projects.

21. **PERSONAL ACCESS DEVICE POLICY**
The Sub-Committee considered a report of the Chamberlain regarding a draft personal access devise policy.

22. **EMAIL USE POLICY**
Members considered a report of the Comptroller and the City Solicitor regarding the email use policy.

- *The Chairman considered item 24 next so that those from Agilisys could leave the meeting after this item.*

24. **TRANSFORMATION - STRATEGIC**
The Sub-Committee received a report of the Chamberlain regarding the IT Transformation Programme.

- *Those in attendance from Agilisys left the meeting at this point.*

23. **IT OPERATING MODEL AND STRUCTURE CHANGES PROPOSAL**
The Sub-Committee received a report of the Chamberlain regarding the IT Operating Model and a proposal to structural changes.

25. **NON-PUBLIC QUESTIONS ON MATTERS RELATING TO THE WORK OF THE SUB COMMITTEE**
There were no non-public questions.

26. **ANY OTHER BUSINESS THAT THE CHAIRMAN CONSIDERS URGENT AND WHICH THE SUB COMMITTEE AGREE SHOULD BE CONSIDERED WHILST THE PUBLIC ARE EXCLUDED**
There was no other non-public business.

The meeting ended at 4.11 pm

Chairman

Contact Officer: Paige Upchurch
Paige.Upchurch@cityoflondon.gov.uk

Information Technology Sub-Committee – Public Outstanding Actions

Item	Meeting Date	Action and target for completion	Officer responsible	To be completed/ Next stage	Progress update
	26 March 2018	Planning Portal report The IT Director commented on a hardware failure with the planning portal in January and that the hardware needs replacing and to be placed on the same Agilisys platform as other systems. The Chairman requested that the IT Director come back to the Sub-Committee with further report on this issue.	Sean Green	May 2018	
	26 March 2018	Data Protection Policy The Chairman commented that the policy should be reviewed at Member level in order to ensure openness and transparency and a Member commented that the reviews should be fazed by section to ensure that the policy is considered closely.	Comptroller	March 2019	
	26 March 2018	Member Survey Report A report is submitted to the next meeting detailing the findings.	Chamberlain	May 2018	

This page is intentionally left blank

Forward Plan – Updated April 2018

Report Title	Report Month	Category	Who
Web Project Update	July 2018	Strategic	BR
Transformation Gateway Paper	July 2018	Strategic	KM
Information Management Recommendations	July 2018	Strategic	SG
CoLP National and Digital Programmes Update	July 2018	Strategic	KM
GDPR Compliance Update	September 2018	Operational	MC
Roadmap Plans Review	July 2018	Strategic	KM
Application Rationalisation Roadmap	September 2018	Strategic	KM
CRM Update and Presentation	September 2018	Strategic	SC
Phase II Transformation Financials	September 2018	Strategic	KM
Post 2020 Strategic IT Outsourcing Plan	September 2018	Strategic	KM
Web Project Update	September 2018	Strategic	BR
GDPR Compliance Update	September 2018	Operational	MC

This page is intentionally left blank

Committee(s)	Dated:
IT Sub-Committee – For Information	31st May 2018
Subject: IT Division – IT Director Summary	**Public**
Report of: The Chamberlain	**For Information**
Report author: Sean Green, IT Director	

Summary

The IT Division has maintained a focus on service availability whilst seeking to progress the transformation programme that will uplift the overall quality of IT services at the City of London Corporation (CoL) and City of London Police (CoLP).

- Key priorities for the IT Service in April and May are implementing the new Service Operating Model in City of London.
- Phase I Desktop transformation programme is now being closed. Network Transformation for CoL will be completed in July 18.
- Phase II IT Transformation proposals and roadmaps have been discussed with relevant Officer committees. These are being presented at the May meeting of the IT Sub-Committee for agreement.
- The IT Operating Model has completed the consultation phase with a final structure now issued. It is expected that the IT restructure will be implemented during June.
- Both organisations experienced external issues such as power failures which affected critical services.
- IT Service Desk User feedback in April remained above target, with 86% for City of London and 99% for City of London Police.
- GDPR changes are going to plan (there is a separate agenda item on this subject).

Recommendation(s)

Members are asked to:

- *Note the report.*

Main Report

1.0 IT Transformation Summary

Phase I IT Transformation

The Desktop rollout to the business is now complete with lessons learned documented with actions for the Phase II IT transformation programme. The IT Target Operating Model and Policy set are progressing well, and management actions are in place to limit any impact to the user community during transition.

Programme closure activities are now underway, including the completion of closure reports, supporting documentation, and data sets handed over.

Phase II IT Transformation CoL and CoLP

Separate agenda items set out the scope of Phase II for CoL and CoLP. The roadmap for both programmes has also been produced with the next steps including business cases being prepared for relevant Member committees to seek funding.

2.0 Service Experience

Both City of London and City of London Police experienced incidents in April – for time synchronisation in City of London Police, and internet access for City of London. The causes of these are understood, were remediated and are not expected to return.

P1 incidents

<u>There was one P1 incident in City of London Police</u>

- A Network Time synchronisation error caused Pronto (forms access to Niche the Crimes reporting and intelligence system) to be unavailable. This was caused by a local server hardware issue which was permanently fixed.

<u>There were 6 P1 incidents in City of London Corporation</u>

- A malware incident in London Councils affected multiple services
- iTrent (HR System) was unavailable when an archive log filled up
- The Library Management System was unavailable because of failure of an external VPN connection
- Internet access was unavailable on 2 occasions when a domain controller stopped authenticating with the Barracuda proxy device (two incidents)
- A power failure caused issues with network login, internet access and telephony

There was a serious malware incident in London Councils affecting all services. Agilisys was able to restore all services with no loss of data. Agilisys are currently in

discussions with London Councils to move to the existing local environment to IaaS as per the standard operating model for City of London. This will reduce the chances of this type of incident reoccurring and vastly improve resilience.

The Service Desk for City of London Police went live in April for 24 x 7 for **all** calls. Previously the CoLP 24 x 7 Service Desk was for Critical applications only. Although the number of calls outside of core hours is small the requirement to resolve these calls is very important. So far, all calls placed have been resolved.

Sean Green
IT Director, IT Division
T: 020 7332 3430
E: sean.green@cityoflondon.gov.uk

This page is intentionally left blank

Committee(s)	Dated:
IT Sub-Committee – For Information	31st May 2018
Subject: IT Division Risk Update	
Report of: The Chamberlain	**For Information**
Report author: Samantha Kay – IT Business Manager	

Summary

All IT Risks are now in the Risk Management System, with actions included, for the ongoing improvement and continuing assessment to the Management of Risk within the IT Division.

- All the IT risks are now being tracked in the corporate risk management system.
- The IT Division currently holds 11 risks, a decrease of one from the previous period. There are currently no RED risks.
- Three risks were mitigated due to actions being completed reducing the score to target level. All risks continue to be monitored and reviewed.
- There are no extreme impact risks, there are 7 major impact and 4 serious impact risks.
- No new risks were added to the IT Risk Register
- IT Division currently hold 2 risks on the Corporate Risk Register. The GDPR Corporate risk in owned by the Comptroller however the IT Division and leading on important mitigating actions for this risk.
- Periodic review meetings are being held with the relevant IT staff to ensure all risks are managed and reviewed in a timely manner.

Recommendation(s)

Members are asked to:

- Note the report.

Main Report

Background

1.0 Risk remains a key focus for the IT Division and we are continuing to ensure that it drives the priority for project works and Change Management decisions. Regular reviews will ensure the ongoing successful management of these risks across the division

Current Position

2.0 The IT Division Currently holds 2 risks on the Corporate Risk Register and feeds in to one other Corporate Risk.

The IT Division currently holds 11 risks, none of which are scored as Red.

All risks have owners, clear actions, with target dates to enable focussed management, tracking and regular and consistent reviews.

2.1 This period the IT Risk Register has seen the following activity:

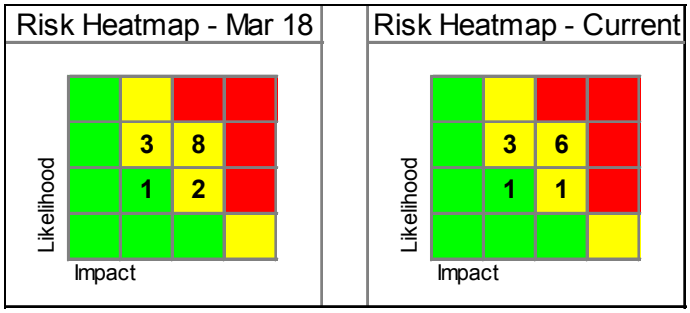
- 3 Risks Mitigated

The remaining risks are static, however they continue to be monitored alongside the relevant on-going projects in place to provide mitigation.

2.2 Three risks were deactivated due to actions being completed thus reducing the impact and likelihood of the risk:

- CHB IT 004 - Business Continuity / Disaster Recovery - planning and management - Score has reduced as Single Points of Failure have been removed through resilient design. Work is continuing to develop plans with the Corporate business continuity team to ensure all aspects are covered.
- CHB IT 015 - Change Control - The score has reduced as the policy has now been agreed with CoL and Agilisys. The policy has been communicated with the wider business.
- CHB IT 020 - PSN Compliance – PSN Certification has been granted. Procurement of bi-annual health checks is underway to ensure the CoL is not in a position of non-compliance going forward.

The current headline figures for the identified risks in the Division are:



2.3 Detailed below is a further breakdown of current IT Division risks:

		Trend
Extreme Impact:		
Risks with "likely" likelihood and "extreme" impact:	0	⟷
Risks with "unlikely" likelihood and "extreme" impact:	0	⟷
Risks with "rare" likelihood and "extreme" impact:	0	⟷
Major Impact:		
Risks with "likely" likelihood and "major" impact:	0	⟷
Risks with "possible" likelihood and "major" impact:	6	↓
Risks with "Unlikely" likelihood and "major" impact:	1	↓
Serious Impact:		
Risks with "likely" likelihood and "serious" impact:	0	⟷
Risks with "possible" likelihood and "serious" impact:	3	⟷
Risks with "unlikely" likelihood and "serious" impact:	1	⟷
Risks with "rare" likelihood and "serious" impact:	0	

Summary of the Corporate Risks

3.0 The summary below outlines the status of the current Corporate IT risks:

- CR 16 – Information Security - Breach of IT Systems resulting in unauthorised access to data by internal or external sources. This risk at a Red status at the IT Sub-Committee in March 2018 it was agreed that this risk should stay at Red whilst further mitigations are being delivered with an aim of bringing the risk down to green by reducing the likelihood of occurrence.
- CR 19 – IT Service Provision - Following the recent improvements to the corporate IT network and systems the risk has reduced to an amber 12. It is likely that over the coming months the risk will be further mitigated to a green rating.
- CR-25 – General Data Protection Regulation – The project is progressing with IT feeding in to the process where necessary and delivering specific IT actions. The GDPR project has made significant progress and it is anticipated that the Corporation will be compliant with GDPR requirements by May 25th 2018. This is covered by a separate agenda item.

Next Steps

4.0 The next steps are:

- Ensuring that IT deal with Risks in a dynamic manner.

- Ensuring all actions are up to date and allocated to the correct responsible owners.

- Ensuring all members of the IT division including suppliers are aware of how Risk is managed within the Corporation and have a mechanism to highlight areas of concern across the estate.

- IT management processes, including Change Management, Problem Management, Continuous Improvement and Incident Management will all now reference or identify risk to ensure that Division risks are identified, updated and assessed on an ongoing basis, so the Risk register remains a live system, rather than a periodically updated record.

Samantha Kay
IT Business Manager
E: Samantha.Kay@cityoflondon.gov.uk
T: 07817 411176

Committee(s)	Dated:
Information Technology Sub-committee	31/05/2018
Subject: General Data Protection Regulation (GDPR) update report	**Public**
Report of: Michael Cogher, Comptroller & City Solicitor	**For Information**
Report author: Michael Cogher, Comptroller & City Solicitor,	

Summary

This report summarises the new requirements of the General Data Protection Regulation (GDPR) which came into force on 25th May 2018 and progress of the GDPR project toward securing compliance with it. GDPR substantially updates data protection law, including changing conditions for processing, strengthening privacy and other rights and increasing penalties for breaches of the rules.

Recommendations

Members are asked to note the report.

Introduction

1. The current data protection regime is based on an EU Directive from 1995 and implemented in the UK by the Data Protection Act 1998. Since then there have obviously been significant advances in IT and fundamental changes to the ways in which organisations and individuals communicate and share information.

2. As a result, the EU has introduced updated and harmonised data protection regulations known as the General Data Protection Regulation ("GDPR") which came into force on 25 May 2018.

3. It will be implemented in the UK, notwithstanding Brexit, by legislation announced in the Queen's Speech.

4. This Report outlines the steps that the Corporation is taking to ensure that it is GDPR compliant.

Impact

5. The Information Commissioner's Office (ICO) which is responsible for guidance and enforcement of data protection has said:

"Many of the principles in the new legislation are much the same as those in the current Data Protection Act. If you are complying properly with the current law, then you have a strong starting point to build from. But there are some important new elements, and some things will need to be done differently".

6. GDPR introduces several new concepts and approaches. Equally many of the existing core concepts of personal data, data controllers and data processors are broadly similar. It remains founded on a principle-based approach.

7. The Corporation is reviewing organisational and technical processes both corporately and departmentally. The basic governance and technical systems required for GDPR compliance will be in place by 25th May. However, these will need to be bedded in, refined and reviewed on an on-going basis as GDPR becomes "business as usual".

GDPR Project Progress

8. The first phase of the Corporation's preparations for GDPR are at the time of writing close to completion and in summary have involved a review of the Corporation's information governance practices, policies and procedures; training and awareness raising; and ensuring the necessary technical IT and information security systems are GDPR compliant.

   These tasks are the subject of a detailed project plan overseen by the Information Board and IS Steering Group and delivered by the GDPR Project Team and departmental Access to Information Network Representatives (AIN) and management teams.

9. The Comptroller & City Solicitor was formally appointed by committee as the Corporation's Data Protection Officer in November 2017.

10. The GDPR implementation project plan covering all tasks required to effectively prepare for GDPR compliance was created in September 2017 and audited by Mazars with a positive outcome and with no minor or major risks to project delivery identified. A further audit was undertaken by Mazars in May 2018 to assess the Corporations readiness and levels of compliance with GDPR requirements the outcome of which will be fed into phase two of the GDPR project.

11. A phase two GDPR project running from 25 May 2018 to 31 December 2018 has been created and resourced the aim being to further embed and refine GDPR knowledge and compliance across the Corporation.

12. Information governance

    - GDPR Corporate Risk CR 25 was created and agreed by Audit & Risk Committee.
    - GDPR compliance requirements and project plan reported to Policy & Resources, Establishment Committees and IT sub-committee.
    - Project delivery is controlled at bi-weekly Project Team stage control meetings which monitor progress, capture GDPR issues and risks, assess required changes and associated corrective action and allocate work packages. The Project Team reports to the Information Board and IS Steering Group, additionally update reports and revised policies are

reported to Policy & Resources and Establishment Committees and to IT sub-committee.
- Regular liaison with IT workstreams are taking place which are reported to the GDPR Project Team for action and to the Information Board.

13. Training and Communication

- Six half day training sessions for AIN representatives and key staff delivered by the Comptroller & City Solicitor and Senior Information Compliance Officer all AIN representatives have undertaken the initial training. Further focused training has been provided to the HR Department, Remembrancer's Events Team and EDO.
- Five training sessions for Members have been delivered, and member guidance substantially revised to incorporate GDPR requirements, template forms issued including RoPA, Privacy notices
- GDPR detailed guidance notes issues to AIN representatives.
- Further training sessions are planned on GDPR specifics such as privacy impact assessments, ROPA, fair processing notices, breach notifications etc. post May 25th to refine and embed policies and procedures
- Chief Officer updates are provided at COG, senior managers nominated as leads in each department, senior manager training sessions scheduled
- A mandatory GDPR e-leaning training package was launched on City Learning on 23 April 2018 compliance levels are being monitored by the Data Protection Officer and reported to Chief Officers, the deadline for staff to undertake the training is 24 May 2018, also available to members
- GDPR corporate communications plan was agreed with the Communications Team and launched on 8 May 2018
- A dedicated GDPR intranet page has been updated to include guidance, news, policies, procedures, the relevant forms and FAQ's
- Detailed guidance tailored to departments has been delivered and will continue as department specific GDPR issues and risks arise

14. Policies:

- GDPR related policies have been revised to incorporate GDPR requirements including Employee Data Protection Policy, Data Protection Policy, Subject Access Rights Policy, Pupil and Parent Data Protection Policy, Data Breach Policy, Appropriate use of IT Policy, Storage of Data Policy, Email use policy, System Vulnerability Scanning Policy, Security Patching Policy and Procedure.
-

15. Procedures:

- GDPR requires a record of processing activities (ROPA), a proforma was issued to departmental AIN representatives, the returns have been

analysed by the Information Compliance Team who and included in a central record which will include the reasons for collection and retention.

- Subject Access Request procedures have been revised
- Standard contract clauses and data processing agreements have been updated and circulated to departments for issue to all existing contractors and existing agreements
- Privacy Impact Assessment template is currently being tested on the CRM project
- Communicating Privacy Information requirements included in the ROPA returns from which the procedure will be developed
- Privacy Notices have been revised and agreed, layered privacy notices are now on the CoL website incorporating all required generic elements under which sit layers of function specific information
- Data Breach procedures and template form revised
- Legal basis for employee personal data has been reviewed and revised
- Lawful basis for processing personal data procedures reviewed and revised
- Privacy Impact Assessment (PIA) procedure revised

16. Information Technology Systems:

- Major service providers have been sent Data Protection Schedules to ensure they agree to new responsibilities
- Agile Solutions and Agilisys to provide proof of concepts during May for a software solution to identify and resolve high risk to storage and processing of personal data and identify where a retention schedule is required
- IT systems capability to support Privacy Impact Assessments (PIA) are being developed; PIA form to be finalised and created as an on-line document
- Information retention schedules and the right to be forgotten are being developed
- Applications Development and Support will start to test major applications that process personal data against the right to erasure
- On line internal Data Breach Notification form is being developed
- Drive rationalisation and security guidelines to be implemented

Validation of Approach & Implementation

17. Because of the risks presented by GDPR a second review of the Corporation's approach and delivery of policies and procedures to meet the requirements was undertaken by its internal auditors, Mazars, in May 2018, their findings will be reported to Summit and committees as appropriate.

Conclusion

18. GDPR places significant obligations on the Corporation in relation to the processing of personal data to protect the rights and freedoms of everyone.

    The GDPR project has made significant progress, subject to the findings of the Mazars audit it is anticipated that the Corporation has achieved baseline compliance with GDPR requirements, further work will be required to embed, reinforce and enforce compliance with GDPR requirements across departments.

Appendices

None

Michael Cogher
Comptroller & City Solicitor
0207 332 3699
michael.cogher@cityoflondon.gov.uk

This page is intentionally left blank

Committee(s)	Dated:
IT Sub-Committee	31st May 2018
Subject: Change and Engagement Approach	**Public**
Report of: The Chamberlain	**For Information**
Report author: Sam Collins, Head of Change and Engagement	

Summary

The scope of Phase 1 the IT Transformation Programme is well documented. Phase 2 focuses on realising the benefits of the Programme through supporting user adoption to make best use of the technology that has been delivered. This report outlines a structured approach to gaining user adoption using the Government Digital Service approach. Initial information demonstrates that technology adoption has been positive so far but is expected to improve in the coming months.

Recommendation(s)

Member are asked to:

- *Note the report.*

Main Report

1.0 Background

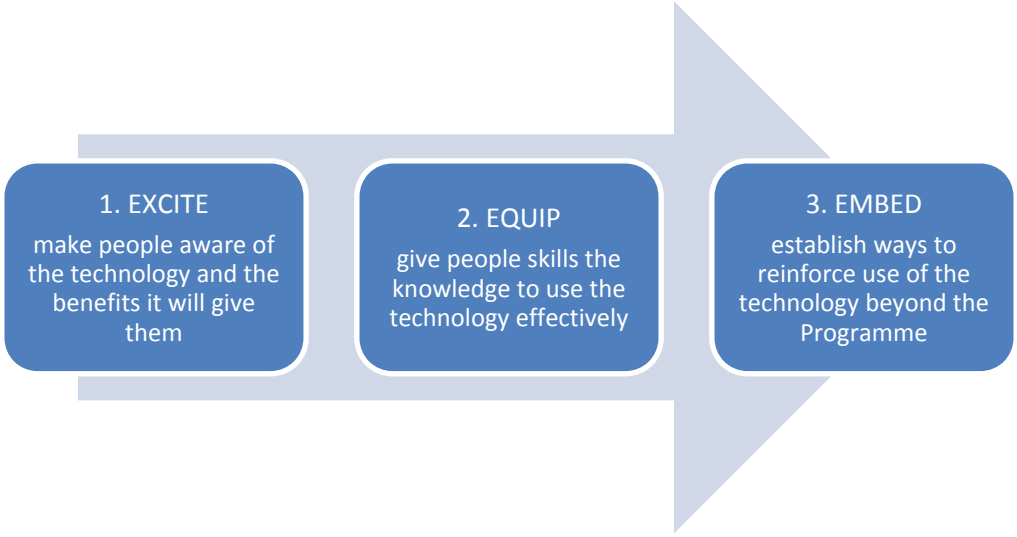
The City of London Corporation (CoL) has embarked on a major IT Transformation Programme over the last 18 months to refresh its end-to-end Technology Stack. The Vision and Strategy set out at the start of the Programme and approved at the IT Sub Committee was:

- Buy not Build
- Use fewer systems more effectively
- Secure and compliant IT systems and services that support the organisation
- Move from complexity to standardised solutions

Phase Two of the Transformation Programme acknowledges that in CoL most of the big infrastructure investments are now done. The key now is to maximise returns on investment, through supporting staff to utilise the capabilities of the new technology.

2.0 Change and Engagement Approach

Without a focussed effort, departments will continue to use the new technology in old ways. Appropriate Change Management, Training and Engagement activity is vital to ensure that CoL Staff understand 'the art of the possible' and are encouraged and supported to use and maximise benefits from the new technology. It is proposed that the Government Digital Service, three-phased approach is used (See Appendix A 'Change and Engagement Approach' for more details);



2.1 Activities to date include;

- A series of 'Familiarisation Sessions' delivered to over 600 staff through programme offering an overview of the rollout process and features of the new technology;
- Classroom based 'Technology Taster' sessions for staff, outlining the technology enhancements and new software – 100 staff should have attended these sessions by the end of May 2018;
- A presence at the City Learning Live event in early May, including 'theatre style' Technology Taster sessions;
- Sessions outside the Gild with a live 'Skype for Business' demonstration;

- Skype for Business demonstrations to several departmental management teams including Human Resources, Open Spaces and City Bridge Trust.

- Regular Communications through the Staff Intranet site and e-mails to Senior Officers.

- The procurement of an Online Training Offer (Training Plus) which will provide module-based on demand Office 365 training for all licensed users.

- Bite size 365 adoption for all Chief Officers SMT meetings and their Direct Reports SMT meetings.

3.0 Measuring Adoption

Feedback on the IT Transformation Programme has been very positive. The most significant change for the organisation has been the move to 70% of staff using laptops and tablets as their main Corporate device, which has been supported by a more agile infrastructure and 'cloud' offering.

Success will be measured qualitatively through the feedback received and a quarterly survey which will launch shortly, entitled 'Have you been Transformed?'. This will seek to understand whether working styles, productivity or processes have improved since the rollout.

To measure the adoption of the technology quantitively, we are using the 'User Adoption Dashboard', delivered through Power BI (the business intelligence software provided through Office 365). This provides detailed metrics including number of active users, the use of Skype and SharePoint, as well as a breakdown by department.

Some of the highlights so far include;

- 3,027 active users in Office 365;
- 93 active SharePoint sites, up from 57 in January 2018;
- 1002 staff members took part in a 1 to 1 Skype call in April;
- Around 250 regularly taking part in Skype calls of more than two people;
- Average 131 hours of video and audio calls over the last 3 months.

4.0 Future Plans for the Next 12 months

During the next 12 months the Change and Engagement team will continue an intensive campaign of communication, outreach and training with colleagues across the Corporation.

Specialist projects are being set up with business teams in Markets and Consumer Protection and Open Spaces to help them adopt new ways of working with mobile solutions and maximise the collaborate opportunities for the Office 365 software.

In addition, the City of London Corporation has been adopted by Microsoft as a Strategic Engagement partner which allows the organisation to have access to specialist support from Microsoft for resolving integration issues and run workshops led by Microsoft specialists to fastrack the development of knowledge and skills within the IT team.

More details are available regarding specific activities to promote new collaborative and information led ways of working in Appendix A.

Sam Collins
Head of Change and Engagement (Interim), IT Division
T: 020 7332 1504
E: sam.collins@cityoflondon.gov.uk

Appendix A – Change and Engagement Approach (Available on request)

Committee(s)	Dated:
PRED IT Sub Committee	29/05/2018 31/05/2018
Subject: Design, build, support and hosting for new website	**Public**
Report of: Town Clerk (Director of Communications)	**For Information**
Report author: Melissa Richardson, Digital Publishing and Content Strategy Lead, Communications, Town Clerks	

Summary

The purpose of this report is to keep Members updated on the progress of the website project. We now have the business requirements (attached as Appendix A) which have been produced by an independent digital consultant.

The business requirements will be supplied as part of the tender process. and be submitted alongside a standard Procurement specification.

The project has been approved at Gateway 3/4 by Projects Sub Committee and has been included in the Chamberlain's consolidated Project Funding Update report to Resource Allocation Sub Committee and, also, approved at Policy and Resources committee, both on 3 May 2018.

We would welcome any comments on the business requirements document at this stage.

Main Report

Background

The current website was launched in 2012 and, inevitably, is showing its age and no longer reflects well on the City of London Corporation.

All support for SharePoint 2010 [the current website platform] will cease in October 2020 (regular support stopped in 2015). SharePoint will not be providing a platform for external sites in future, so it cannot simply be updated. Leaving our website an unsupported platform poses a major risk.

Our current website does not display well on mobile devices, is not task structured (ie lacking user focus) and the out of the box search engine cannot provide the results from across the full range of corporate information (ie Member, Jobs and Media sites are separate) that users would expect.

Because of the above problems the Communications Team began examining the process of replacing the website in July 2017.

A supplier open day was held to test the market and gain feedback on likely costs and timescales for the project. This has provided the estimated figures included in this report.

Subsequently, the IT Category Board agreed the Procurement process and the project was agreed at Gateway 1/2 by Projects Sub Committee.

A digital consultant was employed to consult with Members and officers, gather the business requirements and to draft the invitation to tender.

On 20 February an Options paper was taken to the IT category board and approved.

The Gateway 3/4 paper went to Projects Sub on 14 March and was also approved.

The project has been included in the Chamberlain's consolidated Project Funding Update report to Resource Allocation Sub Committee and, also, approved at Policy and Resources committee, both on 3 May 2018.

It will go out to tender in the summer 2018 with Gateway 5 and IT Category Boards to follow in the autumn.

This will allow an early discovery phase (suppliers liaising in order to make informed recommendations about how to meet required outcomes), enabling work to start properly in early 2019.

Based on previous experience, this will allow a realistic amount of time for building, consultation and testing to ensure the new site is ready before summer 2020.

We hope

- To scope and procure services to deliver a new City of London Corporation website,
- To move to a cloud-based hosting and external support model
- To address known issues, eg Information Architecture (IA - how the site is built and structured), responsiveness (how it displays on mobile devices) and search functionality through the new website design

The initial one-off capital and supplementary revenue estimated cost of £513,000 be funded via a bid to the Policy and Resources Committee for allocations from the 2018/19 City Fund and City's Cash provisions for new schemes and from the general reserves of Bridge House Estates, broadly on a 50/45/5% basis respectively.

The Town Clerk's local risk budget be increased by £40,000 to meet the additional ongoing annual revenue costs, to be funded in the first year via a request for allocations from the Finance Committee contingencies of the three funds on a

50/45/5% basis, together with a base budget adjustment of £40,000 per annum for the following three financial years.

The project officer has liaised with City procurement and PT 3 (options) has been agreed. Procurement have recommended option 1 (detailed above), with the proposed route to market of competitive tender via the digital marketplace (G Cloud)

Conclusion

The business requirements will form an essential part of the tender process due to start in the Summer and Members comments on it at this stage would be welcome.

Melissa Richardson
Digital Publishing and Content Strategy Lead

T: 020 7332 3449
E: melissa.richardson@cityoflondon.gov.uk]

Appendix A - City of London Corporation, Creative Brief for website design and build V5, May 2018

This page is intentionally left blank

Document is Restricted

This page is intentionally left blank

Document is Restricted

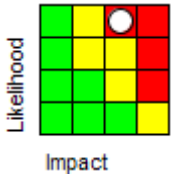
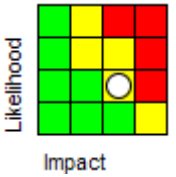
This page is intentionally left blank

APPENDIX 1: CR16 Information Security

CHB Detailed risk register by risk category

Report Author: Hayley Hajduczek

Generated on: 23 January 2018

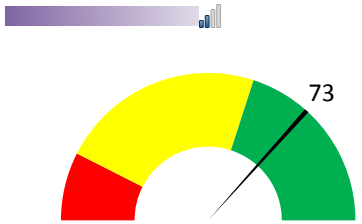
Risk no, title, creation date, owner	Risk Description (Cause, Event, Impact)	Current Risk Rating & Score		Risk Update and date of update	Target Risk Rating & Score		Target Date	Current Risk score change indicator
CR16 Information Security	**Cause**: Breach of IT Systems resulting in unauthorised access to data by internal or external sources. Officer/ Member mishandling of information. **Event**: Cybersecurity attack - unauthorised access to COL IT systems. Loss or mishandling of personal or commercial information. **Effect**: Failure of all or part of the IT Infrastructure, with associated business systems failures. Harm to individuals, a breach of legislation such as the Data Protection Act 1988. Incur a monetary penalty of up to £500,000. Compliance enforcement action. Corruption of data. Reputational damage to Corporation as effective body.		**16**	Work is continuing to complete the implementation of the action plan. Patching of equipment and decommissioning aged and vulnerable equipment has been completed. Following key tasks have now been completed: • Patching regime reviewed; • Vulnerability assessment completed;		**8**	30-Apr-2018	

22-Sep-2014 Peter Kane				• Incident management exercise; • Additional security awareness material purchased. **02 Jan 2018**				

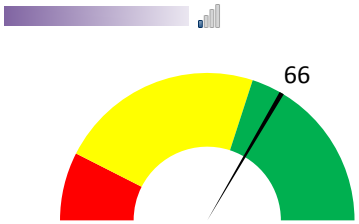
Action no, Action owner	Description	Latest Note	Managed By	Latest Note Date	Due Date
CR16b	For all major systems establish data owner and retention policy for information therein.	This is now being picked up with the GDPR ready project being led from the Comptroller team and IT team in the Corporation and the Information Management and Security team in the Police. Update reports on progress provided to Summit and IT Sub-Committee on a regular basis.	Sean Green	02-Jan-2018	30-Apr-2018
CR16h	Online training to be made available to Members following workshop in February 2016.	Induction training provided - Gary Brailsford-Hart is supporting this risk to execute mitigating actions from plan in place. Training for Officers and Members in 2018 now being developed. The campaign will be launched in June 2018 and a date will be set for members to receive a personal briefing from the CISO.	Gary Brailsford-Hart	04-05-2018	30-Apr-2018
CR16i	The Development and implementation of more technical security infrastructure	Using a recognised Cyber security maturity model there is a dashboard being reported that shows via a RAG status 10 areas of focus to mitigate this risk with training, processes and tools being delivered that in combination will bring the risk to Amber as planned and Green by July 2018.	Sean Green	02-Jan-2018	30-Apr-2018

10 Steps to Cyber Security: Dashboard

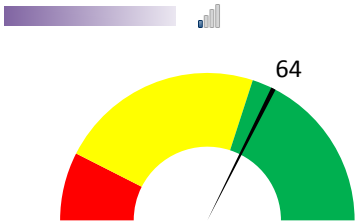
1. Information Risk Management



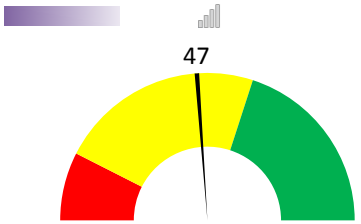
2. Network Security



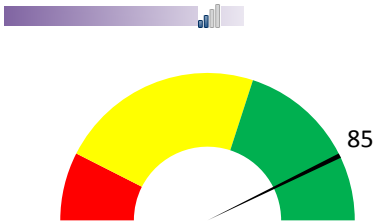
3. Malware Prevention



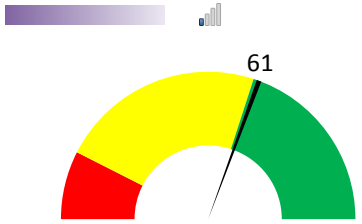
4. Monitoring



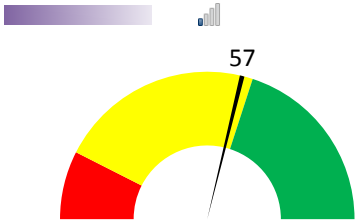
5. Incident Management



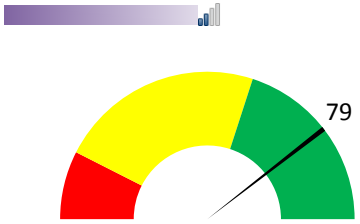
6. Managing User Privileges



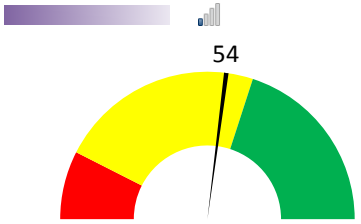
7. Removable Media Controls



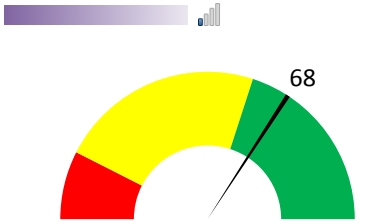
8. Secure Configuration



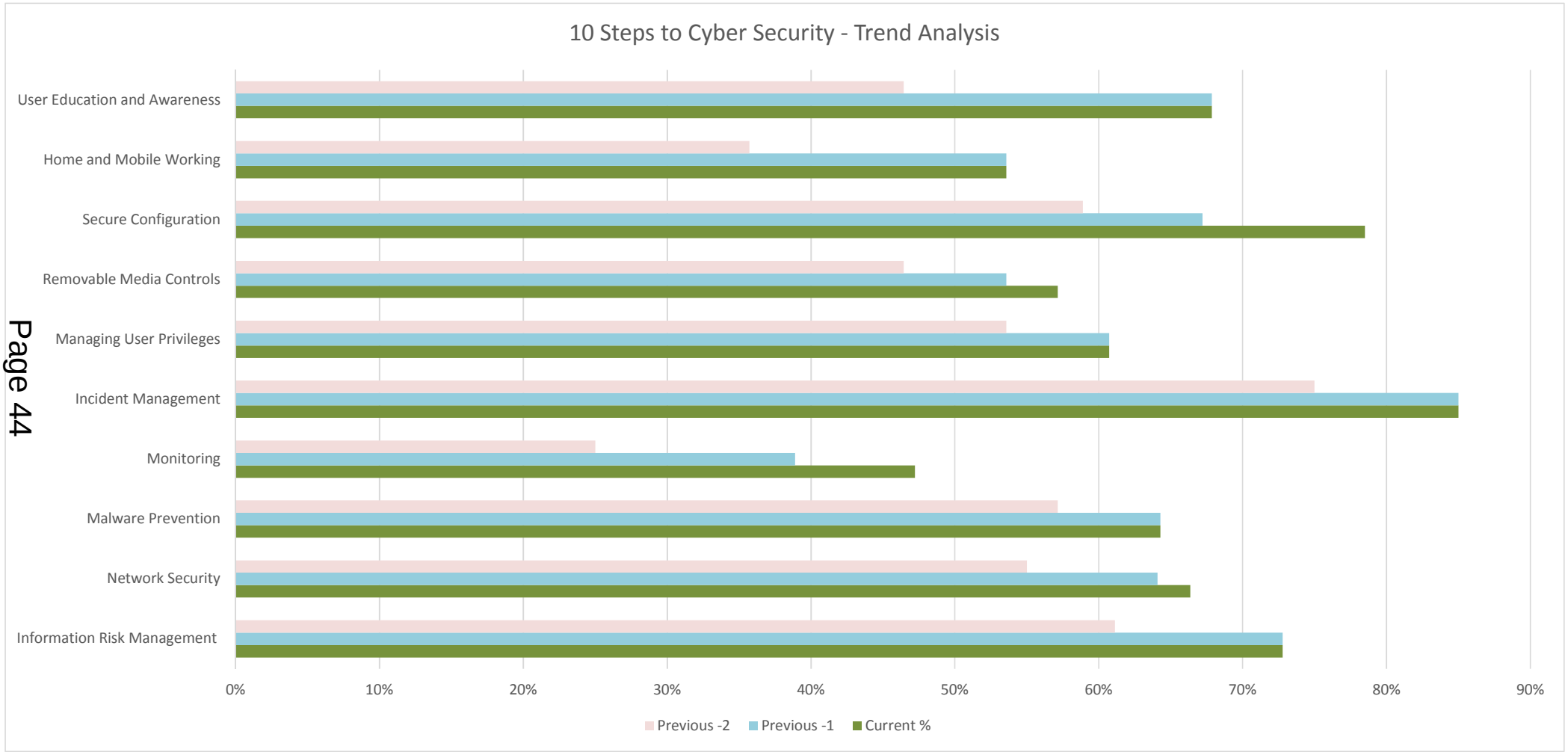
9. Home and Mobile Working



10. User Education and Awareness



City of London Corporation - Report of: Gary Brailsford-Hart, Director of Information & CISO - Assessment Date: 04 May 2018



PROTECT - MANAGEMENT

Information Risk Management	% Complete	Target Score	Actual Score
Establish a governance framework	100%	4	4
Determine the organisation's risk appetite	25%	4	2
Maintain the Board's engagement with information risk	100%	4	4
Produce supporting policies	100%	4	4
Adopt a lifecycle approach to information risk management	100%	4	4
Apply recognised standards	75%	4	3
Make use of endorsed assurance schemes	75%	4	3
Educate users and maintain their awareness	50%	4	2
Promote a risk management culture	30%	4	2

Network Security	% Complete	Target Score	Actual Score
Police the network perimeter	75%	4	3
Install firewalls	100%	4	4
Prevent malicious content	75%	4	3
Protect the internal network	80%	4	3
Segregate network as sets	25%	4	1
Secure wireless devices	100%	4	4
Protect internal IP addresses	25%	4	1
Enable secure administration	25%	4	2
Configure the exception handling process	100%	4	4
Monitor the network	25%	4	1
Assurance process	100%	4	4

Malware Prevention	% Complete	Target Score	Actual Score
Develop and implement anti-malware policies	50%	4	2
Manage all data import and export	75%	4	3
Blacklist malicious web sites	100%	4	4
Provide detailed media scanning machines	25%	4	1
Establish malware defences	75%	4	3
End user device protection	50%	4	2
User education and awareness	75%	4	3

Monitoring	47%	4	2
Establish a monitoring strategy and supporting policies	25%	4	1
Monitor all ICT systems	50%	4	2
Monitor network traffic	50%	4	2
Monitor all user activity	50%	4	2
Fine-tune monitoring systems	50%	4	2
Establish a centralised collection and analysis capability	50%	4	2
Provide resilient and synchronised timing	100%	4	4
Align the incident management policies	25%	4	1
Conduct a lessons learned review	25%	4	1

Incident Management	85%	4	3
Obtain senior management approval	100%	4	4
Provide specialist training	100%	4	4
Define the required roles and responsibilities	75%	4	3
Establish a data recovery capability	100%	4	4
Test the incident management plan	100%	4	4
Decide what information will be shared and with whom	25%	4	1
Collect and analyse post-incident evidence	75%	4	3
Conduct a lessons learned review	100%	4	4
Educate users and maintain their awareness	75%	4	3
Report criminal incidents to law enforcement	100%	4	4

Managing User Privileges	61%	4	2
Establish effective account management processes	100%	4	4
Establish policy and standards for user identification and access control	75%	4	3
Limit user privileges	75%	4	3
Limit the number and use of privileged accounts	50%	4	2
Monitor	50%	4	2
Limit access to the audit system and the system activity logs	25%	4	1
Educate users and maintain their awareness	50%	4	2

Removable Media Controls	57%	4	2
Produce corporate policies	50%	4	2
Limit the use of removable media	50%	4	2
Scan all media for malware	75%	4	3
Formally issue media to users	75%	4	3
Encrypt the information held on media	25%	4	1
Actively manage the reuse and disposal of removable media	50%	4	2
Educate users and maintain their awareness	75%	4	3

Secure Configuration	79%	4	3
Use supported software	80%	4	3
Develop and implement corporate policies to update and patch systems	100%	4	4
Create and maintain hardware and software inventories	80%	4	3
Manage your operating systems and software	75%	4	3
Conduct regular vulnerability scans	75%	4	3
Establish configuration control and management	75%	4	3
Disable unnecessary peripheral devices and removable media access	75%	4	3
Implement white-listing and execution control	100%	4	4
Limit user ability to change configuration	100%	4	4
Limit privileged user function	25%	4	1

Home and Mobile Working	54%	4	3
Asses the risks and create a mobile working security policy	50%	4	2
Educate users and maintain their awareness	50%	4	2
Apply the security baseline	75%	4	3
Protect data at rest	75%	4	3
Protect data in transit	75%	4	3
Review the corporate incident management plans	50%	4	2

User Education and Awareness	68%	4	3
Produce a user security policy	75%	4	3
Establish a staff induction process	50%	4	2
Maintain user awareness of the cyber risks faced by the organisation	75%	4	3
Support the formal assessment of Information Assurance (IA) skills	75%	4	3
Monitor the effectiveness of security training	50%	4	2
Promote an incident reporting culture	50%	4	2
Establish a formal disciplinary process	100%	4	4

Current status of 10 Step control areas across organisation.

ASSESSMENT DATE: 04 May 2018

Control Area	% Complete	Target Score	Actual Score
Information Risk Management	73%	4	3
Network Security	66%	4	3
Malware Prevention	64%	4	3
Monitoring	47%	4	2
Incident Management	85%	4	3
Managing User Privileges	61%	4	2
Removable Media Controls	57%	4	2
Secure Configuration	79%	4	3
Home and Mobile Working	54%	4	3
User Education and Awareness	68%	4	3

City of London Corporation - Report of: Gary Brailsford-Hart, Director of Information & CISO - Assessment Date: 04 May 2018

This page is intentionally left blank

Appendix 3: Statutory Requirements Summary

Data Protection Act 1998

http://www.legislation.gov.uk/ukpga/1998/29/contents

The Data Protection Act regulates the use of personal data by organisations. Personal data is defined as information relating to a living, identifiable individual.

The Act is underpinned by eight guiding principles:

1. Personal data shall be processed fairly and lawfully.

2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4. Personal data shall be accurate and, where necessary, kept up to date.

5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6. Personal data shall be processed in accordance with the rights of data subjects under this Act. [Data subjects have the right to gain access to their personal as held by the City Corporation]

7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

As a data controller, the City Corporation must also notify annually with the Information Commissioner's Office. The Information Commissioner has the power to issue fines of up to £500,000 for a breach of the Data Protection Act.

Freedom of Information Act 2000

http://www.legislation.gov.uk/ukpga/2000/36/contents

The Freedom of Information Act gives individuals a right of access to information held by the City Corporation, subject to a number of exemptions. Requests for information must be made in writing (email, letter or fax) but can be received by any member of staff at the City Corporation. Such requests must be responded to within 20 working days. The City Corporation has an internal appeal process if a requester is unhappy with a response to a request and the Information Commissioner regulates the Act.

Privacy and Electronic Communications Regulations 2003

http://www.legislation.gov.uk/uksi/2003/2426/contents/made

Section 11 of the Data Protection Act allows individuals to control the direct marketing information they receive from organisations. The Privacy and Electronic Communications Regulations specifically regulate the use of electronic communications (email, SMS text, cold calls) as a form of marketing and allow individuals to prevent further contact.

Regulation of Investigatory Powers Act (RIPA) 2000
http://www.legislation.gov.uk/ukpga/2000/23/contents
RIPA regulates the powers of public bodies to carry out surveillance and investigation and also deals with the interception of communications.

Copyright, Designs and Patents Act 1988
http://www.legislation.gov.uk/ukpga/1988/48/contents
The Copyright, Designs and Patents Act (CDPA) defines and regulates copyright law in the UK. CDPA categorises the different types of works that are protected by copyright, including:

- Literary, dramatic and musical works;
- Artistic works;
- Sound recordings and films;
- Broadcasts;
- Cable programmes;
- Published editions.

Computer Misuse Act 1990
http://www.legislation.gov.uk/ukpga/1990/18/contents
The Computer Misuse Act was introduced partly in reaction to a specific legal case (R v Gold and Schifreen) and was intended to deter criminals from using a computer to assist in the commission of a criminal offence or from impairing or hindering access to data stored in a computer. The Act contains three criminal offences for computer misuse:

- Unauthorised access to computer material;
- Unauthorised access with intent to commit or facilitate commission of further offences;
- Unauthorised modification of computer material.

Human Rights Act 1998
http://www.legislation.gov.uk/ukpga/1998/42/contents
The Human Rights Act puts the rights set out in the 1953 European Convention on Human Rights into UK law. Article 8, relating to privacy, is of most relevance to information security – it provides a right to respect for an individual's "private and family life, his home and his correspondence", a right that is also embedded within the Data Protection Act.

Equality Act 2010
http://www.legislation.gov.uk/ukpga/2010/15/contents
The Equality Act was introduced in October 2010 to replace a number of other pieces of legislation that dealt with equality, such as the Equal Pay Act, the Disability Discrimination Act and the Race Relations Act. The Equality Act implements the four major EU Equal Treatment Directives.

Terrorism Act 2006
http://www.legislation.gov.uk/ukpga/2000/11/contents
The Terrorism Act creates a number of offences in relation to terrorism. Section 19 of the Act imposes a duty on organisations to disclose information to the security forces where there is a belief or suspicion of a terrorist offence being committed. Failure to disclose relevant information can be an offence in itself.

Limitation Act 1980
http://www.legislation.gov.uk/ukpga/1980/58
The Limitation Act is a statute of limitations providing legal timescales within which action may be taken for breaches of the law – for example, six years is the period in which an individual has the

opportunity to bring an action for breach of contract. These statutory retention periods will inform parts of the City Corporation's records management policy.

Official Secrets Act 1989
http://www.legislation.gov.uk/ukpga/1989/6/contents
City Corporation members of staff may at times be required to sign an Official Secrets Act provision where their work relates to security, defence or international relations. Unauthorised disclosures are likely to result in criminal prosecution. Section 8 of the Act makes it a criminal offence for a government contractor (potentially the City Corporation) to retain information beyond their official need for it and obligates them to properly protect secret information from accidental disclosure.

Malicious Communications Act 1988
http://www.legislation.gov.uk/ukpga/1988/27/contents
The Malicious Communications Act makes it illegal to "send or deliver letters or other articles for the purposes of causing stress or anxiety". This also applies to electronic communications such as emails and messages via social networking websites.

Digital Economy Act 2010
http://www.legislation.gov.uk/ukpga/2010/24/contents
The Digital Economy Act regulates the use of digital media in the UK. It deals with issues such as online copyright infringement and the obligations that internet service providers (ISPs) have to tackle online copyright infringement.

Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011
http://www.legislation.gov.uk/uksi/2011/1208/contents/made
An amendment to the Privacy and Electronic Communications Regulations in 2011 obliged websites to inform users about their use of cookies and seek consent for setting more privacy intrusive cookies.

Police and Justice Act 2006
http://www.legislation.gov.uk/ukpga/2006/48/contents
Section 39 and Schedule 11 of the Police and Justice Act amend the Protection of Children Act 1978 to provide a mechanism to allow police to forfeit indecent photographs of children held by the police following a lawful seizure.

Counter-Terrorism and Security Act 2015
http://www.legislation.gov.uk/ukpga/2015/6/contents
Accessing websites or other material which promotes terrorism or violent extremism or which seeks to radicalise individuals to these causes will likely constitute an offence under the Counter-Terrorism and Security Act 2015.

General Data Protection Regulation (EU Data Protection Act) – May 2018

The incoming GDPR requires a firm grip on key areas where attacks are increasing. This is particularly true for organisations like local authorities, who routinely collect and share citizens' sensitive data with other organisations (both public and private) to operate effectively. Central Government recently confirmed in its Cyber Security Regulation and Incentives Review that it will also seek to improve cyber risk management through the implementation of the GDPR.

This page is intentionally left blank

Committee(s)	Dated:
IT Sub Committee	**May 2018**
Subject: CR 16 Information Security Risk	**Non-Public**
Report of: Chamberlain	**For Information**
Report author: Gary Brailsford-Hart ,Director of Information & Chief Information Security Officer	

NOT FOR PUBLICATION

By virtue of paragraph 3A of Part I of Schedule 12A of the Local Government Act 1972

Summary

The generally accepted definition of a data breach is a security incident in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen or used by an individual authorized to do so.

CR16 was developed as means to capture and mitigate the risks a 'cyber breach' would present to the City Corporation. It is evident that dependent on the nature of the breach the impact can vary from very low to critical. Cyber threat is often viewed as a complex, dynamic and highly technical risk area. However, what is often at the root of a breach is a failure to get the basics right, systems not being patched, personnel not maintaining physical security, suppliers given too much information.

The National Cyber Security Centre (NCSC) 10 Steps to Cyber Security framework has been adopted to strengthen the controls in this risk area; this framework is now used by the majority of the FTSE350. The control scores are currently low and are reflective of the early phase of adoption across the City Corporation, the risk areas are actively monitored and risk managed. Scores will increase as improvements to people, process and technology are delivered throughout the year. We have a risk management plan which at the end of April 2018 we reviewed and assessed that due to the delivery of appropriate controls the organisation had achieved an acceptable level of assurance against the risk.

Recommendation(s)

Members are asked to:

- Note the report.

Main Report

Background

1. Cyberspace has revolutionised how many of us live and work. The internet, with its more than 3 billion users, is powering economic growth, increasing collaboration and innovation, and creating jobs.

2. Protecting key information assets is of critical importance to the sustainability and competitiveness of businesses today. The City Corporation needs to be on the front foot in terms of our cyber preparedness. Cyber security is all too often thought of as an IT issue, rather than the strategic risk management issue it actually is.

3. Corporate decision making is improved through the high visibility of risk exposure, both for individual activities and major projects, across the whole of the City Corporation.

4. Providing financial benefit to the organisation through the reduction of losses and improved “value for money” potential.

5. The City Corporation is prepared for most eventualities, being assured of adequate contingency plans. We have therefore adopted the NCSC Ten Steps to Cyber Security framework to assist and support our existing strategic-level risk discussions, specifically how to ensure we have the right safeguards and culture in place.

6. The creation of CR16 demonstrates the City Corporations commitment to the identification and management of this risk area.

Current Position

7. The development and implementation of an Information Security Management System (ISMS) was seen as an essential requirement to permit the measurement and assurance of the CR16 risk. A number of frameworks were considered, and the NCSC Ten Steps to Cyber Security framework, supported by the NCSC 20 Critical Security Controls, was chosen as the most appropriate for the City Corporation.

8. To provide an overview of CR16 risk management the current compliance with the HMG Ten Steps assurance programme is detailed below (table 1) under each of the ten steps areas. The control scores are improving and are embedding across the City Corporation, the risk areas are actively monitored and risk managed. Scores will continue to increase as improvements to people, process and technology are delivered as part of the continuous improvement process. We have delivered and assessed the mitigation controls in April 2018 and believe that we have achieved an acceptable level of assurance. Furthermore, the risk management framework will reflect the controls as they mature within the organisation.

Table 1 - HMG Ten Steps assurance for the City Corporation as at May 2018

Ten Steps - **Control Area**	% Complete	Target Score	Actual Score	Trend
1. Information Risk Management	73%	4	3	↔
2. Network Security	66%	4	3	↑
3. Malware Prevention	64%	4	3	↔
4. Monitoring	47%	4	2	↑
5. Incident Management	85%	4	3	↔
6. Managing User Privileges	61%	4	2	↔
7. Removable Media Controls	57%	4	2	↑
8. Secure Configuration	79%	4	3	↑
9. Home and Mobile Working	54%	4	3	↔
10. User Education and Awareness	68%	4	3	↔

Options

9. Endorsement and support for the management and delivery of CR16 risk management plan has been obtained directly from chief officers as well as strategically via papers to Summit Group, IT Sub and Finance Committees.

Proposals

10. Continue to implement the 10 steps programme across the City Corporation.

Implications

11. Failure to demonstrate appropriate controls in this risk area will expose the City Corporation to unacceptable levels of risk and could hinder a number of strategic objectives.

12. There are also a number of statutory requirements to consider for the management of this risk area, these are summarised at Appendix 3.

Health Implications

13. There are no health risks to consider as part of this report.

Conclusion

14. There is an extensive programme of work underway to mitigate the risks identified within CR16. This report articulates the work in progress and clearly identifies where we will be directing continuing effort to manage this risk to an

initial acceptable level and then monitoring as the controls mature across the organisation.

15. The breadth and scope of the necessary controls are cross-organisational and should not be entirely seen as a technical issue to be solved by the IT department. For example if users leave the door open and their computers logged on then technical controls cannot in themselves defend the organisation.

16. The realisation of this risk would certainly have a severe impact on technical systems and directly impact the operational effectiveness of potentially the entire City Corporation. It is therefore imperative that the underlying issue of developing a security culture is supported through the delivery of risk controls for CR16. There is positive support for this work across the organisation and senior management understand and are supportive of the necessary changes to ensure the City Corporation's security.

17. It is important to note that whilst we are improving the CR16 risk position, it will only remain so with the continued operation and maintenance of the controls being put in place to manage it and should not therefore be considered a one-off exercise.

Appendices

Detailed Appendices available on request:

- Appendix 1 – CR16 Information Security
- Appendix 2 – 10 Steps to Cyber Security Dashboard & Breakdown
- Appendix 3 – Statutory Requirements Summary

Gary Brailsford-Hart
Director of information & Chief Information Security Officer

T: 020 7601 2352
E: gary.brailsford@cityoflondon.police.uk

Document is Restricted

This page is intentionally left blank

Document is Restricted

This page is intentionally left blank

Document is Restricted

This page is intentionally left blank

Document is Restricted

This page is intentionally left blank

Document is Restricted

This page is intentionally left blank

Document is Restricted

This page is intentionally left blank

Document is Restricted

This page is intentionally left blank

Document is Restricted

This page is intentionally left blank

Document is Restricted

This page is intentionally left blank

Document is Restricted

This page is intentionally left blank

Document is Restricted

This page is intentionally left blank