Public Document Pack

Digital Services Sub (Finance) Committee

Date: **MONDAY, 4 FEBRUARY 2019**

Time: **11.00 am**

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
Sylvia Moys
Alderman Sir Andrew Parmley
James Tumbridge
Rehana Ameer
Hugh Morris

Enquiries: **Rofikul Islam**
Rofikul.Islam@cityoflondon.gov.uk

Lunch will be served in the Guildhall Club at 1pm
N.B. Part of this meeting could be the subject of audio or video recording

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 of the meeting held on 2 November 2018.

   For Decision
   (Pages 1 - 10)

4. **OUTSTANDING ACTIONS FROM PREVIOUS MEETINGS**
   Joint report of the Town Clerk and Chamberlain.

   For Information
   (Pages 11 - 12)

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

   For Information
   (Pages 13 - 14)

6. **CHAMBERLAIN'S DEPARTMENT DIGITAL ADOPTION**
   Presentation

   For Information

7. **DIGITAL STRATEGIC FRAMEWORK**
   Presentation

   For Information

8. **CASE FOR A DIGITAL STRATEGIC FRAMEWORK**
   Joint Report of the Town Clerk and the Chamberlain

   For Decision
   (Pages 15 - 20)

9. **GENERAL DATA PROTECTION REGULATION (GDPR/DATA PROTECTION ACT 2018 (DPA))**
   Report of the Comptroller & City Solicitor

   For Decision
   (Pages 21 - 30)

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

For Decision
(Pages 31 - 48)

11. **IT DIVISION - IT SERVICE DELIVERY SUMMARY**
Report of the Chamberlain

For Information
(Pages 49 - 54)

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

For Information
(Pages 55 - 58)

13. **UPDATE ON NEW WEBSITE**
Report of the Director of Communications

For Information
(Pages 59 - 60)

14. **MICROSOFT LICENSING AND CLOUD PRODUCTIVITY SUITE (OFFICE 365)**
Report of the Chamberlain.

For Information
(Pages 61 - 72)

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

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

17. **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

18. **NON-PUBLIC MINUTES OF THE PREVIOUS MEETING**
To agree the non-public minutes of the meeting held on 2 November 2018.

For Decision
(Pages 73 - 78)

19. **INFORMATION & CYBER SECURITY STRATEGY - SECURITY SPEND FORECAST**
Report of the Chamberlain

For Information
(Pages 79 - 100)

20. **COLP IT MODERNISATION - MANAGED DESKTOP & O365**
Joint Report of the Chamberlain and the Commissioner of the City of London Police

For Information
(Pages 101 - 112)

21. **SMART WORKING UPDATE**
Report of the Chamberlain

For Information
(Pages 113 - 116)

22. **2020 SOURCING PROJECT - POSITION STATEMENT**
Report of the Chamberlain

For Decision
(Pages 117 - 122)

23. **HOUSING MANAGEMENT SYSTEM UPGRADE**
Report of the Director of Community and Children's Services.

For Information
(Pages 123 - 134)

24. **CONTRACT VARIATION: MIDLAND ITRENT HR AND PAYROLL SYSTEM EXTENSION**
Report of the Chamberlain

For Decision
(Pages 135 - 142)

25. **POLICING PROGRAMMES - UPDATE REPORT**
Joint report of the Chamberlain and City of London Police

For Information
(Pages 143 - 148)

26. **COLP IT MODERNISATION - SECURITY ZONE**
Joint Report of the Chamberlain and the Commissioner of the City of London Police

For Information
(Pages 149 - 156)

27. **COL IT TRANSFORMATION PHASE II IT SERVICE 2020 CONTRACT**
Joint report by Chamberlain and the Commissioner of City of London Police

For Information
(Pages 157 - 166)

28. **MARKETS STOCK CONTROL SOFTWARE**
Report of the Chamberlain

For Information
(Pages 167 - 168)

29. **SYNECTICS COMPLAINT WAIVER**
Report of the Chamberlain

To Follow

For Decision

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

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

This page is intentionally left blank

INFORMATION TECHNOLOGY SUB (FINANCE) COMMITTEE

Friday, 2 November 2018

Minutes of the meeting of the Information Technology Sub (Finance) Committee held at Guildhall, EC2 on Friday, 2 November 2018 at 1.45 pm

Present

Members:
Deputy Jamie Ingham Clark (Chairman)
Randall Anderson (Deputy Chairman)
Deputy Keith Bottomley
John Chapman
Jeremy Mayhew
Sylvia Moys

Officers:

John Cater	-	Town Clerk's Department
Richard Holt	-	Town Clerk's Department
Bob Roberts	-	Director of Communications
Melissa Richardson	-	Town Clerk's Department
Peter Kane	-	Chamberlain
Kevin Mulcahy	-	Chamberlain's Department
Sean Green	-	Chamberlain's Department
Sam Collins	-	Chamberlain's Department
Mohamed Hussain	-	Chamberlain's Department
Michael Cogher	-	Comptroller and City Solicitor
Gary Brailsford-Hart	-	City of London Police
Andrew Bishop	-	City of London Police

In attendance:
Eugene O'Driscoll — Agilisys

1. **APOLOGIES**
   Apologies were received from Tim Levene, Alderman Sir Andrew Parmley 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**

The IT Sub-Committee considered the public minutes of the meeting held on 10 July 2018.

Matters arising from the Minutes

A Member asked for feedback on the use of the Piranha mobile stock control application at Billingsgate Market. The IT Director responded that discussions had been taking place on the cost effectiveness of the Piranha App and whether the App's implementation at other markets would be appropriate. It was agreed that a report be presented to the next meeting of the IT Sub-Committee to provide Members with an update on the Piranha Application.

Replying to a Members comment on GDPR and CRM, the Chairman explained that it would be more suitable for these discussions to take place at the relevant items later in the agenda.

RESOLVED: That the public minutes of the meeting held on 10 July 2018 be approved as an accurate record.

4. **OUTSTANDING ACTIONS FROM PREVIOUS MEETINGS**

The IT Sub-Committee considered a joint report of the Town Clerk and the Chamberlain which provided updates of outstanding actions from previous meetings. The report also provided information of the IT Sub-Committee's proposed work plan for forthcoming meetings.

RESOLVED: That the Outstanding Actions report be noted.

5. **WORK PROGRAMME FOR FUTURE MEETINGS**

The IT Sub-Committee received a report of the Town Clerk and the Chamberlain detailing those reports that were scheduled to be submitted to The IT Sub-Committee through to May 2019. The Chairman commented that the report displayed the considerable work which the IT Sub-Committee oversaw.

RESOLVED: That the Work Programme be noted.

6. **CUSTOMER RELATIONSHIP MANAGEMENT PROJECT UPDATE**

The IT Sub-Committee received a report of the Chamberlain on the approach for managing personal information across both City Dynamics and City Services. It was noted that the report was produced to answer Members queries at the last meeting of the Information Technology Sub-Committee.

RESOLVED: That the Customer Relationship Management Project Update be noted.

7. **CHANGE AND ENGAGEMENT ADOPTION PLAN**

The IT Sub-Committee received a report of the Chamberlain regarding an update on the Change and Engagement Adoption plan. The report informed Members that since the IT transformation Programme completed in February 2018 there had been a steady increase in the adoption of new Office 365 technologies. The report also noted that the IT Division continued to encourage

further adoption including through the 'Collaborate' campaign and this would continue with the rollout of Microsoft Teams. The Head of Change and Engagement noted that there was an error in paragraph 2 and the 'h' should read 'has'.

The Chairman highlighted that the use of the Skype application was particularly useful for offsite working. A Member asked the IT team how best Members should organise the IT training and queried whether a more formal programme of training was due to be implemented. The Director of IT clarified that Member training was planned to take place on a one to one basis on request by Members.

In addition, the Chairman highlighted the issue that City of London Corporation Licensing department wasn't fully engaging with the SharePoint system and asked for the department to be made aware of its facilities. A Member noted that for some members of City of London Corporation staff the use of applications such as Skype was not always practical due to working pattern.

Resolved: That the Change and Engagement Adoption plan be noted.

8. **APPLICATIONS STRATEGY**

The IT Sub-Committee considered a report of the Chamberlain on the Applications Management Strategy proposed by the IT Division for the City of London Corporation ('CoL') and the City of London Police ('CoLP'). Officers explained that the Strategy had previously been agreed by the Police Projects board. The report advised that the proposed strategy aimed to maximise the value-for money that the CoL and CoLP obtain from their joint applications estate through ownership formalisation, estate consolidation and product optimisation. The Assistant IT director explained that the Applications Strategy had been agreed by Police Projects board and was presented to the IT Sub-Committee for Members views.

A Member queried if the endorsement of the Application Strategy would have any significant financial implications. The Assistant IT director explained that the Application Strategy was not expected to involve significant spending and was designed to limit wastage.

RESOLVED: - That –

I. The IT Sub-Committee agreed to endorse adoption of the Applications Management Strategy by CoL and CoLP as the overarching guide to the ongoing ownership, operation and enhancement of their joint applications estate; and
II. That authority be delegated to the IT Director to enable the implementation of the strategy in conjunction with senior officers and the heads of business units.

9. **END USER DEVICE REFRESH PROJECT**

The IT Sub-Committee considered an Outcome Report of the Chamberlain on the End User Device Refresh project. The Chairman highlighted the success of the project and thanked officers for achievements listed in the report. A Member

noted the importance of laptops remaining at a low weight was key to mobile working continued practicality.

RESOLVED: -That-

I. that The IT Sub-Committee noted the lessons learnt; and
II. endorsed that the underspend from the hardware budget is used to refresh further aged devices; and
III. endorsed that following the purchase of the additional hardware, the closure of the project is agreed.

10. **UNIFIED COMMUNICATIONS GATEWAY**

The IT Sub-Committee considered a Gateway 2 report of the Chamberlain related to the Unified Communications Programme. The Chamberlain explained that the £50,000 spent outlined in the report was subject to consideration at the Resource Allocation Sub-Committee.

A Member commented that the estimated cost quoted in the report was an unhelpfully wide range and queried if a more accurate range could be provided. The Chairman confirmed that the correct estimate was closer to £800,000-£1,200,000. The Member queried if the £1,200,000 was within a budgeting structure. The Chamberlain confirmed that the spending was viewed as an investment which would save money in the long term and the funds had been 'earmarked' within the Medium Financial Plan.

It was noted by Members that there was no GDPR assessment included in the report and queried if this was problematic, highlighting the potential for telephone conversations to be recorded. The Comptroller explained that specific GDPR assessments were only completed on high risk projects as directed by the ICO and that as telephone recordings were not a key element of the programme it was not considered a high-risk project. The Comptroller explained that a DDIA could be completed if deemed necessary.

RESOLVED: -That-

i) that the IT Sub-Committee approved the proposal set out in the Gateway report to initiate the Unified Communications Programme.
ii) an impact assessment will be considered for the programme at design stage.

11. **IT SERVICE REPORT (INCLUDE MANAGING CACHED EMAIL ADDRESSES)**

The IT Sub-Committee received a report of the Chamberlain on the IT Division's IT Service Delivery Summary. The IT director explained that IT Service performance had been good for both the City of London Corporation and City of London Police, but that the IT division was committed to continuing high level of service. Furthermore, the IT Director explained that work had been undertaken to remove private Members' cached email addresses from Outlook but that this had proven to be problematic and that continuing communication to officers on the issue of using non-City of London Corporation email addresses was the most effective approach.

A Member queried whether the root cause of the P1 incidents had been properly identified. In reply to this query the IT director said that the Major Incidents Review's identified the root cause in each of the P1 incidents. Replying to a question regarding the IT service delivery at London Councils, the IT Director informed Members that this was due to aged infrastructure of London Councils and that a transformation programme was now in place.

RESOLVED: that the IT Service Delivery Summary be noted.

12. **IT DIVISION RISK UPDATE**

The IT Sub-Committee received a report of the Chamberlain providing an update on the IT Division Risk. The report provided a summary of the IT department's risks including the status of current risks, progress made against previous risks and the new risks which had been identified. The Chairman noted the quality of the report and the work that had been done to refine the report on IT Division Risk. In addition, the Chairman explained that the issues of GDPR and CR16 would be taken under items 14 and 27 respectively.

Resolved: That the IT Division Risk update be noted.

13. **DIGITAL DECLARATION**

The IT Sub-Committee considered a report of the Chamberlain on the Digital Declaration.

The report provided details of the Government initiative and recommended that the City of London Corporation endorses and formally signs up to it. The report further informed Members that the Ministry for Housing, Communities and Local Government had set up a £7.5m fund for local authorities to bid for, to develop digital ways of working, citizen engagement and skills development. The Chamberlain explained that by signing up to the Digital Declaration the City of London Corporation would become an early adopter of the national Scheme and would represent an organisation commitment to digital working.

The Chairman highlighted the opportunity for the City of London Corporation to connect the Digital Declaration with the new Lord Mayor's proposed Digital Skills Strategy. It was further expressed by the Chairman that a change in the name of the IT Sub-Committee was appropriate to incorporate digital services, to better represent the breadth of work the Sub-Committee would be likely to be scrutinising in future. Members expressed board support for this potential change of name but noted that it should not be connected to a change to the IT Sub-Committee's Terms of Reference.

Resolved: that the IT Sub-Committee recommends to the Policy and Resources Committee that the City of London Corporation should sign up to the UK Ministry for Housing, Communities and Local Government (MHCLG) Digital Declaration is agreed.

14. **GDPR UPDATE**

The IT Sub-Committee received a report of the Comptroller and City Solicitor which provided an update on the internal audit of phase 1 of the Corporation's

arrangements for compliance with the General Data Protection Regulation. The report highlighted that oversight of GDPR is the responsibility of the IT Sub-committee and the Audit and Risk Management Committee. The Comptroller highlighted that the Mazars report appended to the main report was in draft but that the finalised report had been produced with no material differences. In addition, the Comptroller provided an update on the issue of third-party contractor's compliance with GDPR, explaining that the relevant departments had been informed of the issue and that the Comptrollers department had administered 120 data processing agreements, with a further update expected in early 2019.

On the issue of GDPR training the Comptroller clarified that the 94% quoted in paragraph 20 of the report was difficult to improve as staff moving departments and leaving or joining the City of London Corporation meant that in practice a higher percentage was unlikely to be achieved. In addition, Members were advised that 85% or over was considered a good industry standard.

A Member expressed a concern on the issue of GDPR compliance with bodies affiliated with the City of London Corporation, but not formally within scope of the City of London Corporation's GDPR oversite, such as the City of London Academy Trust (COLAT). The Comptroller confirmed that the City of London Corporation would offer informal support to organisation such as the COLAT but responsibility for GDPR compliance will remain with the organisation's information officer. Members highlighted that this was a potentially problematic issue as the City of London Corporation's connection to these organisations caused a reputational risk if they were non-GDPR compliant. The Comptroller confirmed that a report would be produced and considered at the May Information Technology Sub-Committee.

Replying to a Member's question regarding a discrepancy in the data in Mazars' report, the Comptroller explained that the he could not provide any further information regarding the data as it was produced by Mazars.

RESOLVED: - That-

I. The report be noted; and
II. That further GDPR monitoring reports be produced on a quarterly frequency.

15. **DESIGN, BUILD, SUPPORT AND HOSTING FOR NEW WEBSITE**

The IT Sub-Committee received a report of the Town Clerk on the design, build, support and hosting for the new website. The report informed Members of the progress on the website project, specifically with relation to date of the tender process. The IT Sub-Committee noted that the current website did not meet the City of London Corporation's needs and did not reflect well on the City of London Corporation. The Director of Communications confirmed that a winning bid for the contract had been decided and that he would confirm the details of this winning bid following the exclusion of the public.

RESOLVED: That the report on the new website be noted.

16. **GIGABIT CITY PROGRAMME UPDATE**

The IT Sub-Committee received a report of the Chamberlain on the Gigabit City Programme. Gigabit City aimed to improve wired and wireless connectivity in the Square Mile. The City's Strategic Infrastructure Advisor informed Members that progress on this project has been good. The main factor that had slowed progress had been engagement with certain landlords within the City of London, but that legal advice had been sourced to resolve the issue.

RESOLVED: That the update on the Gigabit City Programme be noted.

17. **POLICE UPDATE AND NATIONAL PROGRAMMES DRIVERS AND BENEFITS**

The IT Sub-Committee received a presentation from the Director of the Law Enforcement Programme at the Home Office who updated Members on police and national programmes drivers and benefits. The presentation provided a detailed and comprehensive overview of the use of technology in law enforcement and how these technologies could be used by forces such as the City of London Police.

A Member highlighted the issue of redundancies with the ANPR system when fully implemented. The Home Office representative replied that the NAS system was due to replace the APNR and would involve significant improvements. Members highlighted the issue of broadband reaching basements in the City of London which had proven to have limited broadband connectivity. The Home Office representative explained that mobile base stations being introduced in Police vehicles should enable better connectivity, and in areas without broadband connectivity device to device networks would be used as a contingency.

The Chamberlain highlighted the opportunities provided by the Police National Enabling Programme but noted delays in the Programme's delivery and the importance of the impact on financial planning.

RESOLVED: That the presentation be noted.

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

There were no questions.

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

There were no items of urgent business.

20. **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.

21. **NON-PUBLIC MINUTES OF THE PREVIOUS MEETING**
The IT Sub-Committee approved the non-public minutes of the meeting held on 10 July 2018 as an accurate record.

22. **OUTSTANDING ACTIONS FROM NON-PUBLIC MINUTES OF PREVIOUS MEETINGS**
The IT Sub-Committee received a joint report of the Town Clerk and the Chamberlain which provided updates of non-public outstanding actions from previous meetings.

23. **HOUSING MANAGEMENT SYSTEM GATEWAY**
The IT Sub-Committee considered a Gateway 2 report of the Director of Community & Children's Services on the Housing Management System.

24. **TRANSFORMATION PHASE 2 UPDATE**
A) The IT Sub-Committee considered a joint report of the Chamberlain and the Commissioner of the City of London Police on the City of London Police IT Modernisation MTFP Provision Request.

B) The IT Sub-Committee considered a joint report of the Chamberlain on the City of London Corporation IT Modernisation MTFP Provision Request.

25. **POLICE UPDATE REPORT**
The IT Sub-Committee received a report of the Chamberlain and Report of the Commissioner of the City of London Police providing a Police Update Report.

26. **IT TRANSFORMATION PROGRAMME - NETWORK TRANSFORMATION PROGRAMME - ISSUE REPORT**
The IT Sub-Committee received the Issue Report of the Chamberlain on the IT Transformation Programme.

27. **IT SECURITY UPDATE - CR16 AMBER AND FUTURE IT SECURITY PROJECTS**
The IT Sub-Committee received a report of the Chamberlain on the CR 16 Information Security Risk.

28. **2020 SOURCING PROJECT - POSITION STATEMENT**
The 2020 Sourcing Project report was deferred.

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

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

The Chairman accepted a report of the Chamberlain on the Waiver for Virgin Media Ltd Network Provision as an item of non-public urgent business.

There were no further items of urgent business considered in the non-public session.

The meeting ended at 3.48 pm

Chairman

Contact Officer: Richard Holt
Richard.Holt@cityoflondon.gov.uk

This page is intentionally left blank

Information Technology Sub-Committee – Public Outstanding Actions

Item	Meeting Date	Action and target for completion	Officer responsible	To be completed/ Next stage	Progress update
1	November 2018	A Member asked for feedback on the use of the **Piranha mobile stock control application** at Billingsgate Market. The IT Director responded that discussions had been taking place on the cost effectiveness of the Piranha App and whether the App's implementation at other markets would be appropriate.	Sean Green	February 2019	It was agreed that a report be presented to the next meeting of the IT Sub-Committee to provide Members with an update on the Piranha Application. A report has been produced that is being discussed as an agenda item

This page is intentionally left blank

Forward Plan – Updated February 2019

Report Title	Report Month	Category	Who
IT Division Business Plan	March 2019	Strategic	SG
Corporate Web Project Update	March 2019	Strategic	BR
Police Telephony and Call Recording	March 2019	Operational	MG
Transformation Programme Roadmap 2020	March 2019	Strategic	KM
IT Transformation Benefits Realisation Update	March 2019	Strategic	KM
Police Technology Horizon Scanning	March 2019	Strategic	AB
Post 2020 Strategic IT Partner Plan Update	March 2019	Strategic	KM
Migration of Drives and IM Protective Marking	March 2019	Strategic	MG
City of London Corporation Technology Horizon Scanning	March 2019	Strategic	KM
Information Management Roadmap	May 2019	Strategic	KS/SG
Digital Services Roadmap	May 2019	Strategic	KS/SG
Police Accommodation Programme Technology Roadmap Update	May 2019	Strategic	AB
City Broadband and 5G Rollout	May 2019	Strategic	SB
Police National Programmes Update	May 2019	Strategic	AB
IT Operating Model Implementation Review	May 2019	Strategic	SG
IT Service Benchmarking Review	May 2019	Strategic	MG
Review the Data Protection Policy	May 2019	Strategic	MC
Post 2020 Strategic IT Partner Plan Update	May 2019	Strategic	KM
New Ways of Working Review	June 2019	Strategic	SC

Contributors
Sean Green – SG
Sam Collins - SC
Matt Gosden – MG
Andrew Bishop - AB
Kevin Mulcahy – KM
Sam Kay – SK
Gary Brailsford-Hart – GBH
Steven Bage – SB

This page is intentionally left blank

Committee(s):	Date:
Summit Group Digital Services Sub-Committee (DSSC)	23 January 2019 4 February 2019
Subject: The case for a Digital Strategic Framework	**Public**
Report of: Town Clerk and Chamberlain	
Author: Kate Smith, Head of Corporate Strategy & Performance Sean Green, IT Director	**For Decision**

Summary

This paper sets out the case for adopting a Digital Strategic Framework and what should be included in such a framework, for comment and / or adoption.

Recommendations

It is recommended that Digital Services Sub-Committee (DSSC)):

i. Notes the case for a Digital Strategic Framework; and
ii. Comments on and / or adopts the proposed Digital Strategy Framework at Appendix 1.
iii. The report can then be taken through City of London Police (CoLP) governance processes.

Main Report

Background

1. As stated in the Corporate Plan 2018-23, disruptive changes, such as the digitisation of our work and personal lives, are likely to be to bring both threats and opportunities to our residents, workers, visitors, partners and our own organisation. To respond positively and constructively, we will need to be outward looking, outcome-focused and to think and act strategically and at pace, rather than put ourselves on a set course to digitisation.

2. Put another way, rather than set out a 'Digital Strategy' that aims to pre-empt and provide a long-term plan for the work we will need to undertake, what we need is a 'Digital Strategic Framework' that will help us make sure that all of our strategies, or indeed all of our work processes, are fit for a digital, and digitising, age.

3. By couching it within the framework of the Corporate Plan, we can also make sure that we keep our corporate outcomes firmly in mind and resist over-digitising – i.e. moving too many services or too many of our interactions online and risking poorer outcomes as a result – and that the principles we need to keep in mind are common to the many workstreams this will set in train, whether or not it is obvious that they are interrelated.

Context

4. All of the City Corporation's work relies to a greater or lesser extent on processes which have been digitised over the last two to three decades, even if only to the extent of using email to communicate. Many services are now looking to take advantage of more recent technological advances to reduce costs and improve outcomes, for example:

   - more user-friendly interfaces which enable self-service;
   - sensors which can send real-time information from remote points straight out to users or into databases for longer-term analysis;
   - the ability to link databases once and use them for multiple purposes and many times (avoiding double data entry); and
   - improvements in analytical capability and therefore understanding of trends and impacts (business intelligence).

5. At the same time, software options have proliferated and become more affordable and the risks relating to security and consumer rights have become more apparent; hence the enactment of the General Data Protection Regulations (GDPR) in 2018.

Proposal

6. If we are to take advantage of the opportunities presented by digitisation without succumbing to the risks, we need a common set of principles to guide us through the necessary checks and balances and keep us on course and acting as one intelligent and responsible organisation.

7. Appendix 1 sets out a proposed common set of principles, based on the relevant Corporate Plan outcomes, that can be used to guide decision-making across any and all City Corporation work, be it internally-facing, customer-facing or part of our wider work in support of outcomes for London and the UK.

8. Appendices 2 and 3 show how these same principles can be mapped to more specific design principles that can help us keep corporate workstreams, in this case our reviews of how we manage our information and how well we run our customer-facing processes, working in concert.

9. It should be noted that the principles set out in these appendices have all been written with the ultimate goal of creating a joint digital platform shared between

the City of London Corporation and City of London Police in mind, in order to promote closer working and to enable us to share information and intelligence where possible in pursuit of better outcomes. Both organisations working to common principles doesn't mean that a joint platform must be created but will put us in the best possible position either way. Appendix 1 has been shared with officers at the police for comment but formal approval has not been sought.

10. If, as work progresses, it becomes apparent that the principles can be better defined, a revised Digital Strategic Framework will be brought back to the Digital Services Sub-Committee and any changes will be applied retrospectively to relevant workstreams as needed (as per normal change control processes.)

Recommendations

10. It is recommended that Summit Group (then Digital Services Sub-Committee):

i. Notes the case for adopting a Digital Strategic Framework; and
ii. Comments on and / or adopts the proposed Digital Strategy Framework at Appendix 1.

Next steps

11. If the Digital Services Sub-Committee is happy to proceed on the basis set out above, officers will use the Digital Strategic Framework to help us ensure that any work to digitise our work is carried out in such a way as to deliver far reaching corporate as well as local goals.

Kate Smith

Head of Corporate Strategy and Performance

Town Clerk's Department

E: Kate.Smith@cityoflondon.gov.uk

Sean Green

IT Director

Chamberlain's Department

E: Sean.Green@cityoflondon.gov.uk

Appendices

Appendix 1 – Digital Strategic Framework draft principles

Appendix 1: Digital Strategic Framework draft principles

Relevant Corporate Plan outcomes	Internally	Externally	Beyond (City / London / UK level)
1. People are safe and feel safe	Officers, staff and Members' personal information is safe and their use of personal information is compliant with the law	CoLC and CoLP's service and asset users are safe and feel safe using our online services	People and businesses in the City, London and UK know how to be safe online
3. People have equal opportunities to enrich their lives and reach their full potential	Officers, staff and Members with protected characteristics have the same ease of access to information, tools and services as those without	CoLC and CoLP's service and asset users are digitally included (equal accessibility and usability)	People and businesses in the City, London and UK are digitally included
4. Communities are cohesive and have the facilities they need	Officers, staff and Members have appropriate access to information, digital tools and services, including options to self-serve	CoLC and CoLP's service and asset users have the digital tools they need to request services from CoLC, including via self-service where appropriate	Organisations from all sectors use relevant and up-to-date information to promote better outcomes for people, the economy and the environment
8. We have access to the skills and talent we need	CoLC & CoLP have the skills pipeline and access to talent they need to build and operate in a digital environment	CoLC and CoLP's service and asset users can access expert services when needed	City, London and UK businesses have the skills and talent to drive digital productivity and competitiveness People have the digital skills they need to thrive in all aspects of their lives
9. We are digitally and physically well-	CoLC & CoLP's information is easy to access and use many times and for multiple purposes	CoLC and CoLP's services and the environments we manage adapt in real-time to best meet asset	The City, London and UK are known for their world-leading digital experience, smart innovations

Relevant Corporate Plan outcomes	Internally	Externally	Beyond (City / London / UK level)
connected and responsive	CoLC and CoLP's information is as open as possible and connects with Smart tools and technologies	and service users' demands (e.g. lighting, road space, wayfinding, security, bandwidth) People and businesses in the Square Mile have 100% internet coverage and the world's fastest internet speeds	
10. We inspire enterprise, excellence, creativity and collaboration	Officers, staff and Members use the information, tools and services they need to innovate, collaborate and deliver the best possible outcomes for people, the economy and the environment	CoLC and CoLP's customers use information and digital tools and services that help them perform better, innovate and collaborate	The City, London and UK are known for their digital enterprise, excellence, creativity and collaboration
12. Our spaces are secure, resilient and well-maintained	CoLC and CoLP's digital environments are secure, resilient and well-maintained	CoLC and CoLP's customers' personal and business information is secure and as complete and up-to-date as they wish or as is needed to fulfil our duty to them (whichever is higher)	The City, London and UK are known for their digital and physical security and resilience

This page is intentionally left blank

Committee(s)	Dated:
Digital Services subcommittee Audit and Risk Management Committee	4th February 2019 12th March 2019
Subject: General Data Protection Regulation (GDPR/Data Protection Act 2018 (DPA))	**Public**
Report of: Michael Cogher, Comptroller & City Solicitor	**For Information/Decision**
Report author: Michael Cogher, Comptroller & City Solicitor,	

Summary

This report provides a general update on the progress of phase 2 of the GDPR/DPA Implementation Project and the planned outcomes for the final phase of the work to embed GDPR/DPA implementation into the Corporation.

Recommendations

1. Members are asked to note the report.

2. To determine the frequency of further GDPR/DPA monitoring reports in particular in relation to data breaches.

Introduction

1. This Report outlines the status of phase 2 of the GDPR/DPA project. Including the steps taken to address the recommendations of the internal audit by Mazars previously reported to Committee.

GDPR Project Progress

2. Phase two of the GDPR project commenced on 25 May 2018 and has been extended to 31 March 2019. This is to further assist departments to embed GDPR compliance with the following priorities identified in the May 2018 Mazar's GDPR compliance audit:

   - Reviewing third party contracts for GDPR compliance/data processing agreements.
   - Reviewing and refining the overarching Corporation records retention policy and developing detailed departmental records retention policies.

   The GDPR Project Team identified the following additional priority:

   - Auditing departmental compliance with GDPR requirements via a Compliance Monitor system, advising and further embedding GDPR compliance as business as usual.

GDPR Departmental Compliance Monitor

3. All Departments were issued with a self-audit template in November 2018 which covers the key activities, processes and arrangements that are required to ensure GDPR/DPA compliance. All departmental audits have been completed by the departments which process high-volume potentially high-risk personal data, these are:

   Markets and Consumer Protection
   DBE
   City Surveyors
   CoL School – Boys / CoL School – Girls / Freemens School
   DCCS and Community Safety
   Open Spaces
   Human Resources
   Remembrancers
   Chamberlains

   The following departments/teams are due to complete the self-audit by the end of February 2019:

   Electoral Services
   Comptroller & City Solicitor
   Mansion House
   Central Criminal Court
   Contact Centre
   Culture and Libraries
   Economic Development
   Occupational Health
   Guildhall School of Music & Drama

4. The GDPR team undertook a full analysis and audit of the completed returns and produced a compliance monitor; in terms of the core tasks which need to be completed to achieve full compliance, 51 % are fully implemented, 32% are partially implemented, only 2 % are not yet started and 15% do not apply to the department in scope. For example, processing of children's data and use of electronic communications used for marketing are not applicable to most departments. The current Self-Audit Monitors are updated every two months with the next return due at the end of February. A RAG summary of the departmental compliance self-audits is attached at Appendix 1. An example of a compliance self-audit is attached as Appendix 2.

5. Work is being undertaken with the responsible officers in each department (Access to Information Representatives (AIN)) and line managers to move partially implemented actions to fully implemented status during February. This is to ensure that work commences on the 2% of activities not yet started.

6. IT Services are covered by two separate monitors, one which covers the GDPR specific compliance tasks and a second for Systems and Data Security.

Third Party Contractors/Data Processors

7. This is an area rated as high priority by the Mazar's audit. The standard data protection provisions for Contractors/Data Processors was revised and has now been incorporated into all new contracts. All existing Contractors/Data Processors were issued with a written request to confirm that they are GDPR compliant and agreements have been amended where appropriate, of the 29 contracts which were outstanding in November 2018, all have reviewed, and appropriate amendments made. In some cases, contracts have been terminated or no longer used. This work is completed but data processing arrangements will continue to be audited using the compliance monitor.

Records retention policy and schedules.

8. The perceived lack of a record retention schedule was rated as a high priority in the Mazar's audit. Good progress has been made by departments in putting revised retention schedules in place, it is acknowledged that some departments have more complex records than others.

9. All but three departments have data retention schedules in place. City of London Girls School, Markets and Consumer Protection and Open Spaces are currently finalising their data retention schedules.

Information governance

10. Information governance was rated as low risk by the Mazar's report.

11. GDPR Corporate Risk CR 25 was created, agreed by Audit & Risk Committee and continues to be actively managed, monitored and reported to both the Corporate Risk Management Group and to committee.

12. Project delivery is controlled at bi-weekly Project Team stage control meetings. These meetings monitor progress, capture GDPR issues and risks, assess required changes, associated corrective action and allocate work packages. The Project Team reports to the Information Management Board and Digital IS Steering Group, additionally update reports and revised policies are reported to Policy & Resources and Establishment Committees and to the Digital Services Committee.

13. Regular liaison with IT workstreams is taking place which are reported to the GDPR Project Team for action and to the Information Management Board.

Training and communication

14. Six half day training sessions for AIN representatives and key staff were given by the Comptroller & City Solicitor and Senior Information Compliance Officer. In 2018 all AIN representatives have undertaken the initial training.

15. Further focused training has been provided to the HR Department, Remembrancer's Events Team and EDO. Quarterly AIN representatives' training and networking events have commenced with the second session taking place on 24th January 2019.

16. Five training sessions for Members were delivered in 2018, and a Member's guidance booklet was substantially revised to incorporate GDPR requirements. Template forms were also issued including RoPA and Privacy notices.

17. A mandatory GDPR e-leaning training package was launched on City Learning on 23 April 2018. Compliance levels were monitored by the Data Protection Officer and reported to Chief Officers. The current take-up is over 94.04%, as of the 1st January 2019. Full details are provided in Appendix 3. Due to staff turnover 94% constitutes a high level of compliance but the position will be kept under review. The ICO's expectation is that staff should have received training within the last two years.

Data Breaches

18. Under GDPR there is a duty to notify the ICO of data breaches posing a risk to individuals' rights within 72 hours (were feasible) of becoming aware of the breach. Where there is a high risk to data subjects they must also be informed. The Corporation has suitable arrangements in place for dealing with data breaches. Since 25th May (to the 22 Jan 2019) there have been 48 breaches notified to the Data Protection Officer. Of those 48, 7 were judged to be notifiable to the ICO. The ICO has responded to 6 indicating no action will be taken.

19. Of the 7, two related to mechanical problems with payslips/P60s, one to an email held on an outlook folder which was visible to third parties, one to a phishing attack, one to third party data sent to the incorrect applicant as part of the recruitment process and two due to insecure use of post. In all cases departments have been advised of appropriate steps to be taken to prevent future occurrences. Data Subjects were notified in 6 cases. Additionally, of the 7 reported to the ICO, 2 were in relation to activities undertaken by a processor on behalf of the Corporation.

20. The breach notification policy has been revised to provide that the Town Clerk, relevant Chief Officer(s), the Chairman of the Digital Services Committee and the relevant service committee Chairmen are notified of breaches notified to the ICO.

21. Members may wish to receive separate and more detailed reports, for example on a six-monthly basis on data breaches.

Conclusion

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

22. The GDPR project has made significant progress after achieving material compliance with GDPR requirements in May 2018. We are on target to meet the date of 31st March 2019 to close the project and move to business as usual. It is anticipated that a final compliance audit will be undertaken by Mazars following project closure. The Information Compliance Team will continue to monitor and audit departmental compliance with GDPR/DPA, but ownership and management of compliance will rest with departments with advice, training, support and monitoring provided by the Data Protection Officer.

Appendices

1. GDPR Compliance Monitor RAG Summary
2. Sample Departmental GDPR self-audit template
3. GDPR e-learning take up

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

This page is intentionally left blank

Appendix 1

RAG Summary of GDPR Compliance Monitors

v0.3 January 2019

Dept / Compliance Action	M&CP				DBE				City Surveyors							Schools			DCCS & Comm Safety								Open Spaces						HR		Remembrancers				Chamberlains (Non IT)												IT Services
GDPR Risks	Billingsgate	Smithfield	New Spitalfields	Port Health & Public Protection	Transportation & Public Realm	District Surveyor	Planning Policy	Planning & Development Mgt.	Operations Group	Corporate Property Group	Investment Property Group	Projects	Business Perormance & Directorate	CPAT		Col. S	Col. G	Freemens	People	Barbican Estates	Housing & Neighbourhoods	Housing Benefits	Barbican and Comm Libraries	Commissioning & Partnerships	Property	Public Health	Community Safety	The Commons	Epping Forest	Directorate	Cemetry and Crematorium	WH Park and City Gardens	H Heath / Highgate Wood / QP / KH	Org. Development Pay and Grading Learning & Development Support Systems		Busines Support	Parliamentary Counsel	Parliamentary Briefings Manager	City Events	Private Events	City Proc	Anti Fraud	City Revenues	Corp Treasury	Pensions	Dept facing finance units	Payroll	Corp Accountancy	Chamb Court	Directorate		IT Non Systems and Data Security
Areas where there are risks to GDPR compliance such as insecure data handling are notified to AIN reps and the Compliance Team.																																																	
Awareness - Communication & Guidance																																																	
Any job-specific training needs are identified and being managed																																																	
All staff are aware of the GDPR issues and queries process																																																	
ROPA and Records Management																																																	
Records Retention Schedule in place																																																	
Process for updating Retention Schedule is in place																																																	
ROPA in place																																																	
Process for updating ROPA is in place																																																	
Communicating privacy information																																																	
Privacy notices (how the City of London Corporation as a data controller collects and uses personal information) are in place																																																	
Lawful basis for processing personal data - consent																																																	
Records are kept for where consent has been received from the data subject																																																	
Contracts																																																	
There are written agreements in place for new contracts with third party service providers and processors, including those who process personal data on behalf of the City of London Corporation as a data controller, that ensure the personal data that they access and process is protected and secure.																																																	
Data Subjects Rights																																																	
All relevant staff are aware of the process for an individuals' requests to access their personal data (SAR , Right to Access)																																																	
Guidance is in place to respond to individuals' other rights Right to rectification Right to Erasure Right to Restriction Right to Data Portability Right to Object Right to Object to Automated Decision Making / Profiling																																																	
Guidelines for processing children's data are in place																																																	
Data Protection																																																	
All staff have read the CoL Data Protection Policy 2018																																																	
All staff are aware of the Data Protection Impact Assessment Procedure & Guidance																																																	
All relevant staff are aware of the process for identifying and reporting a Data Protection breach																																																	
Electronic communications conform to PECR (Privacy and Electronic Communications Regulations) i.e marketing by phone, email, text ; use of cookies or a similar technology on the CoL website; or compiling a telephone directory (or a similar public directory)																																																	
Guidance in place for transferring data securely outside of the EU																																																	
Guidance in place for transferring data securely between CoL and 3rd parties																																																
All staff have read the CoL Security Policy - People																																																	

IT Services - Systems and Data Security	
Secure storage arrangements are in place and documented to protect records and equipment in event of loss, damage, theft or compromise of personal data.	
Documented procedure in place to securely dispose of records and equipment when no longer required.	
Hardware and software assets are documented; management policy in place	
Security of mobile working and the use of mobile computing devices in place.	
New and existing hardware configured to reduce vulnerabilities and provide only the functionality and services required.	
Controls in place to manage the use of removable media in order to prevent unauthorised disclosure, modification, removal or destruction of personal data stored on it.	
User accounts to authorised individuals set up to provide the appropriate permissions and access to information.	
Password security policy and rules' in place to detect any unauthorised access or anomalous use.	
Anti-malware defences in place to protect computers from malware infection.	
Routine backs-up of electronic information in place to help restore information in the event of disaster.	
User and system activity logged and monitored to identify and help prevent data breaches.	
Security patching policy is place to prevent the exploitation of technical vulnerabilities	
Boundary firewalls in place to protect computers from external attack	
Personal data and information under management to identify / rectify potential risks to security	

Key	
Not yet started	
Partially implemented	
Fully implemented	
Not applicable to this department	

Appendix 2

Example GDPR Compliance Monitor. Dummy information for demonstration purposes only.

GDPR Departmental Self-Audit Monitor **Department : 1** **Reporting Period: December 2018**	**D1**	**D2**	**D3**	**D4**	**D5**	**D6**	**Exceptions**
Compliance Action	***Enter a number between 0-3 using the definitons below against each compliance action***						
GDPR Risks							
Areas where there are risks to GDPR compliance such as insecure data handling are notified to AIN reps and the Compliance Team.	3	2	3	3	3	3	
Awareness - Communication & Guidance							
Any job-specific training needs are identified and being managed	3	2	3	2	1	2	
All staff are aware of the GDPR issues and queries process	3	2	3	3	3	2	
ROPA and Records Management							
Records Retention Schedule in place	3	3	3	3	3	3	
Process for updating Retention Schedule is in place	2	2	2	2	2	2	
ROPA in place	3	3	3	3	3	3	
Process for updating ROPA is in place	1	2	2	2	3	2	
Communicating privacy information							
Privacy notices (how the City of London Corporation as a data controller collects and uses personal information) are in place	0	0	0	0	0	0	
Lawful basis for processing personal data - consent							
Records are kept for where consent has been received from the data subject	2	1	2	2	2	1	
Contracts							
There are written agreements in place for new contracts with third party service providers and processors, including those who process personal data on behalf of the City of London Corporation as a data controller, that ensure the personal data that they access and process is protected and secure.	0	0	0	0	0	0	
Data Subjects Rights							
All relevant staff are aware of the process for an individuals' requests to access their personal data (SAR , Right to Access)	1	2	3	3	3	2	
Guidance is in place to respond to individuals' other rights Right to rectification Right to Erasure Right to Restriction Right to Data Portability Right to Object Right to Object to Automated Decision Making / Profiling	1	1	3	2	2	3	
Guidelines for processing children's data are in place	2	2	2	3	3	2	

Data Protection							
All staff have read the CoL Data Protection Policy 2018	3	3	3	2	3	3	
All staff are aware of the Data Protection Impact Assessment Procedure & Guidance	3	3	3	3	3	3	
All relevant staff are aware of the process for identifying and reporting a Data Protection breach	3	3	3	3	3	3	
Electronic communications conform to PECR (Privacy and Electronic Communications Regulations) i.e marketing by phone, email, text ; use of cookies or a similar technology on the CoL website; or compiling a telephone directory (or a similar public directory)	3	0	3	3	2	0	
Guidance in place for transferring data securely outside of the EU	0	0	0	0	0	0	
Guidance in place for transferring data securely between CoL and 3rd parties	2	2	3	2	2	3	
All staff have read the CoL Security Policy - People	2	2	2	2	2	2	

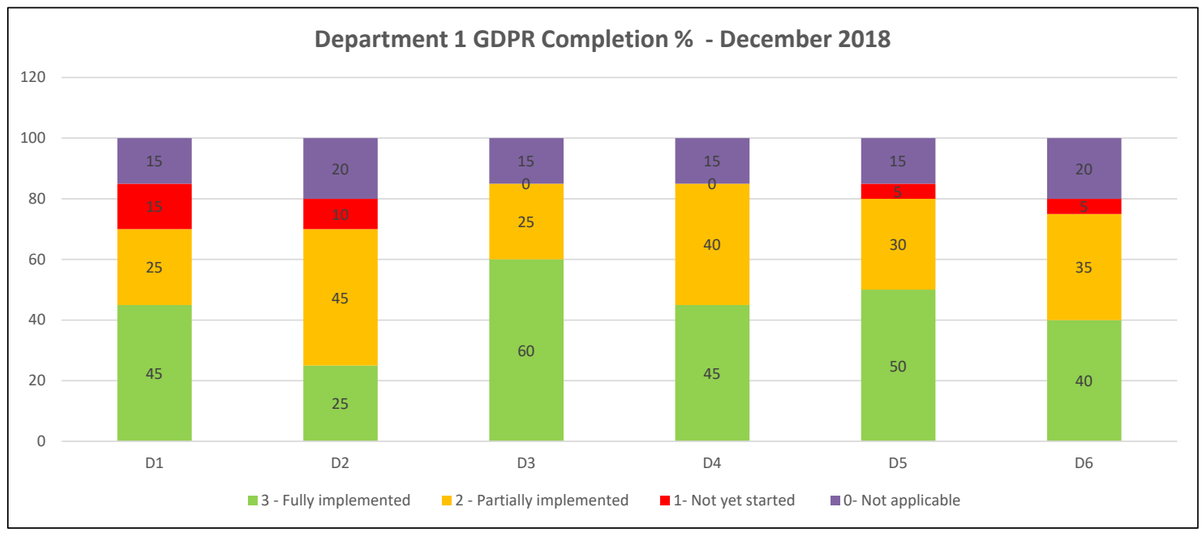
DO NOT ENTER DATA IN THESE CELLS

Count	D1	D2	D3	D4	D5	D6
3 - Fully implemented	45	25	60	45	50	40
2 - Partially implemented	25	45	25	40	30	35
1- Not yet started	15	10	0	0	5	5
0- Not applicable	15	20	15	15	15	20

Supplementary Notes

These questions and definitions are largely taken from the ICO GDPR self-assessment tool

Compliance Graph



Appendix 3 Table: Departments completion of the Data Protection E-Learning Programme, as of 1 January 2019

Department	Complete	Percentage	In Progress	Percentage	Not yet started	Percentage	Exempt	Percentage	Temporary Exempt**	Percentage	Total	Overall Percentage***
Barbican	367	81.02%	14	3.09%	41	9.05%	21	4.64%	10	2.21%	453	**87.86%**
CCC/Mansion House	143	96.62%	0	0.00%	3	2.03%	2	1.35%	0	0.00%	148	**97.97%**
Chamberlain's	293	94.82%	3	0.97%	4	1.29%	7	2.27%	2	0.65%	309	**97.73%**
City Surveyors Department	247	89.49%	1	0.36%	3	1.09%	21	7.61%	4	1.45%	276	**98.55%**
Comptroller's and City Solicitors	61	96.83%	0	0.00%	0	0.00%	2	3.17%	0	0.00%	63	**100.00%**
Dept. of the Built Environment	252	96.92%	3	1.15%	1	0.38%	4	1.54%	0	0.00	260	**98.46%**
Dept. Communities and Children's Services	336	81.55%	7	1.70%	10	2.43%	54	13.11%	5	1.21%	412	**95.87**
Guildhall School of Music and Drama	280	86.69%	17	5.26%	22	6.81%	3	0.93%	1	0.31%	323	**87.93%**
Markets and Consumer Protection	251	91.61%	0	0.00%	2	0.73%	19	6.93%	2	0.73%	274	**99.27%**
Misc.****	4	50.00%	0	0.00%	4	50.00%	0	0.00%	0	0.00%	8	**50.00%**
Open Spaces	332	68.60%	6	1.24%	31	6.40%	113	23.35	2	0.41	484	**92.36%**
Remembrancers	30	90.91%	1	3.03%	1	3.03%	1	3.03%	0	0.00%	33	**93.94%**
Schools*	516	88.36%	14	2.40%	31	5.31%	14	2.40%	9	1.54%	584	**92.29%**
Town Clerks Department	317	90.05%	7	1.70%	14	3.40%	9	2.18%	11	2.67%	412	**94.90%**
Total	**3483**		**73**		**167**		**270**		**46**		**4039**	

* The totals provide for schools, is a combined total for the city of London School, City of London School for Girls and the City of London Freemen's School.

** Those marked temporary exempt will need to complete the course on their return to work, for example they are on a period of long term absence, maternity leave, etc.

*** The overall percentage is a combined total of those who have completed the course, have been made exempt or are temporarily exempt.

****Anyone who has not been assigned a department e.g. Contractors

Committee(s)	Dated:
Digital Services Sub Committee (DSSC)	4th February
Subject: CR 16 Information Security Risk	**Public**
Report of: Chamberlain	**For Decision**
Report author: Gary Brailsford-Hart ,Director of Information & Chief Information Security Officer	

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 not 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 developing well and are reflective of the ongoing adoption across the City Corporation, all risk areas continue to be actively monitored and risk managed. Scores will continue to increase as improvements to people, process and technology are delivered.

The overall objective is to bring our security controls to an appropriate level of maturity. Currently, the organisation has a target maturity score of Level 4 (Managed and Measureable) across all areas, three controls are currently at this level, and seven control areas are currently at Level 3 (Defined Process). The mitigation controls are currently Amber (action required to maintain or reduce rating), with the ongoing improvements the recommendation is to move the CR16 risk to Amber.

Recommendation(s)

Members are asked to:

- Note the report.
- Agree that the risk can be moved to Amber

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. The first step of the ISMS is the “risk management regime**“,** as the NCSC describe it, this is the strategy that glues different controls and processes together. This ensures we do not fragment the approach to cyber security and identify hidden vulnerabilities and potential for compromise, ensuring the ability to measure the risk profile. The remaining nine steps are broken down into four clear delivery areas: Establish, Manage, Enhance, and Deliver.

Information Risk Management	% Complete	Target Score	Actual Score	Trend
Information Risk Management	86%	4	4	↑
Risk appetite statement is the next applicable piece of work in this area. Involves an overarching agreement with the SIRO and then a cascade framework for application in each of the business areas across the City. In addition, a code of connection has been developed to support institutional departments connecting to and consuming core IT services from City. This work is pending review of SIRO role and position within the business.				

Establish	% Complete	Target Score	Actual Score	Trend
Monitoring	72%	4	3	↑
Incident Management	90%	4	4	↑
Secure Configuration	86%	4	3	↑
The deployment, throughout October/November, of the Security Information and Event Management collector has taken place. However, connection work remains outstanding and once in place this will establish direct improvements to the monitoring and secure configuration across the City infrastructure.				

Manage	% Complete	Target Score	Actual Score	Trend
Network Security	69%	4	3	↑
Managing User Privileges	75%	4	3	↑
Network security will directly improve following the implementation of the Security Information and Event Management collector was deployed throughout October/November. The issues of managing user privileges is currently being managed manually and a technical solution has been purchased and is awaiting implementation across the infrastructure – this is a complex piece of software and whilst installation is simple, the application and management will take time to develop and tune.				

Enhance	% Complete	Target Score	Actual Score	Trend
Malware Prevention	68%	4	3	↑
Removable Media Controls	89%	4	4	↑
A project is underway to review the existing anti-malware solution and determine if enhancements are required, this remains ongoing. The removable media controls have recently been reviewed and the deployment of controls have been confirmed. To improve the removable media control score requires further work in respect of policies and user education, this is currently being included within the procedural refresh for removable media across IT, this will include a sign-off process for receipt of devise and responsibilities.				

Deliver	% Complete	Target Score	Actual Score	Trend
Home and Mobile Working	64%	4	3	↑
User Education and Awareness	75%	4	3	↑
The next steps for the Home and Mobile Working control area are for a thorough review of user acceptance policies and guidance. In addition, the aging Citrix infrastructure is being replaced, once complete this will improve the scores in this area. A developed schedule of awareness and training is being rolled out across the organisation with a different theme each month.				

9. 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 continue to improve and are embedding across the City Corporation, the risk areas are actively monitored and risk managed. Scores 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 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 January 2019

Ten Steps - **Control Area**	% Complete	Target Score	Actual Score	Trend
1. Information Risk Management	86%	4	4	↑
2. Network Security	69%	4	3	↑
3. Malware Prevention	68%	4	3	↑
4. Monitoring	72%	4	3	↑
5. Incident Management	90%	4	4	↑
6. Managing User Privileges	75%	4	3	↑
7. Removable Media Controls	89%	4	4	↑
8. Secure Configuration	86%	4	3	↑
9. Home and Mobile Working	64%	4	3	↑
10. User Education and Awareness	75%	4	3	↑

Options

10. 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

11. Continue to implement the 10 steps programme across the City Corporation.
12. Accept the risk is now at an Amber status.

Implications

13. 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.

14. 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

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

Conclusion

16. 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.

17. 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.

18. 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.

19. 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:

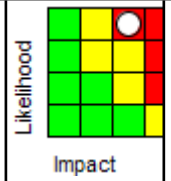
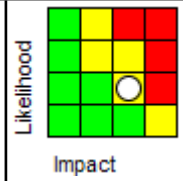
- Appendix 1 – CR16 Information Security
- Appendix 2 – 10 Steps to Cyber Security Dashboard & Breakdown
- Appendix 3 – Statutory Requirements Summary
- Appendix 4 – Maturity Scoring Matrix

Gary Brailsford-Hart
Director of information & Chief Information Security Officer
T: 020 7601 2352 E: gary.brailsford@cityoflondon.police.uk

Appendix 1 -Detailed risk register CR16

Report Author: Samantha Kay
Generated on: 18 January 2019

Rows are sorted by Risk Score

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 22-Sep-2014 Peter Kane	**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 2018. Incur a monetary penalty of up to £500,000. Compliance enforcement action. Corruption of data. Reputational damage to Corporation as effective body.		**16**	This risk will remain at Red until January 2019 when key security projects will be completed, and the 10 Steps maturity model had reached a level 4. The team are on track to reduce this risk to Amber in January. **08 Jan 2019**		**8**	31-Jan-2019	Constant

Action no	Action description	Latest Note	Action owner	Latest Note Date	Due Date
CR16k	Final stages of completing IT security projects so that we can assure Members that the City of London Corporation has implemented all the national government recommended security practices and technology achieving a maturity level of 4.	IT Security projects completed with recommendation that this is risk is moved to Amber	Gary Brailsford-Hart	18-Jan-2019	04-Feb-2019

Page 38

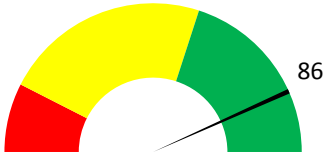
City of London Corporation

10 Steps Maturity Assessment

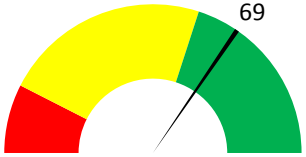
11 January 2019

10 Steps to Cyber Security: Dashboard

1. Information Risk Management

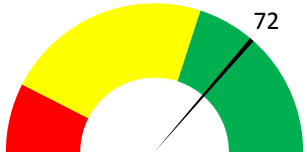


2. Network Security



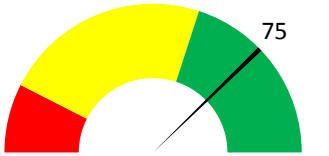
3. Malware Prevention

4. Monitoring

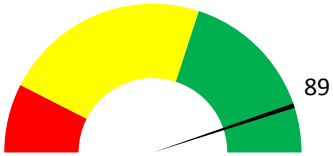


5. Incident Management

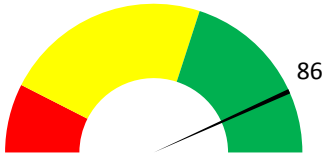
6. Managing User Privileges



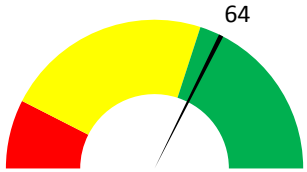
7. Removable Media Controls



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: 11 January 2019

	% Complete	Target Score	Actual Score
Information Risk Management	**86%**	**4**	**4**
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	100%	4	4
Make use of endorsed assurance schemes	100%	4	4
Educate users and maintain their awareness	75%	4	3
Promote a risk management culture	75%	4	3

	% Complete	Target Score	Actual Score
Network Security	**69%**	**4**	**3**
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	50%	4	2
Assurance process	100%	4	4

	% Complete	Target Score	Actual Score
Malware Prevention	**68%**	**4**	**3**
Develop and implement anti-malware policies	75%	4	3
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

	% Complete	Target Score	Actual Score
Monitoring	**72%**	**4**	**3**
Establish a monitoring strategy and supporting policies	50%	4	2
Monitor all ICT systems	75%	4	3
Monitor network traffic	75%	4	3
Monitor all user activity	75%	4	3
Fine-tune monitoring systems	50%	4	2
Establish a centralised collection and analysis capability	75%	4	3
Provide resilient and synchronised timing	100%	4	4
Align the incident management policies	75%	4	3
Conduct a lessons learned review	75%	4	3

	% Complete	Target Score	Actual Score
Incident Management	**90%**	**4**	**4**
Obtain senior management approval	100%	4	4
Provide specialist training	100%	4	4
Define the required roles and responsibilities	100%	4	4
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	50%	4	2
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

	% Complete	Target Score	Actual Score
Managing User Privileges	**75%**	**4**	**3**
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	75%	4	3
Monitor	75%	4	3
Limit access to the audit system and the system activity logs	50%	4	2
Educate users and maintain their awareness	75%	4	3

	% Complete	Target Score	Actual Score
Removable Media Controls	**89%**	**4**	**4**
Produce corporate policies	50%	4	2
Limit the use of removable media	100%	4	4
Scan all media for malware	100%	4	4
Formally issue media to users	100%	4	4
Encrypt the information held on media	100%	4	4
Actively manage the reuse and disposal of removable media	100%	4	4
Educate users and maintain their awareness	75%	4	3

	% Complete	Target Score	Actual Score
Secure Configuration	**86%**	**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	100%	4	4
Conduct regular vulnerability scans	75%	4	3
Establish configuration control and management	75%	4	3
Disable unnecessary peripheral devices and removable media access	100%	4	4
Implement white-listing and execution control	100%	4	4
Limit user ability to change configuration	100%	4	4
Limit privileged user function	50%	4	2

	% Complete	Target Score	Actual Score
Home and Mobile Working	**64%**	**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	100%	4	4
Protect data at rest	100%	4	4
Protect data in transit	75%	4	3
Review the corporate incident management plans	75%	4	3

	% Complete	Target Score	Actual Score
User Education and Awareness	**75%**	**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	100%	4	4
Monitor the effectiveness of security training	50%	4	2
Promote an incident reporting culture	75%	4	3
Establish a formal disciplinary process	100%	4	4

Current status of 10 Step control areas across organisation.

ASSESSMENT DATE: 11 January 2019

Control Area	% Complete	Target Score	Actual Score
Information Risk Management	86%	4	4
Network Security	69%	4	3
Malware Prevention	68%	4	3
Monitoring	72%	4	3
Incident Management	90%	4	4
Managing User Privileges	75%	4	3
Removable Media Controls	89%	4	4
Secure Configuration	86%	4	3
Home and Mobile Working	64%	4	3
User Education and Awareness	75%	4	3

City of London Corporation - Report of: Gary Brailsford-Hart, Director of Information & CISO - Assessment Date: 11 January 2019

This page is intentionally left blank

Appendix 3: Statutory Requirements Summary

Data Protection Act 2018
http://www.legislation.gov.uk/ukpga/2018/12/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 six guiding principles which requires that personal data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency');

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes ('purpose limitation');

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals ('storage limitation');

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')."

As a data controller, the City Corporation must also notify annually with the Information Commissioner's Office. The Act also places a responsibility on the Controller to notify the ICO of data breaches within 72 hours. The Information Commissioner has the power to issue fines of up to 4% of annual global turnover or 20 million euros (whichever is the greater) 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.

This page is intentionally left blank

Maturity Scoring Matrix

Scoring	Definition	Controls	Awareness & Communication	Polices, Plans & Procedures	Tools & Automation	Skills & Expertise	Responsibility & Accountability	Goal Setting and Measurement
0	Non-existent	Complete lack of any recognisable processes. The enterprise has not even recognised that there is an issue to be addressed.	Complete lack of any recognisable processes. The enterprise has not even recognised that there is an issue to be addressed.	Complete lack of any recognisable processes. The enterprise has not even recognised that there is an issue to be addressed.	Complete lack of any recognisable processes. The enterprise has not even recognised that there is an issue to be addressed.	Complete lack of any recognisable processes. The enterprise has not even recognised that there is an issue to be addressed.	Complete lack of any recognisable processes. The enterprise has not even recognised that there is an issue to be addressed.	Complete lack of any recognisable processes. The enterprise has not even recognised that there is an issue to be addressed.
1	Initial/Ad Hoc	There is evidence that the enterprise has recognised that the issues exist and need to be addressed. There are, however, no standardised processes; instead, there are ad hoc approaches that tend to be applied on an individual or case-by-case basis. The overall approach to management is disorganised.	Recognition of the need for the process is emerging. There is sporadic communication of the issues.	There are ad hoc approaches to processes and practices. The process and policies are undefined.	Some tools may exist; usage is based on standard desktop tools. There is no planned approach to the tool usage.	Skills required for the process are not identified. A training plan does not exist and no formal training occurs.	There is no definition of accountability and responsibility. People take ownership of issues based on their own initiative on a reactive basis.	Goals are not clear and no measurement takes place.
2	Repeatable but intuitive	Processes have developed to the stage where similar procedures are followed by different people undertaking the same task. There is no formal training or communication of standard procedures, and responsibility is left to the individual. There is a high degree of reliance on the	There is awareness of the of the need to act. Management communicates the overall issues.	Similar and common processes emerge, but are largely intuitivebecause of individual expertise. Some aspects of the process are repeatable because of individual expertise, and some documentation and	Common approaches to use of tools exist but are based on solutions developed by key individuals. Vendor tools may have been acquired, but are probably not applied correctly, and may even be shelfware.	Minimum skill requirements are identified for critical areas. Training is provided in response to needs, rather than on the basis of an agreed plan, and informal training on the job occurs.	An individual assumes his/her responsibility and is usually held accountable, even if this is not formally agreed. There is confusion about responsibility when problems occur, and a culture of blame tends to exist.	Some goal setting occurs; some financial measures are established but are known only by senior management. There is inconsistent monitoring in isolated areas.
3	Defined process	Procedures have been standardised and documented, and communicated through training. It is mandated that these processes should be followed; however, it is unlikely that deviations will be detected. The procedures themselves are not sophisticated but are the	There is an understanding of the need to act. Management is more formal and structured in its communication.	Usage of good practices emerges. The process, policies and procedures are defined and documented for all key activities.	A plan has been defined for use and standardisation of tools to automate the process. Tools are being used for their basic purposes, but may not all be in accordance with the agreed plan, and	Skill requirements are defined and documented for all areas. A formal training plan has been developed, but formal training is still based on individual initiatives.	Process responsibility and accountability are defined and process owners have been identified. The process owner is unlikely to have the full authority to exercise the responsibilities.	Some effectiveness goals and measures are set, but are not communicated, and there is a clear link to business goals. Measurement processes emerge, but are not consistently applied. IT balanced scorecard ideas are being adopted, as is occasional intuitive application of root
4	Managed and measureable	Management monitors and measures compliance with procedures and takes action where processes appear not to be working effectively. Processes are under constant improvement and provide good practice. Automation and tools are used in a limited or fragmented way.	There is understanding of the full requirements. Mature communication techniques are applied and standard communication tools are used.	The process is sound and complete; internal best practices are applied. All aspects of the process are documented and repeatable. Policies have been approved and signed off on by management. Standards for developing and maintaining the processes and procedures are adopted and followed.	Tools are implemented according to a standardised plan, and some have been integrated with other related tools. Tools are being used in main areas to automate management of the process and monitor critical activities and controls.	Skill requirements are routinely updated for all areas, proficiency is ensured for all critical areas, and certification is encouraged. Mature training techniques are applied according to the training plan, and knowledge sharing is encouraged. All internal domain experts are involved, and the effectiveness of the training plan is assessed.	Process responsibility and accountability are accepted and working in a way that enables a process owner to fully discharge his/her responsibilities. A reward culture is in place that motivates positive action.	Efficiency and effectiveness are measured and communicated and linked to business goals and the IT strategic plan. The IT balanced scorecard is implemented in some areas with exceptions noted by management and root cause analysis is being standardised. Continuous improvement is emerging.
5	Optimised	Processes have been refined to a level of good practice, based on the results of continuous improvement and maturity modelling with other enterprises. IT is used in an integrated way to automate the workflow, providing tools to improve quality and effectiveness, making the enterprise quick to adapt.	There is advanced, forward-looking underestanding of the requirements. Proactive communication of the issues based on trends exists, mature communication techniques are applied, and integrated communcation tools are in use.	External best practices and standards are applied. Process documentation is evolved to automated workflows. Processes, policies and procedures are standardised and integrated to enable end-to-end management and improvement.	Standardised tool sets are used across the enterprise. Tools are fully integrated with other related tools to enable end-to-end support of the processes. Tools are being used to support improvement of the process and automatically detect control exceptions.	The organisation formally encourages continuous improvement of skills, based on clearly defined personal and organisational goals. Training and educationsupport external best practices and use of leading-edge concepts and techniques. Knowledge sharing is an enterprise culture, and knowledge-based systems are being deployed. External experts and industry leaders are used for guidance.	Process owners are empowered to make decisions and take action. The acceptance of responsibility has been cascaded down throughout the organisation in a consistent fashion.	There is an integrated performance measurement system linking IT performance to business goals by global application of the IT balanced scorecard. Exceptions are globally and consistently noted by management and root cause analysis is applied. Continuous improvement is a way of life.

This page is intentionally left blank

Committee(s)	Dated:
Digital Services Sub-Committee – For Information	4th February 2019
Subject: IT Division – IT Service Delivery Summary	**Public**
Report of: The Chamberlain	**For Information**
Report author: Matt Gosden Deputy IT Director and Eugene O'Driscoll, Service Director, Agilisys	

Summary

IT Service performance was generally very good in December for both the City of London Corporation (CoL) and City of London Police (CoLP), though there was a small number of priority incidents with external causes that could not have been predicted, and which took longer than expected for 3rd parties to resolve.

- There were 3 P1 incidents for City of London Corporation and 3 for City of London Police.
- There were no P2 incidents for the City of London Corporation and 1 for City of London Police.
- There were no IT outages over the Christmas and New year period in City of London Corporation and just one for City of London Police which was resolved.
- The Net Promoter Score average for the City of London Corporation and City of London Police for the last 3 months is 60. Any score over 50 is considered very good.
- 84% of users who completed the customer satisfaction survey following contact with the City of London Corporation Service Desk reported a good or very good experience.
- 100% of users reported a good or very good experience of the City of London Police Service Desk.
- The City of London Police and city of London Corporation annual PSNP and PSN readiness assessments were carried out in June and November 2018 respectively. This identified some areas of work required to maintain accreditation. The majority of these have been completed and mitigation statements are being prepared for PSN discussion with the accreditors.

Recommendations

Members are asked to note this report

Main Report

Service levels and exceptions

1. **City of London Police (CoLP)**

P1 incidents

There were 3 P1 incidents

Affected Service	Reason	Resolution
Pronto	CoLP firewall fault prevented users from logging in to Pronto.	Firewall clusters were restarted.
Pronto	Pronto supplier Airwave server fault prevented Pronto clients from synchronising	Airwave restarted the servers
PNC	Software configuration issue during Vodafone planned maintenance	Vodafone reversed the change

P2 Incidents

There was 1 P2 incident

Affected Service	Reason	Resolution
O2 data services	O2 data services were unavailable due to a software fault in the O2 environment	Resolved by O2

2. **City of London Corporation (CoL)**

P1 incidents

There were 3 P1 incidents

Affected Service	Reason	Resolution
X250 laptops	A Microsoft security update prevented this laptop model from working.	The laptops were reconfigured or rebuilt; to avoid future issues the devices will be replaced in 2019.
Internet access	Internet access was disrupted during a planned change outside of core business hours.	The change was halted and reversed, with no impact on users during business hours.
COL public website	Monitoring detected a significant increase in suspicious traffic to the CoL public website.	Once verified that the source of the traffic was unknown and unauthorised, the source was blocked.

P2 Incidents

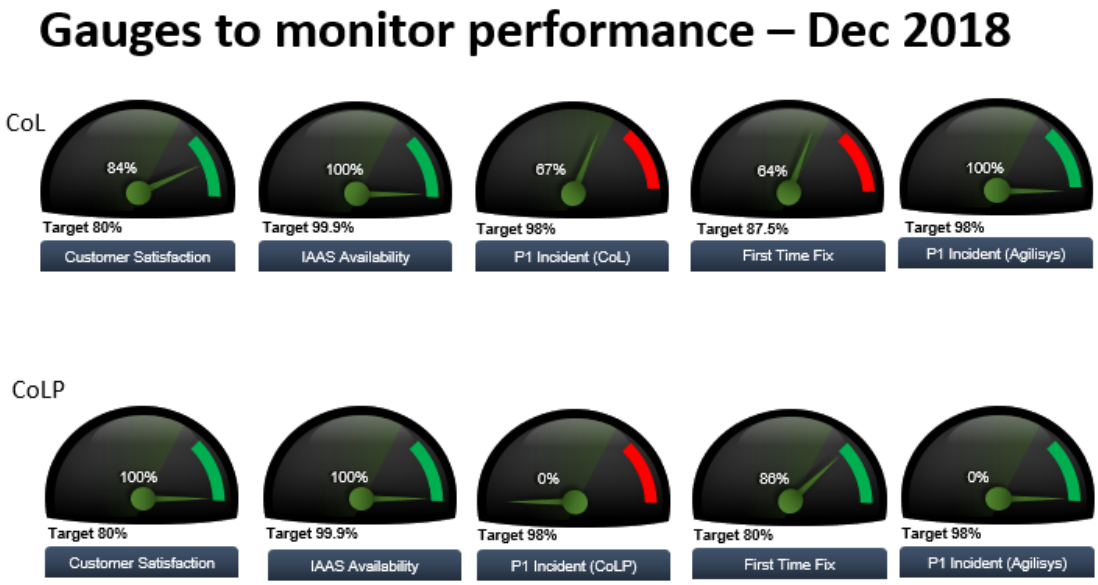
None to report

With regards to the P1 incident for Lenovo X250 laptops in City of London Corporation, the incident was caused by a correct software release from Microsoft that required an engineer visit to each computer to rectify. The X250 laptops use older components that carry an increased risk of incompatibility with future software releases and this model will be retired from service in 2019.

With regards to the P1 incident for the City of London Corporation public website, it should be noted that IT monitoring and response processes were effective such that the website was fully available at all times with no degradation of service. Sudden and sustained increases in traffic can be signs of an attack on the websites, either to consume system resources to deny service to legitimate users (Denial-of-service attack) or to hack the website to gain unauthorised access. The incident was reported to City of London Police Action Fraud as an attack.

With regards to the two incidents affecting Pronto in City of London Police, suppliers have been engaged to investigate and improve firewall reliability. A detailed review meeting will be held with the suppliers to focus on ensuring service stability.

Service performance summary is detailed in the dashboard below.



Service improvements

3. City of London Police Improvements include:

    - Improvements to process have been made for handling P1 and P2 incidents for Pronto and Niche.

    - There has been a steady decline in incidents reported by remote access (VPN) users. This is due to a client upgrade, production of a user guide and targeted assistance to customers to ensure correct use and installation.

    - Agilisys proposals for enhanced support for Microsoft SQL, IMS/DRS and Blackberry have been presented to the City of London Police and are awaiting sign-off.

    - A proposal from Agilisys for an upgrade to City of London Police's Sharepoint implementation is awaiting approval.

4. City of London Corporation improvements include:

    - Agilisys demonstrated new tools for user self-service which will improve compliance with policies for the processing of new starters and of leavers.

    - The City of London Corporation's very successful Desktop Transformation programme was extended to London Councils. 80% of the London Councils team is now working with new Windows 10 laptops and supporting technologies. Feedback from the users has been very positive, indicating a smooth transition. Further work is planned for services currently operating on an unstable local infrastructure, which will be migrated to the IaaS environment. This will enable the organisation to realise benefits associated with its accommodation strategy in 2019.

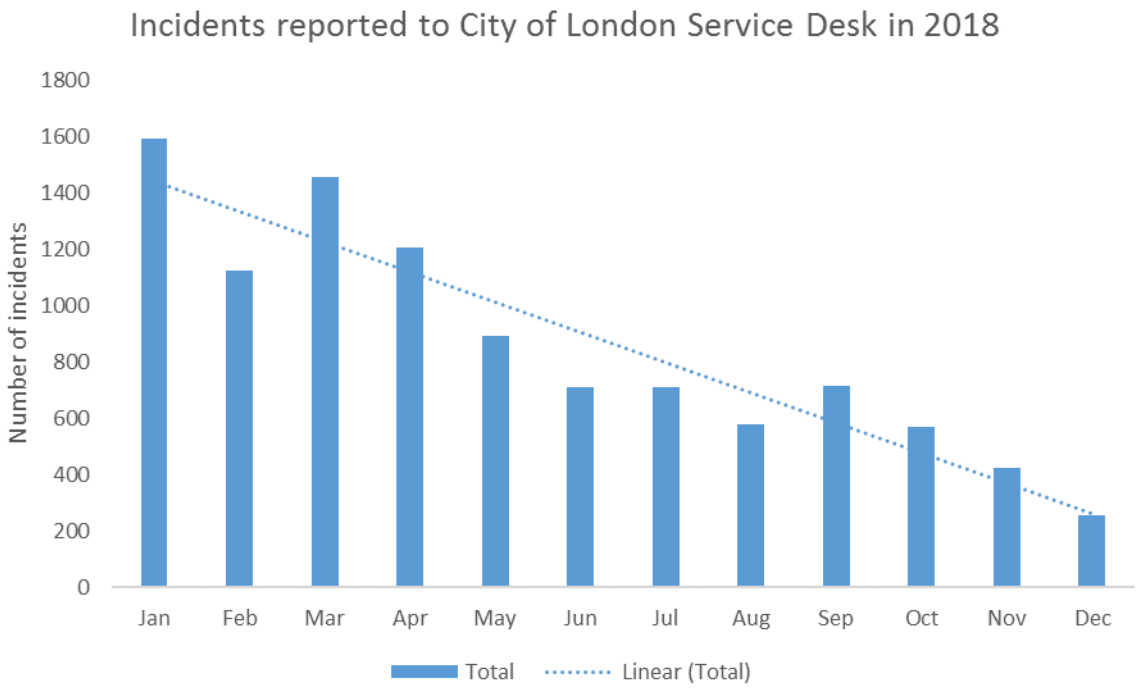
    - A proposal was presented by Agilisys to migrate storage for both the Corporation and Police from the Agilisys IaaS platform to a multi-cloud, multi-provider solution managed by Agilisys. This will maintain the current high-quality service provision and reduce costs for the organisation.

5. Transformation success – reduced number of incidents reported to Service Desk.

    The blue lines in the graph below represents the number of incidents reported to the City of London Corporation Service Desk each month in 2018.

    There has been a 60% reduction in the number of incidents reported, from a high of almost 1600 incidents in January 2018 to a low of 250 in December 2018.

    This is an important success indicator for the Desktop Transformation project, which transformed the user experience, and supports the high rates of reported user satisfaction.



Public Services Network (PSN) Accreditation

6. The City of London Corporation needs to renew our PSN annually to remain connected to National Government IT systems such as those provided by the Department of Work and Pensions. To do this our IT security systems and processes need to be reviewed annually though a third party consultancy.

7. The IT Security review (IT Security Healthcheck) was completed in June18 for CoLP and November 18 for CoL.

8. The actions for CoLP have been remediated and the PSNP submission is now ready.

9. PSN actions for CoL are being remediated prior to submission in February 19 to obtain PSN accreditation sign off.

10. At point of writing this report any critical actions are on track for completion prior to submission.

Matt Gosden
Deputy IT Director
T: 07714 746996
E: Matt Gosden@cityoflondon.gov.uk

Eugene O'Driscoll
Service Director
Agilisys
T: 0755 7150020
E: Eugene.O'Driscoll@cityoflondon.gov.uk

NOT PROTECTIVELY MARKED

This page is intentionally left blank

Committee(s)	Dated:
Digital Services Sub Committee – For Information	4th February 2019
Subject: IT Division Risk Update	**Public**
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. The IT Division currently holds 7 risks, a decrease of two from the previous period. There are currently no RED risks. There are no extreme impact risks, there are 3 major impact, 4 serious impact and no Minor impact risks.

IT currently holds 1 risk on the Corporate Risk Register, whilst feeding in to the GDPR Corporate risk which is owned by Comptrollers.

Summary of the Corporate Risks

CR 16 – Information Security - This risk is recommended to move to Amber as key security projects have been completed, and the 10 Steps maturity model has reached a maturity level of 4.

CR-25 – General Data Protection Regulation –

Progress on high risk areas identified in the Mazars audit:

- 1.Significant progress has been made toward facilitating departmental compliance with GDPR requirements
- 2.Significant progress has been made toward ensuring contractor compliance with GDPR requirements
- 3.An overarching CoL retention schedule is in place and 75% of departments have responded with detailed retention schedules.
- 4.The management of unstructured data constitutes a significant GDPR compliance risk. Four potential suppliers have been identified. Now developing a business case to secure funds

Recommendation(s)

Members are asked to:

- Note the report.

Main Report

Background

1. 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. The IT Division Currently holds 1 Amber risk on the Corporate Risk Register and assists to mitigate one other Amber Corporate Risk. The IT Division currently holds 8 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.

Current status

3. Since the last report the IT Risk Register has seen the following activity:

    - 2 Additional risks have been identified
    - 2 Risks have been reduced from Departmental to Divisional level.
    - 1 Risk has been deactivated

    The remainder are static and continue to be monitored alongside the relevant on-going projects.

Risks with Score Changes

4. **New Risks**

    - **CHB IT 020** Public Service Network Compliance – This risk previous featured on the Departmental Register, however when PSN compliance was gained the risk was marked as mitigated. In order to retain PSN compliance there are some areas of in need of remediation activities, therefore the risk has been added back to Departmental level for focus.
    - **CHB IT 004 – Business Continuity/Disaster Recovery –** This risk was being monitored at a service level, however in order to ensure focus from the business and IT, it was deemed appropriate to return this risk to a Departmental level risk.

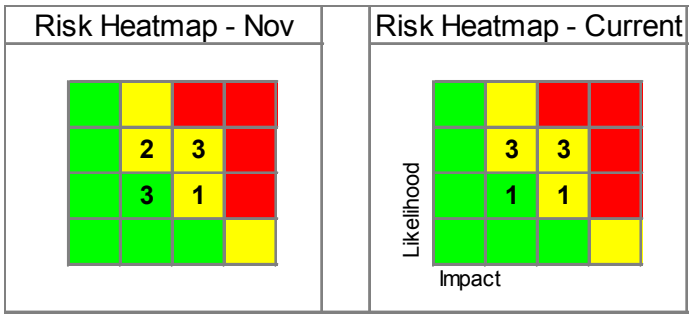
5. **Deactivated Risks**
    - **CHB IT 024 – IT Service Provision** – Following the downgrading of the Corporate Risk for IT Service Provision this risk was established as a departmental risk, however following a more detailed review the mitigating actions were covered at a more detailed level across other departmental risks. Therefore, this risk will be deactivated.

6. Risks reduced from Departmental to Divisional Level

The following risks have been reduced to division level due to mitigating actions being completed, and processes implemented to maintain systems going forward.

- **CHB IT 002 – Connectivity – Local & Wide Area Network** – Due to completion of Network Transformation Programme – this will be monitored as a Service Level Risk
- **CHB IT 022 – Transformation – Benefits Realisation** – Due to reductions IAAS Costs & User Adoption – This will be monitored as a Service Level Risk

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



7. Further breakdown of current Division risks:

Major Impact:

Risks with “likely” likelihood and “major” impact:	0	⟷
Risks with “possible” likelihood and “major” impact:	3	↓
Risks with “Unlikely” likelihood and “major” impact:	1	⟷

↑ Increase in No.
↓ Decrease in No.
⟷ Static No.

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	↓

8. Next steps

- 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:
Digital Services Sub Committee Public Relations and Economic Development Committee	04/02/2019 05/02/2019
Subject: Update on new website	**Public**
Report of: 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, specifically to establish progress to date.

The current website does not meet our needs and does not reflect well on the City of London Corporation. The content management system of the current website will also be redundant after Summer 2020.

Therefore, we wish to replace the current website with one with the ability to display well on mobile devices, to provide comprehensive search results and to provide information in a task-based and user-focused manner.

The project went out to tender in summer 2018 and the results were verified at the IT Category Board on 9 October 2018. The suppliers, Zengenti, were appointed in November 2018.

The project has been approved at Gateway 5 enabling funding to be released which has allowed recruitment for a Project Manager to begin.

Main Report

Background

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

2. All support for SharePoint 2010 [the current website platform] will cease in Summer 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.

3. 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.

Current Position

4. The project went out to tender in August with evaluations in September 2018. The results of these evaluations went to the IT Category Board on 9 October. The award was made to the supplier following the Gateway 5 report. This has let the project commence and has released the funding.

5. The contract has been let under the Crown Commercial Services framework, G-Cloud 10. The call off contract has been agreed with the successful supplier following the approval of the Gateway 5 report. The new supplier, Zengenti. will commence the initial phases of the project during January 2019 in line with the outline project plan.

6. The discovery phase next steps are
    a. talk to internal and external stakeholders
    b. establish user needs
    c. establish business requirements.

7. Members will be asked to participate in the discovery phase and in user testing. This will contribute to how the site is designed and the testing of its functionality.

8. A dedicated Project Manager is currently being recruited now that funding has been released.

9. This allows 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.

Conclusion

10. Members are asked to note the report.

Melissa Richardson
Digital Publishing and Content Strategy Lead

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

Committees: Corporate Projects Board *[for information]* *Projects Sub [for Decision]* Digital Services Sub *[for information]*		**Dates:** 17 December 2018 18 January 2019 4 February 2019
Microsoft Licencing and Cloud productivity suite (Office 365)	**Unique Project Identifier:** 117937	**Outcome Report** **Approval Route** **Regular**

PUBLIC

Summary

[S1] Key conclusions

The Scheme delivered against the core deliverables as set out below. It has provided a significant uplift in the capability of the IT for Corporation staff and Members. Significantly the solution provides greater opportunity for agile working, business continuity and collaboration. Overall the programme was positively received by the user community. Effective working relationships and a “one team” ethos was evident between Corporation IT Division and the as the delivery partner.

The success of the scheme has been acknowledged with the Project having been shortlisted for the Local Government Chronicle Awards.

- Office365 business case with options for on premise and cloud-based solutions.
- Definition of active users and documented analysis of user population
- Definition of user journeys documented and alignment to future requirements for New Ways of Working.
- Phoenix appointed as our Microsoft Large Account Reseller
- 2996 users migrated to O365 Mail
- 2996 users migrated to OneDrive
- 936 users migrated from Good to Intune
- Legacy SharePoint upgraded to SharePoint online
- New Intranet solution deployment on SharePoint online
- Transition to support and supporting KPIs
- Modern platform enabling business collaboration
- The spend against the approved budget of £965k is £963k

[S2] Key Learning and Recommendations

As part of the IT Strategy an Office 365 business case was produced and signed off with Members to move Exchange, SharePoint and user data to Office 365.

Multiple options were analysed, and Office 365 delivered the greatest return on investment at the lowest capital outlay compared to retaining the service on premise or moving to the cloud. Infrastructure to support the Office 365 migration was setup.

Mailbox data and Public folder data was migrated to Office 365. The Exchange, Enterprise Vault and associated data on premise and in IaaS was fully decommissioned.

New SharePoint architecture and configuration implemented. New Intranet implemented and retained content was fully migrated.

All user data was migrated to OneDrive. The new environment created was documented and handed into support.

[S3] Decisions required

Members are asked to approve the content of this Outcome Report, note the lessons learned, and the close the project.

Main Report

Design & Delivery, Variation and Value:	
Design & Delivery Review-	
[1] Design into Delivery	*Did the Design of the project adequately prepare for the Delivery of the project? If not, what elements could have been better designed?* The project followed Microsoft best practice principles. These involved a High level design phase a Detailed design phase, a pre-pilot phase, a pilot phase, and finally a live deployment of the end to end solution.
[2] Options appraisal	*Did the option chosen allow the project to meet the project's objectives and provide long term value?* *Were any compromises or changes made against the options approved (i.e. Scope or time changes)?* The project progressed in line with the recommended option at Gateway 5.
[3] Procurement Route	*If services were procured, what was/were the method(s) used to procure them? (framework, open tender etc.) Did this work or were revisions required.* Implementation services were acquired via the IT Managed Servicers contract with Agilisys, which provided for a complaint procurement process.
[4] Skills base	*Did the City of London project team have the required skills and experience to deliver the project? Were external resources or training required, or new staff brought in?* A project team was established. This was a mix of specialists from the IT Managed Service, as specialised from the retained CoL IT function. CoL provided a client-side lead to work alongside the delivery partner. This approach worked well as was identified as a strength by the external assurance process
[5] Stakeholders	*Were stakeholders engaged and managed well, were they satisfied with the conclusion?* A Chief Officer group provided executive oversight to the programme. Members were also engaged by way of a workshop and regular progress reporting to IT Sub and Projects Sub. Extensive engagement was carried out throughout the project. An active user group set up, with representatives from across the business. Further-more a change manager oversaw a detailed change and engagement plan. This used a variety of media to communicate the change and training aspects. The use of dedicated "floor walkers" to support the roll-out was also well received by end users during implementation. External assurance was also sought from specialised third parties, which highlighted a successful approach to delivery.
[6] Closing RAG rating	

	<table><tr><td>Project Risk Assessment</td><td>Low</td></tr><tr><td>Project RAG rating</td><td>Green</td></tr></table>
[7] Positive reflections	**1.** The O365 Programme has successfully delivered a much-improved technology platform broadly on time and to budget. **2.** The number of delivery issues impacting users appears to have been low for a programme of this type. **3.** User engagement and communication was generally good. **4.** The Programme appears to have developed considerable goodwill among the business user community. **5.** There was strong senior officer and Member sponsorship and engagement with the Programme. **6.** A core programme team was established with a mix of internal, supplier and external staff. Joint working was with the Corporation and supplier community was very good. **7.** A pragmatic approach was taken to management of the programme, with an appropriate mix of formal process and more agile techniques. **8.** There was a strong focus on delivering at pace. **9.** Excellent joint working practices were embedded across between CoL and the Delivery partner. **10.** This benefited from an able external programme director and strong alignment with the client programme lead.
[8] Improvement reflections	*What didn't work so well within the design and delivery arrangement.* Poor quality base data in terms of asset management, user data, and user cases impeded the progress of the programme. This requires procedures to ensure all assets are correctly recorded and tracked. The absence of IT policies and standards meant that such items needed to be defined by the programme team.
Variation Review-	
[9] Assessment of project against key milestones	*Please provide a short assessment of progress against key milestones, during the project's design and delivery.* The project followed a tested methodology, and utilised specialist on-boarding support from Microsoft. This helped to maintain momentum and enabled a "fast track" resolution to technical issues associated with the migration.
[10] Assessment of project against Scope	There were no significant scope changes required post GW5.
[11] Change	There were no significant scope changes required post GW5.

<table>
<tr><td>[12] Risks and Issues</td><td>Did identified risk occur, if so, what was the effect?
Did unidentified risks occur, what were their impact?

Yes, identified risk did occur, and mitigation plans reduced the impact. For examples failed deployment visits were factored into the resourcing model.

Unidentified risks did materialise, for example the level of communications and engagement resource was greater than originally planned for. Management action mitigated any adverse impact on delivery and operations.</td></tr>
<tr><td>[13] Transition to BAU</td><td>Did the project have a clear plan for transfer to operations / business as usual? Did this work well?

A detailed transition plan was defined, and early engagement was undertaken with the support partner. Despite this service transition to support took longer than had been planned for. Early “life support” was provided by the project team. This was in part due to a delay in transitioning support staff to new roles, and the impact of bedding in new operational policies.</td></tr>
<tr><td colspan="2">Value Review</td></tr>
<tr><td>[14] Budget</td><td>
<table>
<tr><td>Budget envelope at Gateway 2:</td><td>£250k-£5millon</td></tr>
</table>
<table>
<tr><td></td><td>At Authority to Start work (G5)</td><td>At Completion</td></tr>
<tr><td>Fees</td><td>£ 965k</td><td>£ 963k</td></tr>
<tr><td>Total</td><td>£965k</td><td>£963k</td></tr>
</table>
Licence fees associated with O365 are met through IT Division revenue budget.

*If ‘Other’ provide a brief note on the contents

Please confirm whether or not the Final Account for this project has been verified.*

*Please note that the Chamberlain’s department Financial Services division will need to verify Final Accounts relating to medium and high-risk projects valued between £250k and £5m and all projects valued in excess of £5m. All Final accounts which exceed £50,000 in value will be subject to an independent verification check, undertaken by a suitably experienced officer within the relevant implementing department, regardless of whether the overall risk of the project has been assessed at some point as low, medium or high risk,

In addition, final accounts of £2,000,000 and above will also be subject to final account verification by the Chamberlain’s Financial Services Division (FSD) where (I) the value is £2,000,000 to £10,000,000 and the overall risk of the project has been assessed at some point as “Medium” or “High”, and (ii) the value exceeds £10,000,000 regardless of the risk assessment.
</td></tr>
</table>

[15] Investment

If this project was an invest to save or revenue generating opportunity, what were the expected returns (At Authority to start work stageG5)?
What returns have been made so far, are these in line with initial expectations?

The original business case identified benefits as a consequence of the move to O365 at a value of £233,000. As a result of a business decision to retain an archive of data that the original business case assume would be deleted, an additional data storage of 13TB will now remain (in a low-cost archival storage solution at £5k p.a). The opportunity remains open to review the need for the retention of this data at future date. At which point further saving could be realised.

Area	Business Case	Actual	Delta
Servers decommissioned (Email & SharePoint)	40	41	1
Email volume migrated	15TB	16.9TB	+1.9TB
SharePoint data migrated	5TB	3.8TB	-1.2TB
Home drive to OneDrive data migrated	10TB	12.1TB	+2.1TB
Data being archived	0	13.38TB	13.38TB
Cost saving (£k) based upon total excluding licensing	-£233,000	-236,900	+3,900

Based upon a full year cycle.

[16] Assessment of project against key measures of success

Did the project deliver against its key measures of success?

- Defining the end to end technology solution

The project delivered a review of the technology stack and defined the future sate based upon adoption of Microsoft Cloud services.

- A design meets the IT strategy

The project delivered against the latest available Microsoft solution architecture. Making use of Cloud technologies to provide reliance and highly available core productivity services.

- Technology solutions that are aligned to industry standards and best practice

The project delivered against the latest available Microsoft solution architecture

- Technology aligned to business needs and requirements

Technology aligned to the core principles of the CoL IT Strategy specifically to "move from complexity to commodity.

[17] Assessment of project against SMART Objectives

Did the project deliver against its SMART objectives?

Compliant licensing model in place by end of current agreement. - Achieved
Licence model that better matches consumption and demonstrates value for money. - Achieved

[18] Key Benefits realised	• Enhanced and consistent user experience • Flexible working significantly enhanced • Consumption based user licensing • Future Email and SharePoint upgrades included • Enhanced functionality including instant messaging, Skype, OneNote • Robust security and reliability • Patching and maintaining email and SharePoint environments removed • Mail-box storage limits increased to 50GB per user • Savings are delivered by a reduction of 32 servers and 20TB of data in IaaS

Lessons Learned and Recommendations	
Lessons Learned-	
[19] General Purpose Review	*Are there any points of learning or improvements we can learn from this project?* *If the organisation attempted to deliver something similar what missteps could be avoided, or efficiencies realised?* **1.** The need to ensure that IT operate within a policy lead environment. **2.** That the asset and user data "cleansed" through the programme are maintained in line with the agreed policies. **3.** There is a need to define benefits in both qualitative and qualitative terms, with measurements which explicitly demonstrate the business benefits. **4.** Poor quality base data in terms of asset management, user data and user cases impeded the progress of the programme. **5.** The absence of policy and standards meant that such items needed to be defined by the programme team. **6.** Transition to support was hampered by a lack of awareness and engagement with operational teams and the service provider.
[20] Learning sharing and use	*How will learning from this project be shared and used in the future?* 1. Lessons learned will be shared via the IT Project management community TeamSite.
Recommendations-	
[21] Recommendations	*Are there any recommendations that could be made to aid the process of designing and delivering future similar projects?* *1.* Please see lessons learned above. Specifically, the need to define clear and measurable benefits (both tangible and in-tangible) would make for a stronger business case and drive the project to deliver the appropriate outcomes.

[22] AOB	1. The project formed part of the IT Transformation Programme and was featured as a case study of successful O365 deployment by Microsoft 2. The Programme has also been shortlisted for the Local Government Chronicle Awards 2018.

Decisions required
If any decisions are required in addition to the approval of this outcome report, please describe them here:
N/a

Appendices

Appendix 1	Project Coversheet
Appendix 2	
Appendix 3	

Contact

Report Author	Kevin Mulcahy
Email Address	Kevin.mulcahy@cityoflondon.gov.uk
Telephone Number	0207 1133713

Project Coversheet

[1] Ownership

Unique Project Identifier: 11793 **Report Date:**03/12/2018
Core Project Name:
Microsoft Licencing and Cloud productivity suite (Office 365)

Programme Affiliation (if applicable): IT Transformation Programme
Project Manager: Kevin Mulcahy
Next Gateway to be passed: Gateway 6

[2] Project Brief

Project Mission statement:

- Move current licensing to subscription based onto Microsoft Office 365 subscription consisting of full desktop version of Office products, Windows, Client Access Licenses (CAL's), Hosted Exchange and SharePoint Office 365.
- Migrate users email and SharePoint to the Cloud
- Decommission current environments in IaaS

Definition of need:
The project objective was to migrate CoL to a "best in class" modern Cloud based technology solution based upon Microsoft technology, utilising Office 365.
Key measures of success:

1) Enhanced functionality including instant messaging, Skype, OneNote
2) Flexible working significantly enhanced
3) Mail-box storage limits increased to 50GB per user

[3] Highlights

Finance:
Total anticipated cost to deliver [£]:£965k
Total potential project liability (cost) [£]: £965k
Total anticipated on-going commitment post-delivery [£]:
Programme Affiliation [£]:

Do not use ranges in this table. Either Highest range value or best estimate at this time.

[A] Budget Approved to Date*	[B] New Financial Requests	[C] New Budget Total (Post approval)
£965k	Nil	£965k
[D] Previous Total Estimated Cost of Project	**[E] New Total Estimated Cost of Project**	**[F] Variance in Total Estimated Cost of Project (since last report)**
£965k	£963k	(£2k)
[G] Spend to Date	**[H] Anticipated future budget requests**	

£963k	Nil

Headline Financial changes:

Since 'Project Proposal' (G2) report:
◄► Order of magnitude costs provided at GW2. £250k-£5million.
Since 'Options Appraisal and Design' (G3-4) report:
▼ Combined GW3/4/5 Report submitted with a cost of £965k
Since 'Authority to start Work' (G5) report:
◄► Combined GW3/4/5 Report submitted with a cost of £965k

Project Status:
Overall RAG rating: Amber
Previous RAG rating: Amber

[4] Member Decisions and Delegated Authority

None

[5] Narrative and change

Date and type of last report:
Update Report to IT Sub – September 2018
Key headline updates and change since last report.
Project has delivered all required components.

Headline Scope/Design changes, reasons why, impact of change:

Since 'Project Proposal' (G2) report:
CoL Intranet upgrade to SharePoint online in-scope.
Since 'Options Appraisal and Design' (G3-4 report):
None
Since 'Authority to Start Work' (G5) report:
None

Timetable and Milestones:
Expected timeframe for the project delivery: Project completed
Milestones:

1) Renew Microsoft agreement utilising O365 suite
2) Design new environment by
3) Migrate all users by

Are we on track for this stage of the project against the plan/major milestones? Yes
Are we on track for completing the project against the expected timeframe for project delivery? Project Completed

Risks and Issues
Top 3 risks:

Risk description	Transition to new support model
Risk description	People and Behaviours not aligned to new model.
Risk description	Business case not achievable.

See 'risk register template' for full explanation.

Top 3 issues realised

Issue Description	Impact and action taken	*Realised Cost*
Transition to Support	Inability of service to fully support new capabilities.	
Retention of legacy date	Low cost storage solution provisioned.	£5k

Has this project generated public or media impact and response which the City of London has needed to manage or is managing?
None.

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

Document is Restricted

This page is intentionally left blank

Document is Restricted

This page is intentionally left blank