



Digital Services Sub (Finance) Committee

Date: FRIDAY, 24 JANUARY 2020
Time: 1.45 pm
Venue: COMMITTEE ROOMS - WEST WING, GUILDHALL

Members: Randall Anderson (Chairman)
Deputy Jamie Ingham Clark (Deputy Chairman)
Deputy Keith Bottomley
Tim Levene
Jeremy Mayhew
Rehana Ameer
Deputy Hugh Morris
Deputy Roger Chadwick
Benjamin Murphy
John Chapman
Sylvia Moys
Barbara Newman
James Tumbridge

Enquiries: Rofikul Islam
Tel No: 020 7332 1174
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 Friday, 1 November 2019.

For Decision
(Pages 1 - 6)
4. **OUTSTANDING ACTIONS FROM PREVIOUS MEETINGS**
Joint report of the Town Clerk and the Chamberlain.

For Information
(Pages 7 - 8)
5. **DESIGN, BUILD, SUPPORT AND HOSTING FOR NEW WEBSITE**
Report of the Town Clerk (Director of Communications).

For Information
(Pages 9 - 12)
6. **DIGITAL TECHNOLOGY IN THE CITY SURVEYOR'S DEPARTMENT**
The City Surveyor's Department to be heard.

For Information
(Pages 13 - 24)
7. **2020 IT MANAGED SERVICES UPDATE**
Report of the Chamberlain.

For Information
(Pages 25 - 30)
8. **CITY OF LONDON CORPORATION INFORMATION HANDLING (PROTECTIVE MARKING)**
Joint report of the Comptroller and City Solicitor and the Chamberlain.

For Information
(Pages 31 - 34)
9. **ORACLE ERP STRATEGY - INTERIM PAPER**
Report of the Chamberlain.

For Information
(Pages 35 - 38)

10. **IT DIVISION - IT SERVICE DELIVERY SUMMARY**
Report of the Chamberlain.
For Information
(Pages 39 - 46)
11. **IT DIVISION - CHANGE MANAGEMENT SUMMARY**
Report of the Chamberlain.
For Information
(Pages 47 - 52)
12. **IT DIVISION RISK UPDATE**
Report of the Chamberlain.
For Information
(Pages 53 - 62)
13. **CR 16 INFORMATION SECURITY RISK**
Report of the Chamberlain.
For Information
(Pages 63 - 74)
14. **QUESTIONS ON MATTERS RELATING TO THE WORK OF THE SUB COMMITTEE**
15. **ANY OTHER BUSINESS THAT THE CHAIRMAN CONSIDERS URGENT**
16. **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

17. **NON-PUBLIC MINUTES OF THE PREVIOUS MEETING**
To agree the non-public minutes of the meeting held on Friday, 1 November 2019.
For Decision
(Pages 75 - 80)
18. **CR 16 INFORMATION SECURITY RISK**
Report of the Chamberlain.
In conjunction with item 13.
For Information
(Pages 81 - 102)

19. **LAN AND WAN CIRCUIT RENTAL FOR CITY OF LONDON POLICE FOR ANPR CIRCUITS, FIREWALLS AND CORPORATE NETWORK**
Report of the Chamberlain.

For Decision
(Pages 103 - 108)
20. **POLICE DEEP DIVE EMERGENCY SERVICES NETWORK**
The Commissioner of the City of London Police to be heard.

For Information
(Pages 109 - 118)
21. **IT DISASTER RECOVERY TESTING PLAN FOR 2020**
Report of the Chamberlain.

For Information
(Pages 119 - 124)
22. **CORA PPM (CORPORATE PROJECT MANAGEMENT SOFTWARE)**
Report of the Town Clerk.

For Decision
(Pages 125 - 138)
23. **FREEMEN'S SCHOOL MANAGED IT INFRASTRUCTURE SERVICE**
Report of Roland Martin, Headmaster and Chief Officer.

For Information
(Pages 139 - 146)
24. **NON-PUBLIC QUESTIONS ON MATTERS RELATING TO THE WORK OF THE SUB COMMITTEE**
25. **ANY OTHER BUSINESS THAT THE CHAIRMAN CONSIDERS URGENT AND WHICH THE SUB COMMITTEE AGREE SHOULD BE CONSIDERED WHILST THE PUBLIC ARE EXCLUDED**

DIGITAL SERVICES SUB (FINANCE) COMMITTEE

Friday, 1 November 2019

Minutes of the meeting of the Digital Services Sub (Finance) Committee held at the Guildhall EC2 at 1.45 pm

Present

Members:

Randall Anderson (Chairman)	Deputy Hugh Morris
Deputy Jamie Ingham Clark (Deputy Chairman)	John Chapman
Deputy Keith Bottomley	Barbara Newman
Rehana Ameer	James Tumbridge

Officers:

Rofikul Islam	- Town Clerk's Department
Sean Green	- Chamberlain's Department
Kevin Mulcahy	- Chamberlain's Department
Ryan Dolan	- Town Clerk's Department
Matt Gosden	- Chamberlain's Department
Sam Collins	- Chamberlain's Department
Samantha Kay	- Chamberlain's Department
Andrew Carter	- Community and Children's Services
Mohammed Hussain	- Community and Children's Services
Gary Brailsford-Hart	- City of London Police
John Awosoga	- City of London Police
Graeme Quarrington-Page	- Chamberlain's Department

In attendance:

Asif Iqbal	- Agilisys
Anthony Byrne	- Agilisys

1. APOLOGIES

Apologies were received from Jeremy Mayhew, Deputy Roger Chadwick and Sylvia Moys.

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

There were no declarations.

3. MINUTES OF THE PREVIOUS MEETING

RESOLVED: That the public minutes of the meeting held on Tuesday 8 October 2019 be approved as an accurate record, subject to the changes suggested by the Digital Publishing and Content Strategy Lead and Sylvia Moys.

4. **FORWARD PLAN**

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

RESOLVED – That the Sub Committee notes the report.

5. **OUTSTANDING ACTIONS FROM PUBLIC MINUTES OF PREVIOUS MEETINGS**

The Sub Committee received a joint report of the Town Clerk and the Chamberlain outlining outstanding action from the previous meetings. The current outstanding action points are to be completed by the next meeting.

RESOLVED – that the Sub Committee notes the report

6. **COMMUNITY AND CHILDREN'S SERVICES - TECHNOLOGY OVERVIEW**

The Sub Committee received a verbal update and presentation of the Director of Community and Children's Services on his Department's use of Technology.

Members were informed that the department has 14 housing offices managed by the City of London across different locations. The Department was one of the early adopters of agile working, as part of its business continuity and reduction in travel time for staff.

The Director spoke of the success of using the MOMO App, which has enabled the City of London to engage with its younger generation of residents. The MOMO App allows the young people to tap into the department resources in an innovative way. Although the Department uses its technology to advance its objectives, it is also mindful of the fact that the human touch needs to be visible when dealing with vulnerable residents.

Members were further informed that the new Housing Management System will allow advanced usage. The system will allow the use of social media to act as a sign posting service and will enable improved business intelligence. Furthermore, the new system will allow residents to access a range of services through self-services online.

The Director spoke of the need for moving away from being paper based and allow room for innovation and growth. An example of the need for innovation is the current system to book any of the City of London's Community Rooms. Currently a hirer has to call into a dedicated phone line to check its availabilities. A paper booking form is completed, and an approval process is engaged. If charges are incurred, an invoice is prepared. All of this is expensive and needlessly complex. Going forward the Department would like to be able to allow its customers to check availabilities, make bookings and pay for the room booking via an online system.

A Member asked how the department measured its targets and effectiveness. The Sub Committee was informed that at present the Department is looking at

mapping out customer processes and customer requirements. This work which will take a further 3 months will better inform the targets and measures the department develops to measure effectiveness.

A Member queried how much of Artificial Intelligence (AI) can the City of London embrace to provide a better service. The Committee was informed that using AI technology is on the roadmap, but we are not making use of any AI systems currently.

The Sub Committee was advised that the City of London has information sharing agreements with relevant partners to improve the integrated and joined up service that can be provided to customers. The City of London continues to learn from others and shares its own good practices too.

RESOLVED – That the Sub Committee notes verbal update.

7. **CITY OF LONDON CORPORATION INFORMATION MANAGEMENT METRICS**

The Sub Committee considered the report of the Comptroller and City Solicitor on the City of London Corporation Information Management Metrics. It was noted that quarterly reports on the matter should be provided to the Sub Committee.

A Member asked who is driving the information management strategy forward. The Sub Committee was informed that the Comptroller and City Solicitor is the Senior Information Risk Owner (SIRO) for the City of London and as such in his capacity he has set up an Advisory Group on Information Management that jointly developed the Information Management strategy. The strategy is a Corporate strategy and is owned by the Town Clerk. The Sub Committee was further informed that the Advisory Group consists of Lead Officers from various Departments within the City of London and City of London Police.

RESOLVED – That the Sub Committee approves the report and the draft metrics documented in Appendix B.

8. **CITY OF LONDON CORPORATION INFORMATION MANAGEMENT PROTECTIVE MARKING**

The item was withdrawn from the agenda, pending a decision from the Summit Group.

9. **IT SERVICE DELIVERY UPDATE**

The Sub Committee received a verbal update of the Deputy Director of IT and the Agilisys Service Director on the IT service delivery update.

The Committee was informed that present the service performance maintains a high-level satisfaction. There were several P1 and P2 category issues reported in the period. Any P1 issue is documented with a lesson learned report.

The Sub Committee was further advised that there will be a forensic security check on the City of London's IT network to support the application that the City of London prepares for the annual PSN service provision certificate due in April 2020.

RESOLVED – That the Sub Committee notes the report.

10. **IT RISKS**

The Sub Committee received a verbal update of the Director of IT on the IT risks. There were not material changes in IT risks since the last meeting of the Sub-Committee. The Director of IT noted that the Mazars GDPR Compliance Review draft audit report undertaken in July & August 2019 was received in September 2019 and reviewed by the Data Protection Officer for the City of London and C&CS Information Compliance Manager.

The draft audit report rated GDPR compliance as amber 'an adequate control framework is in place but there are weaknesses and or a lack of compliance which may put some system objectives at risk'.

Some suggested amendments to the report findings were made and the revised report is awaited, the core findings and recommendations remain unchanged. Further updates on this corporate risk will be provided to the Sub-Committee at future meetings.

RESOLVED – That the Sub Committee notes the report.

11. **WINDOWS 7 MIGRATION AND EXTENDED SUPPORT**

The Sub Committee received the report of the Chamberlain on the Windows 7 Migration and Extended Support. The Sub Committee was informed of the plans to remediate the remaining applications prior to the end of Windows 7 support in January 2020.

The Sub Committee stated that it did not expect to any see Windows 7 devices left on the City of London network by the end of the Windows 7 support in January 2020.

RESOLVED – That the Sub Committee notes the report.

12. **THE CASE FOR A SECURITY OPERATING MODEL**

The Sub Committee received the report of the Chamberlain the case for a Security Operating Model.

Members were informed that the report presented before them is to formalise the IT Security management processes and ensure that IT security is provided to the City of London within a programme of continuous improvement to protect the organisation and sufficiently mitigate the Corporate IT Security risk CR16.

RESOLVED – That the Sub Committee;

- Support the development of a Security Operating Model; and
- Endorse the identified measures within the 10 steps gap analysis.

a) **Formalisation of Governance Structure to Support Senior Information Risk Owner (SIRO) and Information Management Risk Appetite**

Item 19 was moved to the Public Session of the meeting thus seen as 12.1.

The Sub Committee received the report of the Chamberlain on the case for a Security Operating Model.

The Sub Committee was advised that one of the key roles in the organisation is that of the Senior Information Risk Owner (SIRO) currently held by the Comptroller. To assist the corporate SIRO all Chief Officers in the City of London have agreed to take on local SIRO roles in their departments.

Members were further informed that data retention schedules are in place with all departments across the City of London. This allows the City of London to dispose of information when it is no longer required and retain information only for as long as it is necessary ensuring we comply with the Data Protection act. Additionally, a new Records Management policy has been agreed by Chief Officers to support the enforcement of good records management practices across the City of London.

RESOLVED – That the Sub Committee notes the report and the updated Records Management Policy Appendix C.

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

There were no questions.

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

There were no items of urgent business.

15. **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.

The meeting closed at 15:40

Chairman

Contact Officer: Rofikul Islam
Rofikul.islam@cityoflondon.gov.uk

This page is intentionally left blank

Digital Services Sub (Finance) Committee – Outstanding Actions (Public)

Item	Meeting Date	Action and target for completion	Officer responsible	To be completed/ Next stage	Progress update
10	24 January 2020	IT Risks Amendments to the report findings were made and the revised report is awaited, the core findings and recommendations remain unchanged. Further updates on this corporate risk will be provided to the Sub-Committee at future meetings.	Sam Kay	January 2020	Updated IT risks report on the agenda

This page is intentionally left blank

Committee(s)	Dated:
Digital Services Sub Committee	24/01/2020
Subject: Design, build, support and hosting for new website	Public
Report of: Town Clerk (Director of Communications)	For Information
Report author: Melissa Richardson, Digital Publishing and Content Strategy Lead, Communications, Town Clerks	

Summary

This report is to keep Members updated on the progress of the website project.

This went out to tender in summer 2018 and the suppliers, Zengenti, were appointed in November 2018. A Project Manager was appointed in March 2019.

Both the Build and the Testing & Training phases are almost complete at the time of writing. The Content Creation phase is underway, with quality assurance to follow.

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 October 2020 (regular support stopped in 2015). SharePoint will not be providing a platform for external sites in future, so it cannot simply be updated. Leaving our website an unsupported platform poses a major risk.
3. Our current website does not display well on mobile devices, is not task structured (i.e. lacking user focus) and the out of the box search engine cannot provide the results from across the full range of corporate information (i.e. Member, Jobs and Media sites are separate) that users would expect.

Current Position

4. The new supplier, Zengenti, began the initial phases of the project during January 2019 in line with the outline project plan. They favour an Agile working practice [collaboration at every stage incorporating improvements]

and have undertaken simultaneous design, build and testing.

5. A Project Manager was recruited in March 2019.
6. Discovery and Design phases are complete.
7. Build and the Testing & Training phases are almost complete. The Build phase has been run in tandem with testing so that any issues could be addressed as part of the build. 107 editors have been trained across the organisation and they are now creating the content that was agreed as a priority for launch in the content audit.
8. The search engine is now functional and the final stage of integrating the Jobs data is underway.
9. The next steps will be ensuring all the audited content has been recreated and then undergoing a number of quality tests.

Conclusion

10. The new supplier, Zengenti, began work in early 2019. Based on previous experience, this will allow a realistic amount of time for building and testing to ensure the new site is ready before October 2020.

The project has a green status and currently is on time, on budget and within scope.

Melissa Richardson

Digital Publishing and Content Strategy Lead

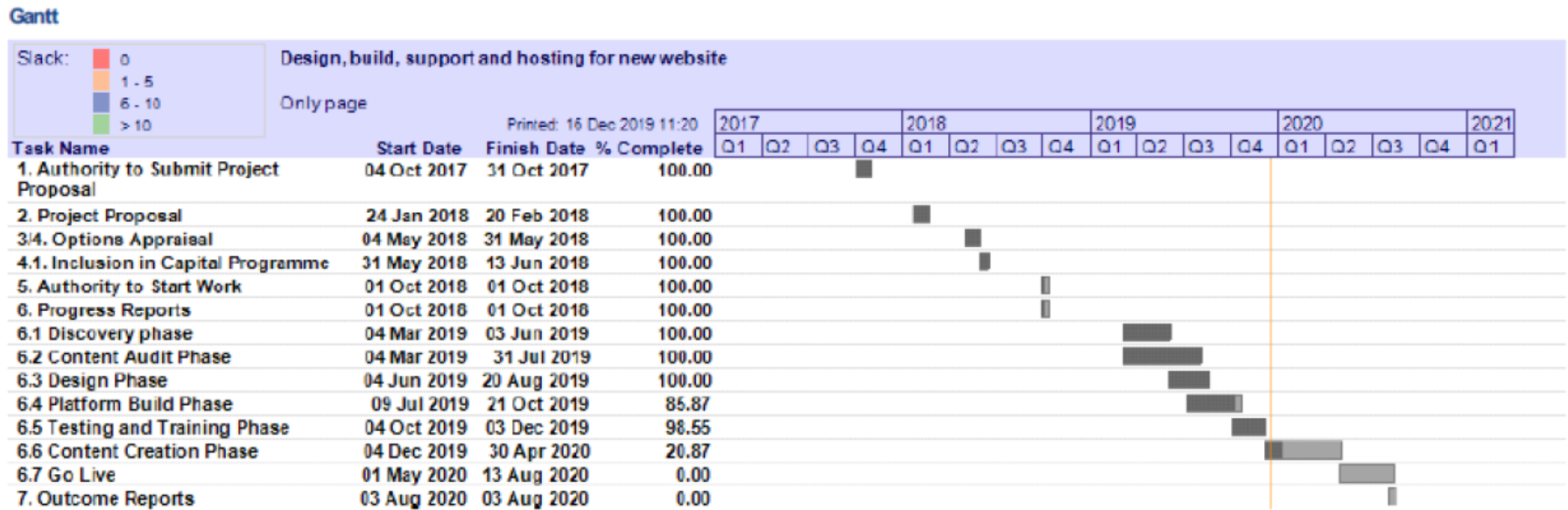
T: 020 7332 3449

E: melissa.richardson@cityoflondon.gov.uk]

Appendix A – Project Update Gantt Chart

Appendix A - Project Update Gantt Chart

Project Update Gantt Chart – Appendix A



This page is intentionally left blank

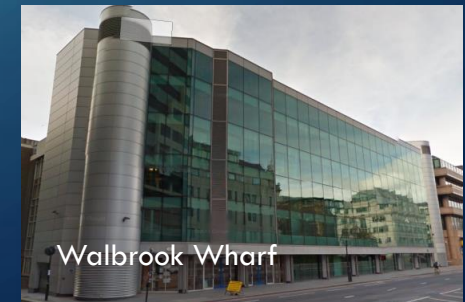


DIGITAL TECHNOLOGY IN THE CITY SURVEYOR'S DEPARTMENT

DIGITAL SERVICES SUB-COMMITTEE

JANUARY 2020

CITY SURVEYORS DEPARTMENTAL STRUCTURE



PROPERTY MANAGEMENT

- **Oracle Property Management Module (OPN)** since March 2015; contains circa 820 properties, 1 235 buildings and is essentially used to manage leases and rent income.
- Benefits:
 - Cheaper than other Property Management Systems on the market
 - Integrated with Oracle Financial
- Challenges:
 - Services charges can't be efficiently managed via this system
 - Limited Property Management Functionalities, no valuation, limited to a small number of customised reports
- Plans for the future:
 - Electronic Invoicing
 - Management Dashboards for Asset managers.
 - The next version of Oracle from 2023 will be a major change with a cloud version which will not include the property management module.

FACILITIES MANAGEMENT (1)

- **MICAD** was implemented in 2017 for managing repairs and maintenance and includes Asbestos and Legionella compliance modules.
- 803 buildings recorded on MiCAD, representing 1722 floors; 924 floor plans have been uploaded so far (54%).
- 26,783 jobs reported for the last 12 months; phone calls to Property Service Desk have dropped by 5000 since launch of the Customer Portal.
- Benefits:
 - Integrated customer portal.
 - Management information extracted has benefited the Facilities management team to discover hotspots of faults.
 - Compliance documents housed in central point.
 - Jobs are assigned to engineers by the system on mobile devices.

FACILITIES MANAGEMENT (2)

- Challenges:
 - Data accuracy
 - Having up to date floors' plans is expensive and time consuming
 - Keeping accurate asset and compliance data is also resource intensive
 - Slowness of the system
- Plans for the future:
 - The end of contract with MiCAD will require to run a tender
 - Ideally, a link to the corporate financial system to better understand our costs and reduce these.

Desk Booking Screens

Create a great experience for every flexible workspace.



SMART WORKING

- Implementation of Hot desking for FM staff and extended for the move of all CSD office staff on 4th floor. (Condeco)
- Use of Tablet-laptops (Mix) for Project Managers in PPG
- Skype Screen in City Surveyor's meeting room

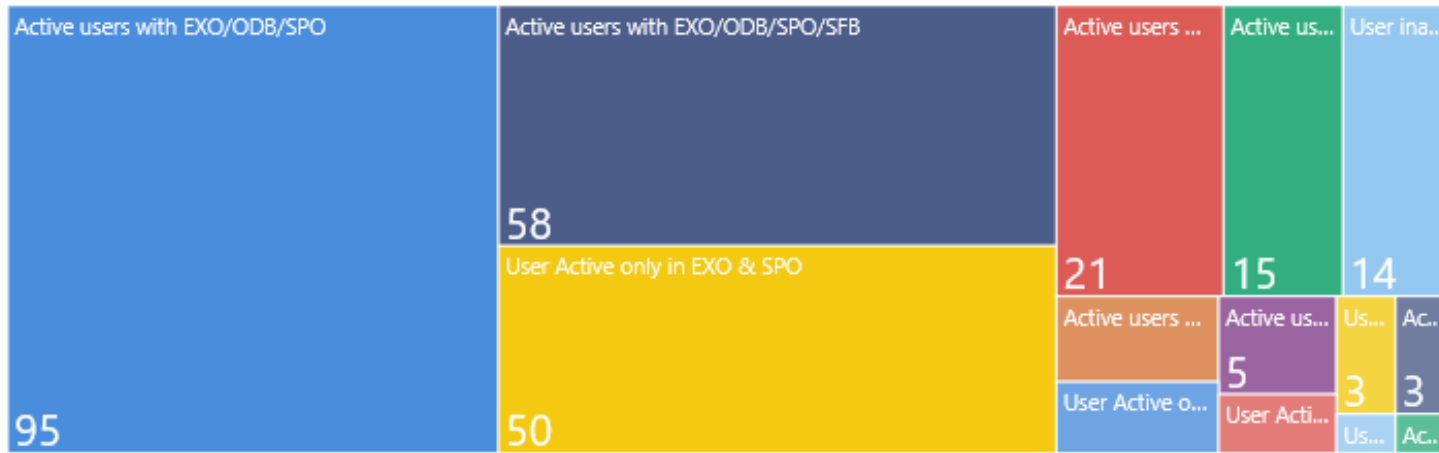
Meeting Room Screens

Display meeting bookings right outside the room.



DIGITAL ADOPTION DASHBOARD

Departmental Breakdown by Product Usage



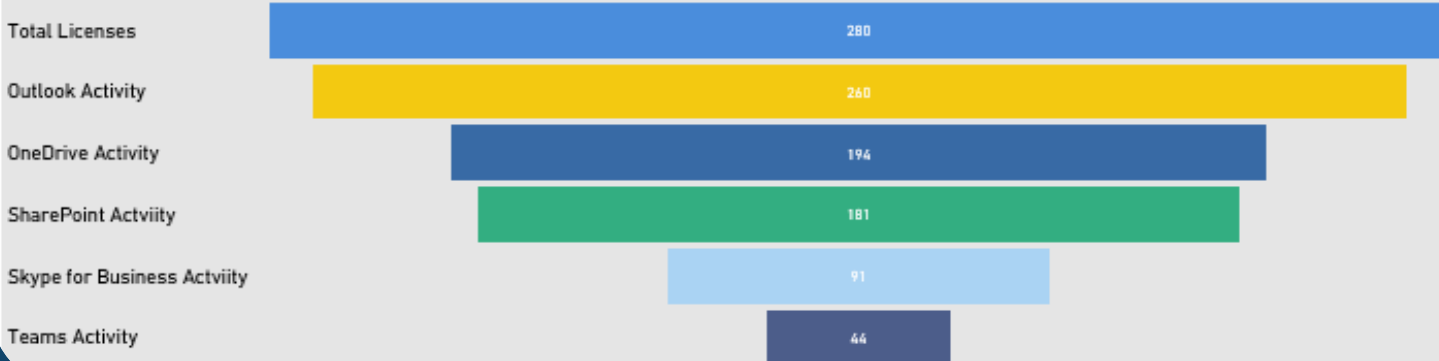
Department

City Surveyors

280
TotalUserCount

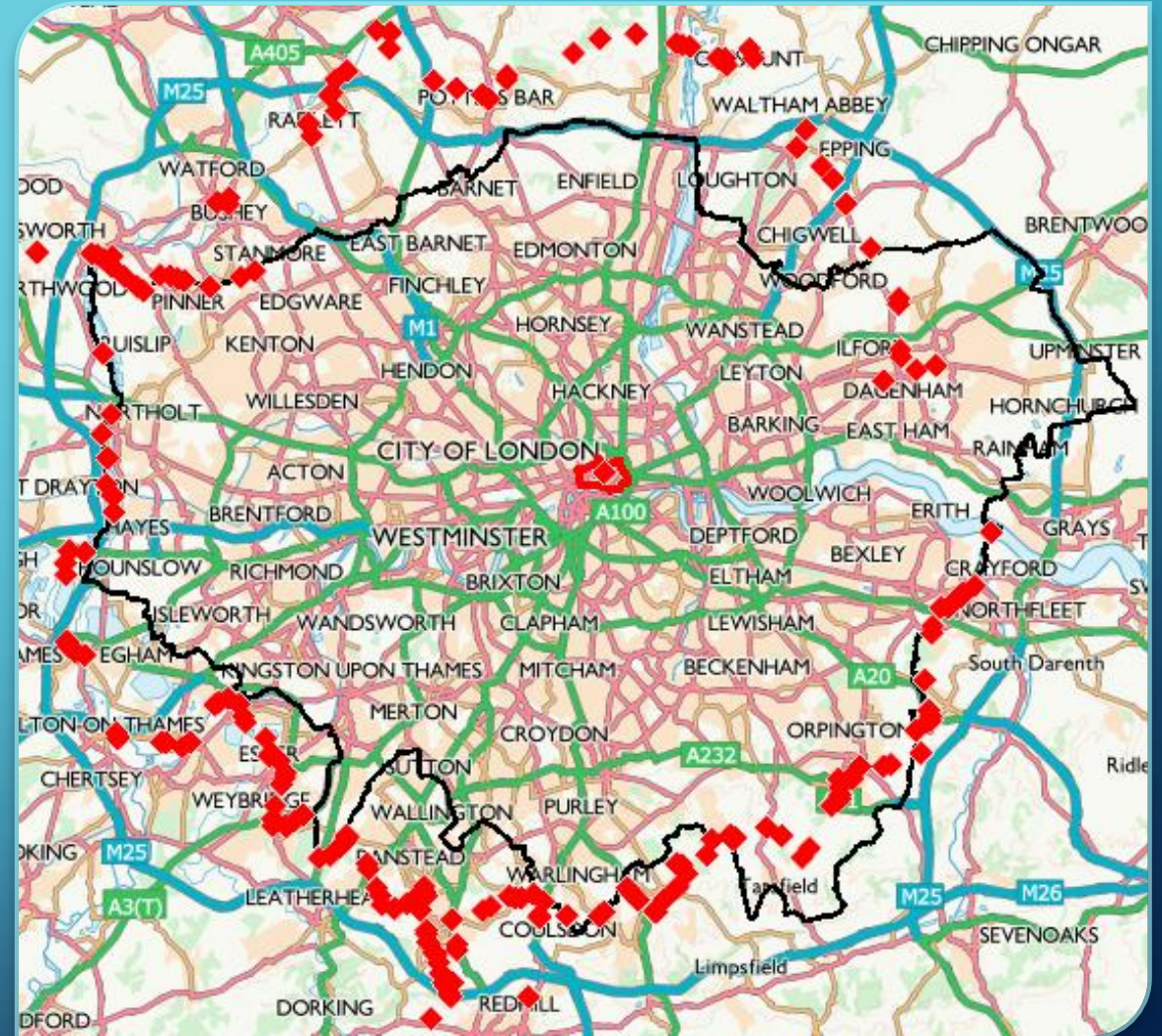
December 2019

Office 365 Activity by Product



OTHER EXAMPLES

- GIS: Coal Post
- AutoCAD (Computer Aided Design) software for architecture and mechanical design
- Historic Buildings have used technology extensively to understand the condition of the buildings it cares for. Use of a drone to check Guildhall roof conditions

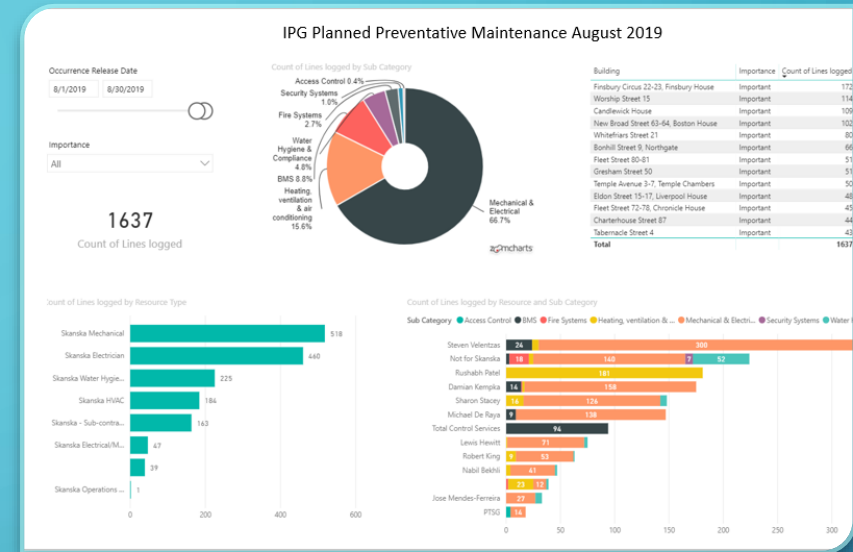


GIS: Red squares are Coal Posts – Black line marks the Greater London boundary (<https://www.mapping.cityoflondon.gov.uk>)

There are many more examples

CURRENT PROJECTS

- Use of PowerBi with MiCAD and for Risk Management
- Commercial Tenant portal with FIRMSTEP
- Radar survey at the London Wall Car Park (non-invasive method) to know more about the strength of the concrete slab



CHALLENGES

- Procurement and implementation of new property management system
- Data accuracy – get it right 1st time
- Make best use of our data (stored in various systems) to inform/speed up business decisions
- Automate simple/routine/time intensive tasks to free staff to focus on more added value/complex work.
- Digital education/ staff upskilling

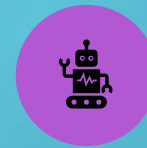
PLANS FOR THE FUTURE



Smart working



Digital by default



Automation



Business intelligence



Continuous improvement



Up-skilling



New, best of breed,
property
management system



Use technology to
inspect historic
buildings

Connecting people to accelerate innovation

Innovate UK
Knowledge Transfer Network

<https://ktn-uk.co.uk/>

Committee(s): Digital Services Sub – For Information	Date(s): 24 th January 2020
Subject: 2020 IT Managed Services Update	Public
Report of: Chamberlain	For Information
Report author: Kevin Mulcahy Assistant IT Director	

Summary

This report provides Members with an update on the IT 2020 Managed Service project.

Recommendation(s)

Members are asked to:

- Note the report.

Main Report

Background

1. On 15th May 2019, Procurement Sub-Committee approved the procurement strategy report (Stage 1) for the procurement of IT Managed Services for CoL, CoLP and London Councils.
2. The current contract expires 31st August 2020 and therefore a replacement needed to be procured to ensure IT services can be provided and maintained without interruption.
3. The IT Division has developed a new Service Design covering all IT services, including those to be provided in-house and by third party suppliers. This design reflects the current and future needs for a corporate IT service, covering the needs of the CoL and the CoLP.
4. The scope of the contract will cover the following core IT services currently provided by the incumbent supplier under the terms and conditions of the existing contract that ends 31st August 2020:
 - Service Desk and Field Engineering
 - End User Computing

- Operational system support and administration
 - Management of remotely hosted servers
5. The Service Design process identified certain services were best placed in-house, and the following elements of the IT Service will be brought back under direct control, which will involve transfer of 3 full-time posts under TUPE. The costs of these roles have been included in the cost comparisons.
6. Following the conclusion of a tender process through a further competition under the Crown Commercial Services (CCS) Framework for Technology Services 2 (RM3804) Lot 3, Agilisys, the current (incumbent) is the preferred bidder having achieved the highest score.

Current Position

7. Further to the recent competitive procurement process the preferred bidder will provide CoL, CoLP and London Councils with the following core IT services:
- Service Desk and Field Engineering
 - End User Computing
 - Operational system support and administration
 - Management of remotely hosted servers
8. A new service design has been developed with input from across the organisation. The service design reflects the needs of all organisations in scope, and includes:
- ITIL v4 aligned service model underpinning the delivery of future services
 - Implementation of ServiceNow IT service management tool, which will deliver:
 - Seamless integration within a multi-supplier, multi-service environment
 - Single interface for Azure cloud environment
 - Transparent configuration management system/CMDB across suppliers and services
 - An intuitive and modern self-service portal
 - Cloud management framework allowing rapid adoption of emerging services
 - Next generation service model with capabilities and capability to harness the evolving functionality in Microsoft 365, maintaining security and compliance
 - UK based location strategy with the optimal blend of onsite dedicated and leveraged resources
 - Creation of an on-premise 'technology support bar' delivering human-interactive support
 - Dedicated Service Delivery Managers for the Corporation and Police
 - User-experience centred customer service measurement framework

Programme Delivery

9. The programme has been structured into three workstreams each overseen by a senior manager acting in the capacity as a Senior Responsible Owner (SRO)
 - Exit Management
 - Transition
 - Target Operating Model and TUPE
10. In terms of programme management practice all project resources are professionally qualified to PRINCE2®. A dedicated SharePoint site being used to hold all documents to ensure effective document configuration management. This will be a shared repository with the supplier. A Master project plan with separate plans for each stream is currently being developed. However, there is a need to have a contract in place with the supplier to secure access to the required resources and to mobilise the full programme team. This is expected to take place in February 2020.
11. A dedicated and experienced transition manager has been appointed to lead the CoL resources to work alongside, and in partnership with the Agilisys transition team. A single RAID log and resource plan being developed in conjunction with the PMO.
12. Having completed all required governance, the focus of the project team is to now mobilise the new contract. The target date to complete the due diligence is February 2020.
13. Detailed discussions are required with Agilisys to determine the final position in relation to potential TUPE transfer of staff into the Corporation. This together with any staffing implications arising from the new target operating model will be subject to a report by the Director to the relevant committees.
14. In parallel with the commercial and contractual matters being concluded, detailed project plans will be developed for the three workstreams. In the meantime, all readiness work to onboard the new services are being undertaken, in particular the network links required to operate public cloud services within the Microsoft Azure environments.

Corporate & Strategic Implications

15. Provision of an effective and efficient corporate IT service is vital to the whole organisation. Currently, not all parts of the organisation use the Agilisys contract, but all core services use the infrastructure and associated IT services. Therefore, it is essential that a replacement service is provided ensuring business continuity.
16. The aims within the Corporate Strategy are underpinned by IT systems and services, and any replacement service must ensure these aims continue to be fully supported.

Implications

17. Awarding the contract will enable the following benefits to be delivered during its initial term:

- Move to public cloud (Microsoft's Azure service) for lower cost data storage and server hosting. Once this is completed, any new service contract will not need to move systems and data again. This move will enable further cost savings once an information management policy is fully adopted.
- Implementation of a Tech Desk at Guildhall and a Police site to allow staff to drop-off and collect equipment and get a face-to-face problem resolution and advice service.
- Revised and improved SLA and consequence regime for failure to deliver services within the SLA.
- Improved balance of outsourced and in-house services which will deliver efficiencies and service improvements to customers.
- Revised Social Value offering better aligned to latest organisational policies.

Conclusion

18. Good progress has been made in delivering this work to plan, to date. The programme remains on target and within budget.

19. The full delivery of the transition and migration will further strengthen the end user experience and drive greater value on efficiency in support of the objectives of the fundamental review.

Appendices

- Appendix 1 – Outline plan

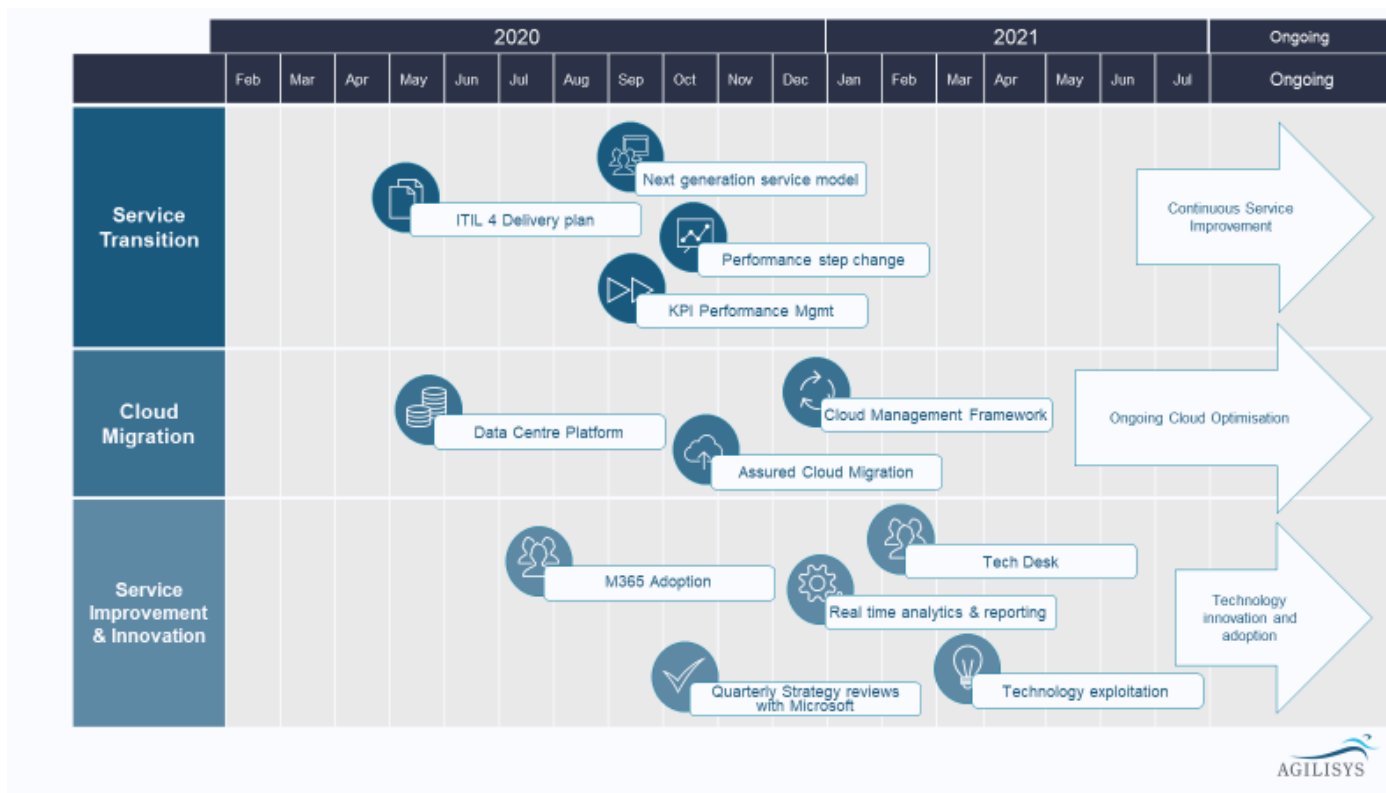
Kevin Mulcahy

Assistant Director IT -Projects & Programmes

E: kevin.mulcahy@cityoflondon.gov.uk

Appendix 1

Outline Plan



Phase	Event	Date	
Launch Phase	Launch tender	11th July	Completed
	Deadline for Clarifications	24th July	Completed
	Deadline for submissions	13th August	Completed
Evaluation Phase	Bid Evaluation start	14th August	Completed
	Commercial Evaluation	14th - 23rd August	Completed
	Technical Evaluation	14th Aug - 2nd Sept	Completed
	Technical Moderation	5th September	Completed
	Supplier Presentations	9th & 10th September	Completed
	Presentation Moderation	11th September	Completed
	Bid Evaluation end	11th September	Completed
Approval Phase	Steering Board	12th September	Completed
	Members' Reference Group	13th September	Completed
	Draft report (HR/Legal/Finance comments)	17th September	Completed
	Police IT Strategy Board	23rd -25th Sept	
	Strategic Resources Group	23rd -25th Sept	Completed
	Summit	26th September	Completed
	IT Category Board	2nd October	
	Deadline for revised (draft) committee report	17th October	Completed
	Procurement Sub Committee	29th October	Completed

	Establishment Committee	29th October	
	Digital Services Sub Committee	6th November	Completed
	Finance Committee	12th November	Completed
	Policy & Resources Committee (info only)	21st November	
	Police Authority Board	28th November	Completed
	Court of Common Council	5th December	Completed
	Notification of award	6th December	
	Standstill period end	16th December	Completed
	Announcement of award	16th December	Completed
Transition Phase	Finalise contract and onboard supplier	February 2020	
	Contract Start	March 2020	
	Transition Planning and Initiation	March 2020	

Committee(s)	Dated:
Summit Digital Services Sub Committee (DSSC)	26 th November 2019 24 th January 2020
Subject: City of London Corporation Information Handling (Protective Marking)	Public
Report of: Michael Cogher - Comptroller Peter Kane - Chamberlain	Summit for Decision DSSC for Information
Report authors: Sean Green – IT Director	

Summary

The Information Management (IM) Strategy was agreed by Summit in March 2019 and the Digital Services Sub-Committee in July 2019.

A Corporate risk was developed in March 2019 (see Appendix A below) that recognises the cultural and maturity issues the organisation faces currently with how we manage and support good information management curation and practices.

This paper presents the proposal to implement a protective marking schema in the organisation which, based on our current Microsoft licencing, will initially be manually applied however with future licence investment in 20/21 much of this can also be automated.

Recommendation(s)

Members are asked to:

- Note this report.

Main Report

Background

1. In March 2018 Summit agreed the IM Strategy
2. The strategy seeks to transform IM capabilities (tools and skills) and culture (values and behaviours) across CoL and its partners so that accurate and timely information is routinely and effectively used as the basis for decisions and actions, thereby leading to better service outcomes.
3. When the IM Strategy was presented to Summit in March 2019 it was recognised that a corporate risk should be created (See Appendix A attached)
4. Protective Marking came into effect in April 2014 and describes how HM Government classifies information assets to ensure they are appropriately

protected; support Public Sector business and the effective exploitation of information; and meet the requirements of relevant legislation and international / bilateral agreements and obligations.

5. The Government's protective marking system is designed to help individuals determine, and indicate to others, the levels of protection required to help prevent the compromise of valuable or sensitive assets. The markings signal quickly and unambiguously, the value of an asset and the level of protection it needs.
6. It applies to all information that government collects, stores, processes, generates or shares to deliver services and conduct business, including information received from or exchanged with external partners.
7. The City of London Police applies security classification to all documents and emails internally and externally and has been in force for many years.
8. The use of the protective marking schemas in of itself can change the culture of how staff perceive and value the information that they manage on behalf of the organisation. This would be the main benefit that would accrue to CoL.
9. As we move to a more flexible model of remote working from smaller locations and home the potential for in appropriate handling and release of sensitive information could increase therefore the cultural impact that protective marking should bring about should be of benefit to CoL.
10. In summary implementing a simplified protective marking scheme improves our information security and supports the mitigating actions for CR29 (see Appendix A attached).

Proposal for Implementation of Protective Marking

11. It has been agreed by Summit that CoL will apply protective labelling in a more pragmatic and practical way than the standard definitions provided by National Government with 2 labels and sub-categories that staff can choose that will be both be applied in the header, footer and watermark of the document
12. 3 labels can be chosen from a drop-down list:
 - a. Official – All routine public-sector business, operations and services should be treated as OFFICIAL;
 - b. Official Sensitive – A limited subset of OFFICIAL – information could have more damaging consequences (for individuals, an organisation or government generally) if it were lost, stolen or published in the media.

Note: Anything not marked will be considered as Non-business data for personal use only;

13. When Official Sensitive is chosen any email used to send the document will be encrypted. In addition, for this category there are 3 sub-categories that the member of staff will be offered from a drop-down list which are:
 - a. Internal only – Will be encrypted so that it can only be opened with internal organisational email address or through whitelisted email addresses or domains;
 - b. Commercial – Email or document can be externally sent and opened but will be encrypted.
 - c. Personal Data – Contains personal data as defined by the data protection act. Can be sent externally but will be encrypted.
14. The process for applying labels to documents will be manual with a recommended default to 'official' as a public-sector organisation we subscribe to a policy of openness and transparency.
15. To ensure officers, recognise the role of the Communications Director and his team for the release of any CoL information with any public forum a new footer will be added to all CoL documents that states:

“This information remains the property of the City of London Corporation. Any requests to share this information in a public forum should be made through the City of London’s Communication team”
16. Alongside the small system changes there will be online training and an information management cultural change and communication campaign.
17. In the future when we upgrade our current Microsoft licences, we can automate the application of protective marking labels based on sensitive and personal data detected in documents using Artificial Intelligence rules.

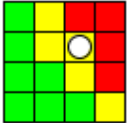
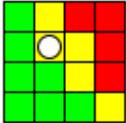

Next Steps

18. Following launch of Protective Marking staff will be encouraged to undertake short training course and explanation of the benefits of the using the schema will be communicated through communication campaigns.
19. Feedback and use of Protective Marking and Information Handling will be sought 3 months after launch to evidence mitigation of the Corporate IM risk.
20. Further automation (using AI rules) and protection of sensitive data should be implemented in 2020 following proposed upgrades to the organisation’s Microsoft Office licences.

IT Director
Chamberlain’s Department
E: Sean.Green@cityoflondon.gov.uk

Appendences
Appendix A – IM Corporate Risk

Appendix A – IM Corporate Risk

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
<p>CR29 Information Management</p> <p>08-Apr-2019 John Barradell</p>	<p>Cause: Lack of officer commitment and investment of the right resources into organisational information management systems and culture.</p> <p>Event: The City Corporation’s IM Strategy (2018-2023) is not fully and effectively implemented</p> <p>Effect:</p> <ul style="list-style-type: none"> • Not being able to use relevant information to draw insights and intelligence and support good decision-making • Vulnerability to personal data and other information rights breaches and non-compliance with possible ICO fines or other legal action • Waste of resources storing information beyond usefulness 	<p>Likelihood</p>  <p>Impact</p>	<p>12</p>	<ul style="list-style-type: none"> • New business intelligence dashboards continue to be developed for improved decision making by the Corporate Strategy and Performance team • An Information Management Awareness campaign starts from 19 February to 12 March. • Work will begin to review relevant staff roles that should have an information management competency added • A paper covering the benefits and proposed implementation of Protective was agreed by Summit in their December meeting • Capital bids submitted for information management investment to support the mitigation of this risk <p>11 Dec 2019</p>	<p>Likelihood</p>  <p>Impact</p>	<p>6</p>	<p>30-Jun-2020</p>	<p></p> <p>Constant</p>

Committee(s): Digital Services Sub-Committee	Date(s): 24 th January 2020
Subject: Oracle ERP strategy – interim paper	Public
Report of: The Chamberlain	For Information
Report author: Shoid Islam, Head of IT Applications	

Summary

The Chamberlain's IT team have been working with colleagues in the Finance Division on an Oracle Enterprise Resource Planning (ERP) strategy based on decisions that need to be made on this critical system as we get closer to the requirement for a major upgrade and other major linked or related IT applications going through strategic reviews.

The City of London Corporation (CoL) uses multiple systems to carry out functions for finance, property management, payroll and HR with no overarching reporting solution. The IT division are assisting in investigating the options to rationalise the various systems into a single ERP and reporting solution to reduce software, licensing and support costs (Consistent with the Corporate IT Applications Strategy) and the benefits of specialist best of breed systems for the different business functions.

An independent consultancy will be commissioned in January 2020 to support the short options review.

Recommendation(s)

Members are asked to note this report

Main Report

Background

1. CoL currently uses multiple best of breed solutions to carry out key lines of business, such as Oracle Financials for Finance and Commercial Property management, Midland's City People for both HR and Payroll.
2. These applications were procured several years ago and are now due for re-procurement.

3. These applications are currently hosted in Agilisys datacentres and are considered 'on premises' from a vendors' perspective. As part of the IT strategy there is a desire to migrate to a Software as a Service (SaaS) solution where possible.
4. Oracle's extended support ends in December 2021 for the City's current version of Oracle Financials.
5. The current Oracle solution is considered not fit for purpose by the Department of City Surveyors. Oracle do not provide a SaaS solution for commercial property management. The Department of City Surveyors prefer a best of breed commercial property management solution.
6. Oracle do provide a SaaS solution for the Finance module. The Chamberlains Department have submitted a capital project bid for the migration of the application from current on prem to the SaaS solution, to ensure that the City remains on a maintained and supported solution.
7. Oracle Business Intelligence (OBI) is the reporting tools which is currently being used to report from Oracle Financials for both Finance and Commercial Property management.
8. Midland's City People (iTrent) is currently used for Payroll processing and HR with Business objects providing the reporting function.
9. This application is currently on a supported version and will continue to be so with the future upgrades in the current IT project pipeline.
10. The City recognises that having multiple solutions may not be the most efficient method (i.e. support, maintenance, software and license cost etc) of working and has therefore commissioned a workstream to investigate this further.
11. There are various work streams currently underway which will lead to an options appraisal paper for a decision by June 2020.

Current Position

12. A Tender Working Group has been setup, which consists of Procurement, IT, Finance, Payroll and HR.
13. The purpose of this group is to lead on the re-procurement of the key lines of business solutions discussed in this paper.
14. Due to the current hard deadline for Oracle Finance, the Chamberlain's Finance team have submitted a capital project bid for funding a hosted SaaS Enterprise Resource Planning (ERP) solution. This bid assumes that both HR and Payroll are to be incorporated into the one solution and costings are

based around this, however a decision is yet to be made on the viability of this option.

15. Enterprise resource planning (ERP) is the name for the integrated management of and organisation's main business processes, often in real-time and mediated by software and technology.
16. ERP is usually referred to as a category of business management software — typically a suite of integrated applications—that an organization can use to collect, store, manage, and interpret data from many business activities.
17. ERP provides an integrated and continuously updated view of core business processes using common databases maintained by a database management system.
18. The City Surveyors Department have also submitted a capital project bid for Commercial Property Management, as there is no upgrade path to Oracle's SaaS solution for this module.
19. No capital project bids have been made for the replacement of Midland's City People (iTrent HR/Payroll system).

Potential Options

20. CoL will need to decide on one of the following options:

- a. Continue the status quo – Continue to maintain all applications on existing platforms.

Risk: Support life cycle is limited and potential Procurement law breaches.

- b. Best of breed solutions – All lines of business procure individual best of breed solutions.

Risk: Increased cost of software, license, support and maintenance.

- c. ERP – A single solution.

Risk: Business processes may need to be altered in certain business areas.

21. Considerations and decisions will need to be made on how reporting will be provided, if the decision is to not to go with a single ERP solution, which may have further financial implications.

22. Integration with the Financial systems will be required for any best of breed system chosen.

Corporate & Strategic Implications

23. A single ERP solution aligns with the Application strategy of rationalising applications where possible. The Application strategy feeds into the IT strategy which has a strong desire to migrate applications to a SaaS solution where possible.

Conclusion

24. A consultancy is being commissioned in January 2020 to provide an options review on ERP vs Best of Breed IT solutions for Finance, HR/Payroll and Commercial Property Management.

25. The Tender Working Party will need to agree the options appraisal paper at its earliest convenience to provide senior stakeholders with the ability to make an informed decision on the direction of the City's ERP solution. This decision will form the basis of Oracle's short, medium and long-term strategies.

Shoid Islam

Head of Applications

T: 020 7332 3560

E: shoid.islam@cityoflondon.gov.uk

Committee(s)	Dated:
Digital Services Sub-Committee – For Information	24th January 2020
Subject: IT Division – IT Service Delivery Summary	Public
Report of: The Chamberlain	For Information
Report author(s): Eugene O’Driscoll, Agilisys Client Director Matt Gosden, Deputy IT Director	

Summary

There was a total of 2 P1 and 9 P2 incidents for the City of London Corporation and City of London Police in November. 8 of these incidents were caused by external factors such as supplier works outside of the direct control of Agilisys.

Problem records have been created where appropriate to identify root causes and to manage improvements.

- There were 0 P1 incidents for City of London Corporation and 2 for City of London Police.
- There were 4 P2 incidents for the City of London Corporation and 5 for City of London Police.
- 82.5% of users reported a good or very good experience of the Service Desk.

Recommendations

Members are asked to note this report

Main Report

Service levels and exceptions

1. City of London Police (CoLP) P1 incidents

There were 2 P1 incidents

Affected Service	Duration	Reason	Resolution	Problem Management plan
PNC/Internet	05:15	Following planned domain controller shutdown, there was an issue with the automatic failover of the Barracuda device.	TBA at the time of this report.	Problem record created.
Network (Clearpass)	08:33	Clearpass server dropped off the domain	Clearpass was re-joined to the domain	Problem record created.

2. City of London Police P2 Incidents

There were 2 P2 incidents

Affected Service	Duration	Reason	Resolution	Problem Management plan
Internet	18:15	Wood Street Barracuda (proxy server) hardware failure	A group policy was changed to reroute traffic through the New Street Barracuda CP8-Barra01	Barracudas to be removed under the CoLP Modernisation programme.
VPN Stonesoft	00:31	The Service had stopped responding	The service was restarted	N/A
Public Folders	01:41	CP8-DAG01 was shut down without a full assessment of impact as part of a Change	Firewall changes	Post power shutdown review
External outgoing Emails	47:22	An Interface was disabled. (Not related to New St shutdown).	Resolved by 3rd party Vodafone	CoLP IT to review with 3rd party
Network - Wood St/Snow Hill	01:15	Forescout server was powered up, but not switched on following a New Street power down. Part of a change.	Forescout server was switched on	Post power shutdown review

3. City of London (CoL) P1 incidents

There were no P1 incidents

4. City of London P2 Incidents

There were 4 P2 incidents

Affected Service	Duration (hh:mm)	Reason	Resolution	Problem Management plan
Laptop connectivity	176:00	A change to update Lumension security software was misconfigured by a supplier.	Most issues resolved after a device restart, but a number required manual intervention to clean up the updated installation.	MI report and review carried out. Testing group to be expanded and given more structure.
Gower Epilog	00:07	Cemetery database unavailable	Database server was restarted	Existing
Slowness accessing the internet	06:19	A domain controller in Guildhall was not processing authentication attempts when accessing the internet.	The web proxy server was directed to authenticate with an alternative domain controller in IaaS. The domain controller was restarted.	The physical server is under monitoring to see if there has been any lasting damage from power outages and overheating that might explain its performance.
London Councils public Wi-Fi	17:15	Resolved without intervention	O2 reported no action was taken	Service review meeting

- In respect of the incident for laptop connectivity, a supplier configured a system upgrade package for the Lumension system, which manages USB port access controls. This was not part of the regular Windows patching cycle. The system upgrade consequently sent an upgrade package to each user computer in the environment. Pre-release testing, supplier guidance and user testing did not indicate an expected noticeable impact on users.
- Approximately 7% of users found that their devices were not responsive during the update. This resolved when the users restarted their computers, which completed the application installation. The Lumension upgrade was not successful for a further 3% of users, whose devices were left in an unusable state until engineering teams visited to reconfigure them to apply a 5-minute fix. This could not be applied remotely, and users reported issues over several days in which they made their devices available to engineers. Additional resources were brought in to assist with the process.

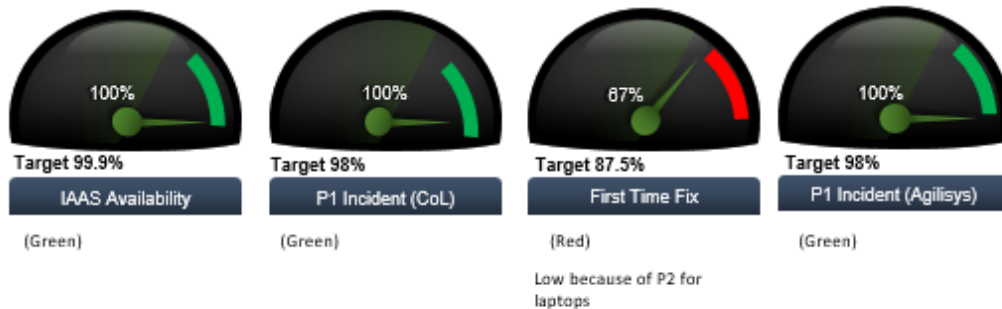
7. A major incident review meeting was held between Agilisys and the IT division. Key outputs included:

- Improved management communications during incidents
- Larger and structured user testing group will be formed to minimise the risk of repeat incidents
- User test results will be detailed and documented to inform decisions to deploy updates.
- In addition to a wider testing base for changes, updates and patches, CoL and Agilisys are developing improvements in how updates are carried out toward a more evergreen model. Where lower risk updates are delivered automatically, allowing the IT Team to focus on the higher risk, or more significant changes where an issue would cause unacceptable business impact.

Service performance summary is detailed in the dashboard below:

Gauges to monitor performance – November 2019

CoL



CoLP



Service improvements and highlights

8. Police Improvements include:

- Remediation of high and medium priority items in the 2019 IT Health Check (ITHC) progress: 38/52 High complete, 21/38 Medium complete.

- The Desktop modernisation programme team has moved to New Street and has entered the high-level design stage.

9. Corporation improvements include:

- New Service Desk communication templates to users about their requests were approved by the Business Users Group and implemented. These provide more relevant information and a more modern presentation to users.
- Server 2008 upgrade programme under way and on target to complete by mid-January. Very few exceptions identified that will require extended support from Microsoft past this date.

Guildhall Justice Room Exit Plan

10. The Chairman of DSSC requested an update on the plan the IT Division has in place to exit from one communications room in Guildhall Justice Room (GJR)

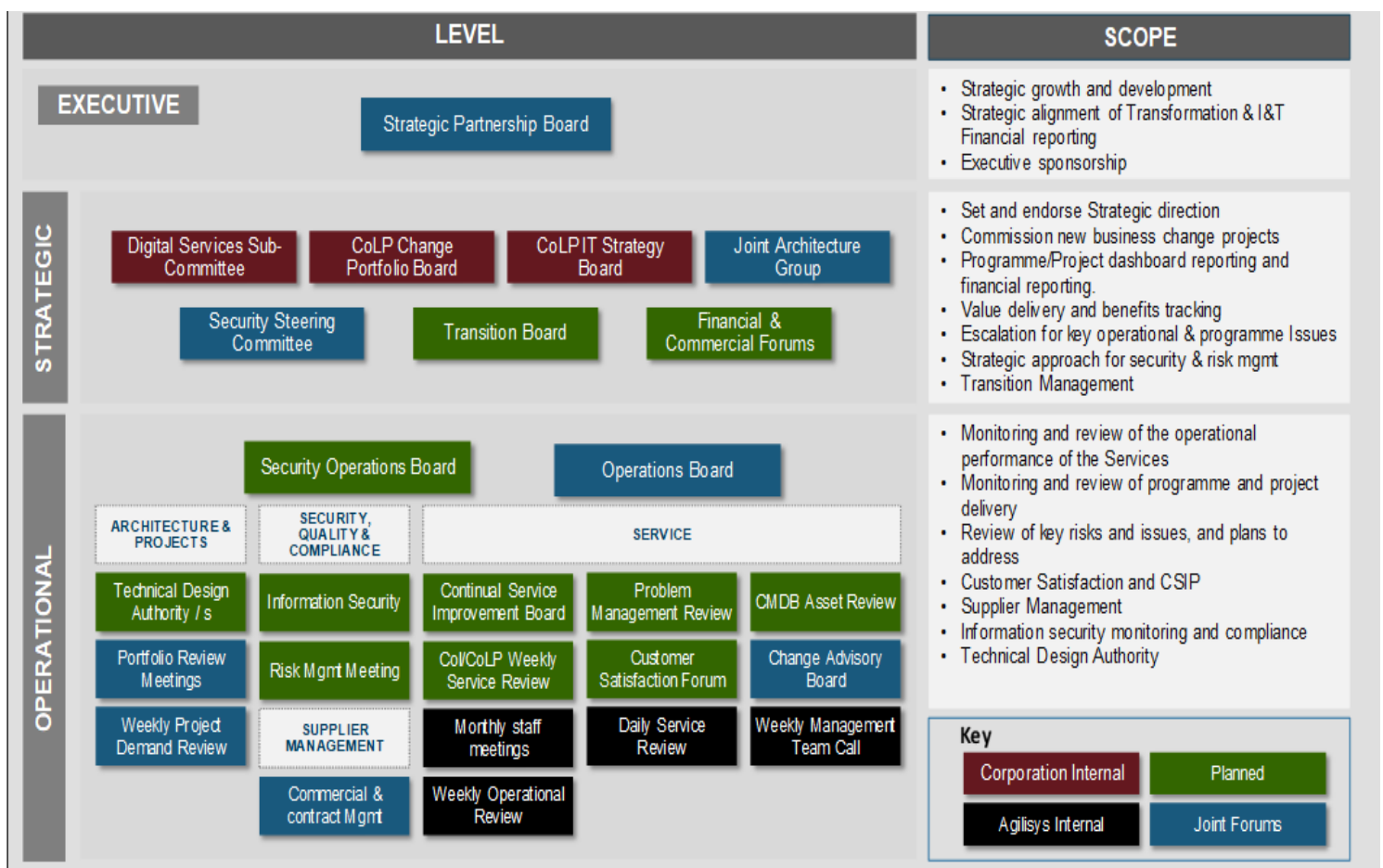
- Agilisys has provided a plan to the CoL IT team to complete the exit of technical equipment from the GJR basement.
- Subject to agreement, work will begin in January 2020 and is planned to complete by end of June. This is a large piece of work with multiple suppliers and complexities.
- This Technical Equipment Room has suffered from multiple failures of air conditioning and power supply and migrating equipment to more robust environments will remove the associated risks.
- CoL’s IT Division and Agilisys have prioritised this work and Agilisys will manage all suppliers who have equipment in the room. The completion date will be dependent on the migration of the Spatial system, which CoL is planning to complete by the end of June 2020.

PROJECTS	Jan	Feb	Mar	Apr	May	Jun
Systems ready for decommissioning	█					
Systems ready for decommissioning – with BT line dependency	█					
Systems ready for decommissioning – with network dependency	█					
Spatial system migration & decommissioning	█					
Project scoping	█					
Application discovery	█					
Migration delivery				█		
System stabilisation & decommissioning					█	
Active systems scoping & relocation	█					
Project scoping	█					
Estimate system relocation			█			
Review/revisions					◆	█
Final approval/closure						◆

11. Partnership improvements include:

- City of London named Agilisys as the preferred bidder for IT Services from September 2020.
- Detailed discussions begin in January 2020 to start service transition which will complete by end of August.
- The new service will be characterised by:
 - New service management tool
 - Improvements in asset management, change management
 - Increased automation using robotics
 - New user self-service interface with IT services
 - Improved governance model to monitor and develop services

New CoL IT and Agilisys Governance Model for 2020



Eugene O’Driscoll
Client Director
Agilisys

Matt Gosden
Deputy IT Director

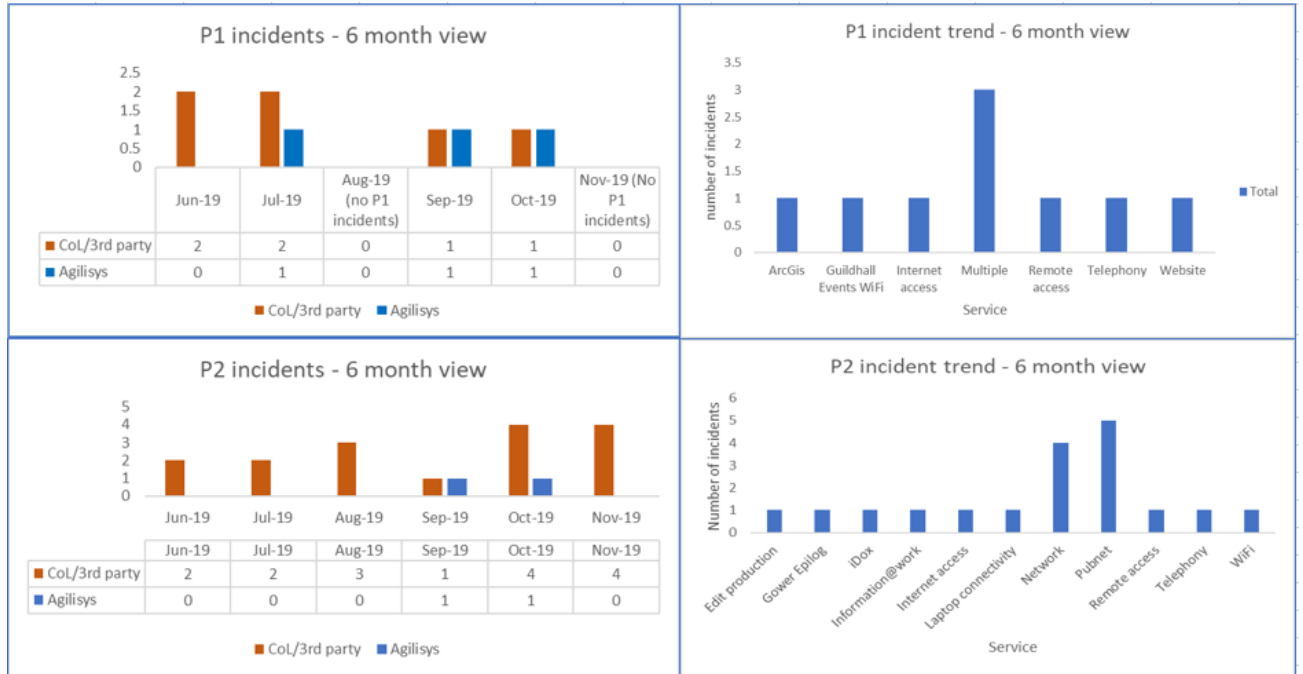
E: Eugene.Odriscoll@cityoflondon.gov.uk E: Matt.Gosden@cityoflondon.gov.uk

Appendences

Appendix 1 – CoL and CoLP P1 and P2 Trend Graphs

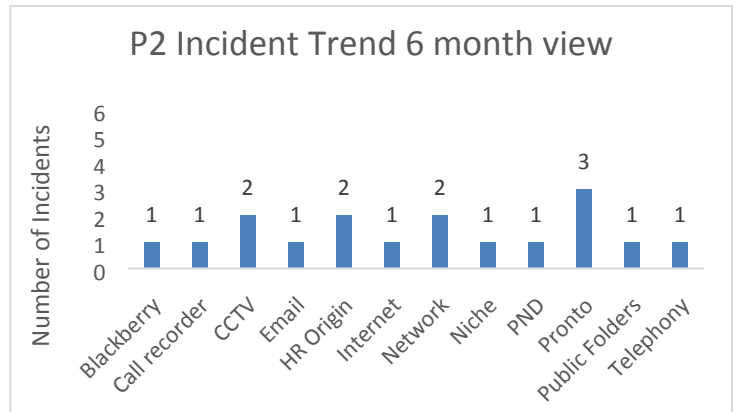
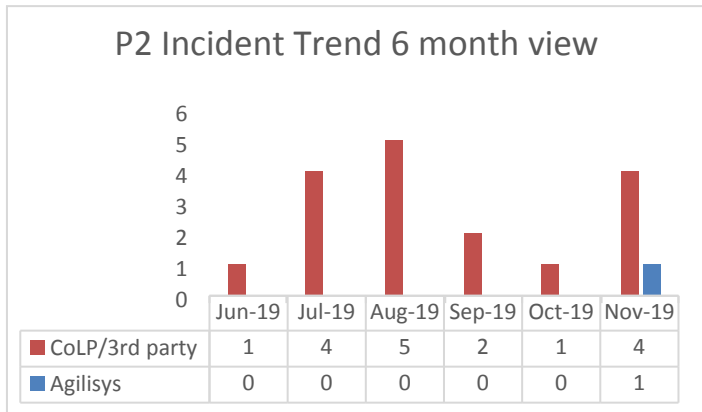
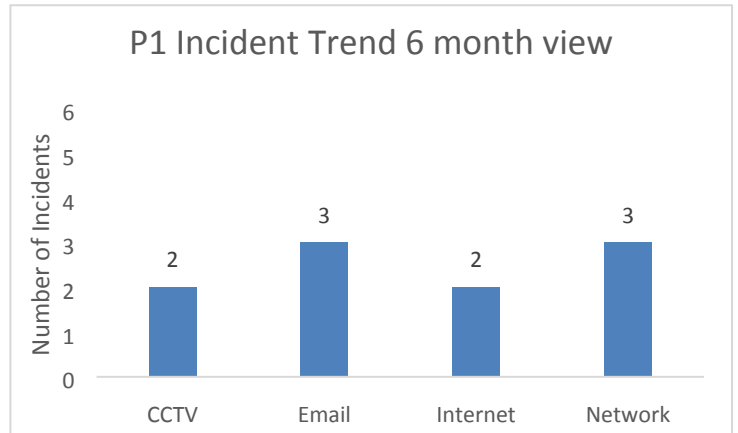
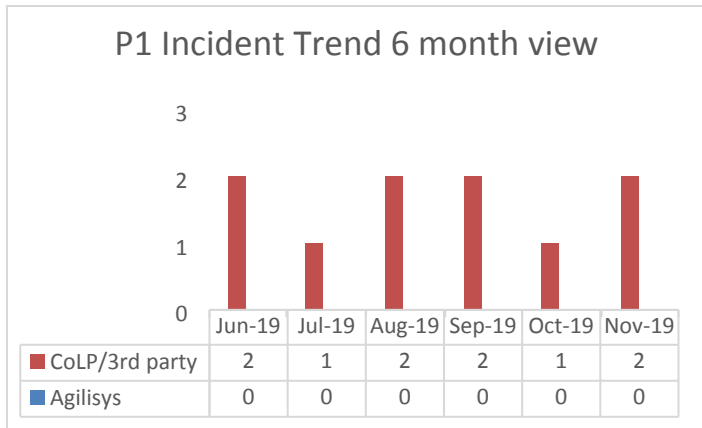
Appendix 1 – Trend Graphs

CoL Priority Incident trending – 6-month view



3 P1 incidents for Agilisys in 6 months
2 P2 incidents for Agilisys in 6 months

CoLP Priority Incident trending – 6-month view



0 P1 incidents in Agilisys control in 6 months
 1 P2 incident in Agilisys control in 6 months

Committee(s)	Dated:
Digital Services Sub-Committee	24th January 2020
Subject: IT Division - Change Management Summary	Public
Report of: The Chamberlain	For Information
Report author: Eugene O'Driscoll Agilisys Client Director Matt Gosden – Deputy IT Director	

Summary

This paper aims to support the Digital Services Sub Committee's understanding of the effectiveness of the management of changes to the IT environment.

The paper describes three specific areas:

- An overview of the IT Change Management process
- Performance measurements
- Future opportunities

Recommendation(s)

Members are asked to note this report

An overview of the IT Change Management process

1. The ITIL definition of change is "the addition, modification or removal of any authorized, planned, or supported service or service component that could have an effect on IT services"
2. The goal of Change Management is to ensure that standard procedures are used for efficient and prompt handling of all changes, in order to minimise the impact of Change related Incidents on service quality.
3. Change Management can only occur when IT management can recognise when Change has occurred and verify that it is both authorised and has a purpose.
4. The City of London Corporation (CoL) Change Management Policy must be complied with by all users and administrators of IT.
 - All Members of IT, including Facilities, Strategic technology partners and 3rd party suppliers.

- All CoL and CoL sites and Institutional bodies of the Corporation where CoL-owned technology are impacted by the change.
5. The IT Director owns the policy.
 6. All IT suppliers, internal teams and 3rd parties are responsible for complying with this policy.
 7. Agilisys is responsible for managing the process and co-ordinating any Change Management activities.

Change Approval Board

8. A Change Approval Board is held weekly to review and authorise changes, or more frequently during periods of greater change. The Board is run by the Agilisys Change Manager and always includes representation from technical teams and senior management in Agilisys and the City of London IS team.
9. Review includes confirming that the proposed changes:
 - conform to City of London policies
 - have been tested
 - are risk-assessed
 - are resourced
 - are communicated to users

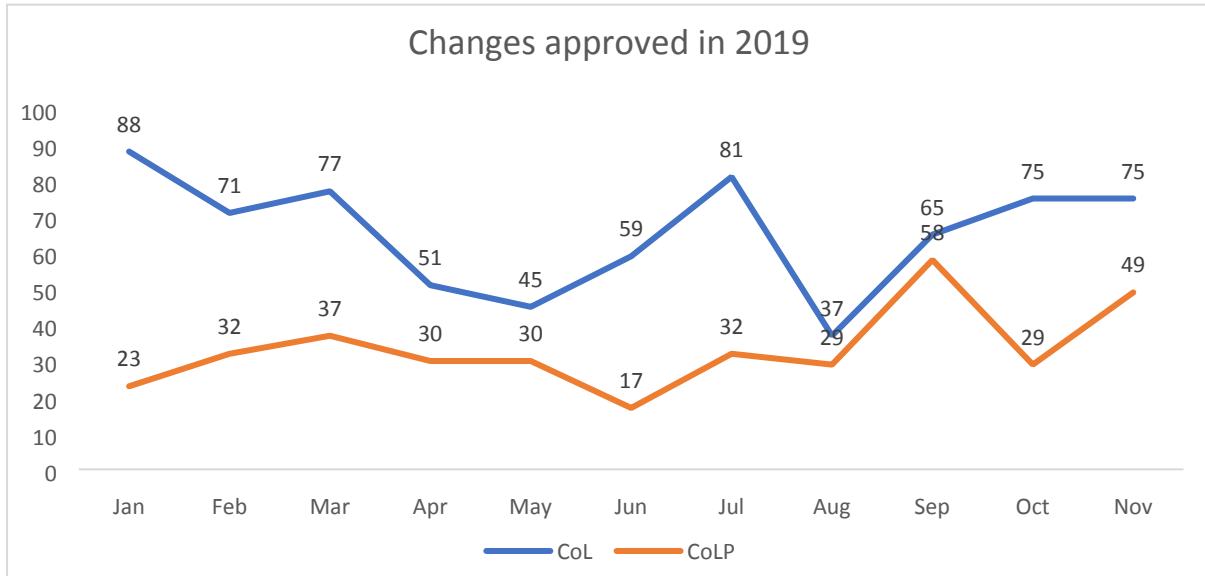
Classification of changes

10. Changes fall into one of the following categories:

Change Type	Change Example
Standard change	Standard Changes are pre-approved changes that are considered relatively low risk, are performed frequently, and follow a documented (and Change Management approved) process.
Non-Standard Change (Non-Standard Request or RFC)	Addition of new services, software, hardware; installation of enhancements or fixes; configuration Changes to systems; major hardware moves and data migrations. It also includes: <ul style="list-style-type: none"> • Emergency Changes and Retrospective Changes - including urgent fixes to correct problems. • Retrospective changes – In order to immediately fix a fault, the Change takes place before there is time to hold a CAB meeting (so as minimise interruptions to service).

Performance measurements

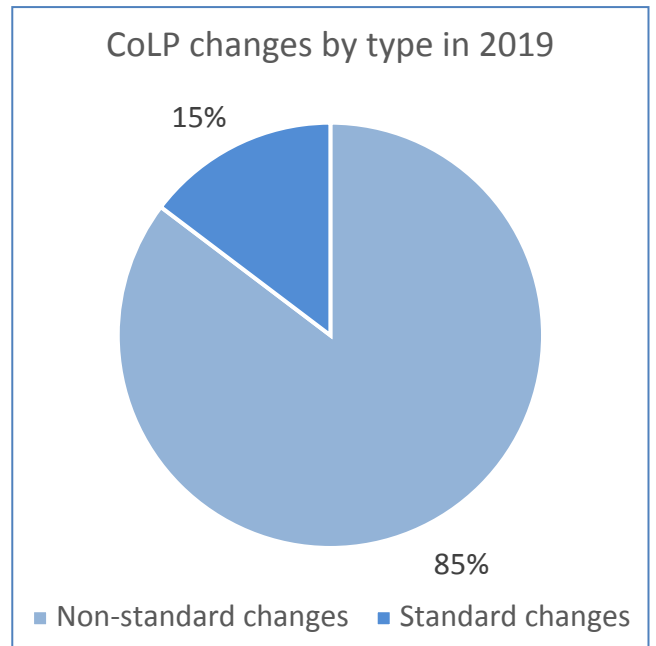
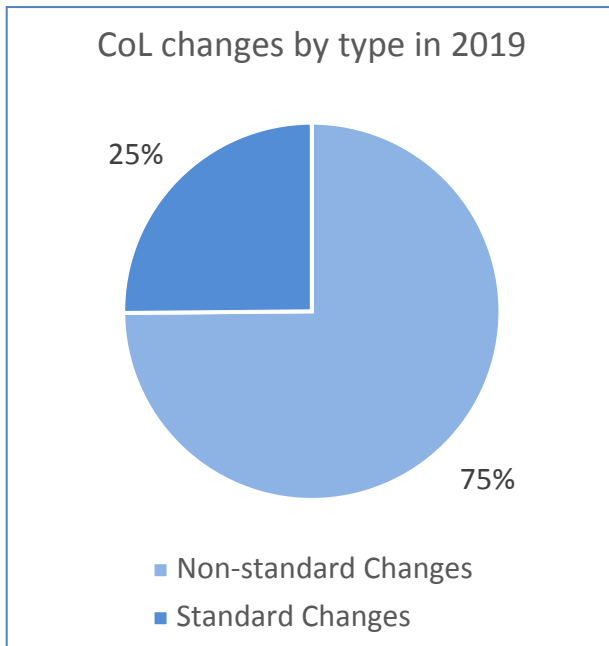
11. The Change Approval Board approved an average of 66 changes per month for CoL and 34 for CoLP in 2019.



12. Changes may be raised because of planned project work to implement new services, as part of routine maintenance and occasionally to support urgent work to fix service issues.

13. Standard changes are not service-impacting and are often carried out during business hours without awareness in the business. Typically, standard changes are related to existing services and applications and are repeatable and low risk, e.g. data extracts or application template changes.

14. Non-standard changes are reviewed for potential business impact and are normally carried out in the evening or at weekends. Typically, non-standard changes include the introduction of new technology, upgrade or significant modifications to existing services, and carry a higher risk or impact.



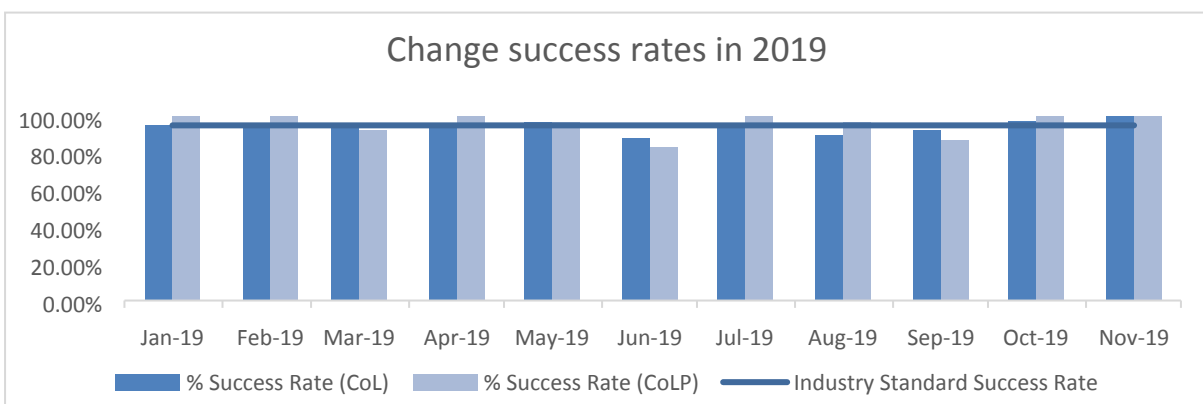
Measuring success

15. A change is regarded as a success if it completed without unexpected impact on business users. 100% of Standard Changes were successful in 2019.

16. A change is regarded as a failure if it failed to complete or completed but with an unexpected impact on business users.

17. Changes may be rejected by the Change Approval Board if they do not meet all the criteria to proceed or they may be cancelled if circumstances change.

Month	Jan-19	Feb-19	Mar-19	Apr-19	May-19	Jun-19	Jul-19	Aug-19	Sep-19	Oct-19	Nov-19
Industry Standard Success Rate	95%	95%	95%	95%	95%	95%	95%	95%	95%	95%	95%
% Success Rate (CoL)	96%	94%	96%	94%	97%	88%	95%	90%	92%	97%	100%
% Success Rate (CoLP)	100%	100%	93%	100%	97%	83%	100%	97%	87%	100%	100%



Risks

18. Pre-change testing is always carried out in the IT service, but because there is a wide range of end user equipment and application configurations, this cannot be guaranteed to identify all issues.
19. The current service management tool has limited capability to predict the impact of change on other systems.
20. It is not possible to always avoid impact on business users. Business toleration of some disruption or service unavailability is necessary.

Future opportunities

21. A larger test group of users, selected to maximise the number of use cases, is being prepared by the IS division and will improve confidence that the impact of planned changes is well understood.
22. The IS division is working with business users to improve the quality of User Acceptance Testing will provide assurance that there is consistent and auditable testing which informs decisions to release changes to larger groups of users.
23. Agilisys will be implementing a new service management tool which will dynamically capture the relationships between systems and provide valuable input into change decision-making.
24. The new service management tool will assist with making available the decisions of the Change Approval Board and provide a forward schedule of changes.
25. The service management team reviews the overall change profile to seek opportunities to increase the percentage of low-risk standard changes.

Eugene O'Driscoll

Client Director

Agilisys

E: Eugene.Odriscoll@cityoflondon.gov.uk

Matt Gosden

Deputy IT Director

E: Matt.Gosden@cityoflondon.gov.uk

This page is intentionally left blank

Committee(s)	Dated:
Digital Services Sub Committee – For Information	24th January 2020
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 4 risks. There is currently 1 RED risk. There are no extreme impact risks, there are 3 major impact, 1 serious impact and no Minor impact risks.

IT currently holds 2 risks on the Corporate Risk Register.

Summary of the Corporate Risks

CR 16 – Information Security

Following review with Audit & Risk committee and DSSC it was agreed that further steps were required to achieve maturity level that could bring the score to its target. As a result of the Deep dive report to A&RMC in September 2019, the risk description has been amended to reflect an emphasis on CoL preparedness.

CR 29 – Information Management

- New business intelligence dashboards continue to be developed for improved decision making by the Corporate Strategy and Performance team
- An Information Management Awareness campaign starts from 19 February to 12 March.
- Work will begin to review relevant staff roles that should have an information management competency added
- A paper covering the benefits and proposed implementation of Information Handling (Protective Marking) was agreed by Summit in their November 2019 meeting
- Capital bids submitted for information management investment to support the mitigation of this risk.

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 2 Amber risks on the Corporate Risk Register. The IT Division currently holds 4 risks, one of which is 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:
 - 1 additional risk has been added to the Departmental Risk Register
 - 1 Risk have increased in score
 - 1 Risk has decreased in score
 - 1 Risk has been deactivated

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

Movement of Risks

4. New Risk

- **CHB IT 030 - 2020 - Managed Service Contract**– The transition and implementation of the new IT Service Contract has delays beyond the end of the contract on the 31st August 2020.

5. Increase in Score

- CHB IT 001 – Power and Resilience – Following a number of power failures out of the control of the IT Division this risk has been increased in score to RED as these failures have led to IT failures.

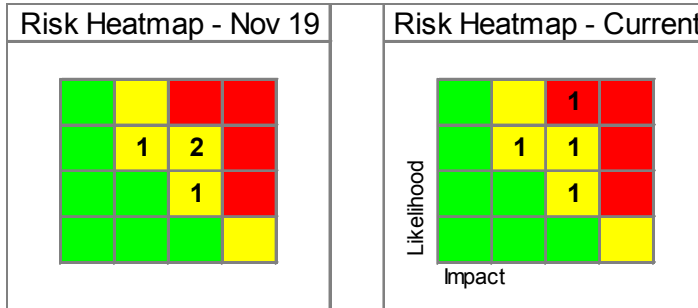
6. Decrease in Score

- CHB IT 004 – Business Continuity/Disaster Recovery – Following the implementation of the resilient circuit into the Guildhall it is deemed that loss of connectivity is less likely.

7. Deactivated Risk

- CHB IT 028 - Air Conditioning in Datacentres – Following the implementation of heat monitoring in the data centres the risk has been reduced, and the outstanding actions will be picked up in CHB IT 001.

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



8. Further breakdown of current Division risks:

		Trend	
Major Impact:			
Risks with "likely" likelihood and "major" impact:	1	↑	
Risks with "possible" likelihood and "major" impact:	1	↓	
Risks with "Unlikely" likelihood and "major" impact:	1	↔	
Serious Impact:			
Risks with "likely" likelihood and "serious" impact:	0	↔	
Risks with "possible" likelihood and "serious" impact:	1	↔	
Risks with "unlikely" likelihood and "serious" impact:	0	↔	

9. 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

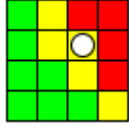
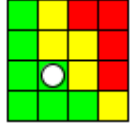

E: samantha.kay@cityoflondon.gov.uk

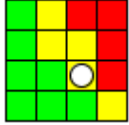
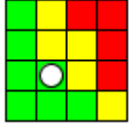
T: 07817 411176

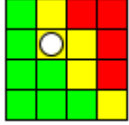
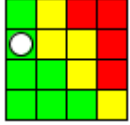



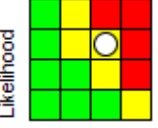
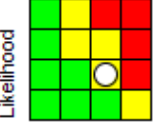

APPENDIX A - CHB IT All DEPARTMENTAL risks

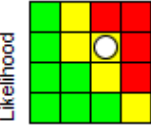
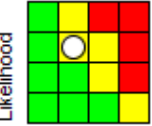

Risk no, title, creation date, owner	Risk Description (Cause, Event, Impact)	Current Risk Rating & Score		Risk Update and date of update	Target Risk Rating & Score		Target Date	Current Risk score change indicator
CHB IT 001 Resilience - Power and Infrastructure. 30-Mar-2017 Sean Green	<p>Cause: There is a lack of resilient or reliable Power services or Uninterruptable Power Supply (UPS) provision in multiple Comms rooms and datacentres in COL and COLP buildings.</p> <p>Event: There will be intermittent power outages of varying durations affecting these areas/buildings.</p> <p>Effect:</p> <ul style="list-style-type: none"> • Essential/critical Systems or information services are unavailable for an unacceptable amount of time • Recovery of failed services takes longer than planned • Adverse user/member comments/feedback • Adverse impact on the reputation of the IT division/Chamberlain's Department 	<p>Likelihood</p> <p>Impact</p>	16	Following recent, regular power failures that effect the IT service the risk has increased in likelihood to 'Likely' This is now being raised with the Corporation Facilities Team at a Senior Level. Monitoring on the air-conditioning units has been added to the Tier 1 comms rooms. UPSs are being installed in the main 2 Guildhall Comms rooms; a capital bid has been submitted based on the audit to install UPS across the estate where appropriate. 11 Dec 2019	<p>Likelihood</p> <p>Impact</p>	2	30-Jun-2020	 Increasing

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
<p>CHB IT 030 2020 - Managed Service Contract</p> <p>11-Oct-2019 Sean Green</p>	<p>Cause: New IT Services contract being implemented to replace the current contract we have with Agilisys Event: The transition and implementation have delays beyond the end of the contract on the 31st August 2020 Effect: Additional costs/dual running costs incurred and potential reputational impact of any failures or service disruption during the Transition and Implementation</p>	 <p>Likelihood</p> <p>Impact</p>	<p>12</p>	<p>The contract award has now been approved by Court of Common Council and is now in its 10 day stand still period.</p> <p>Phase 2 work streams have been formed and following the award can now start working with the supplier to plan transition activities.</p> <p>Job descriptions for in sourced roles are being drafted.</p> <p>11 Dec 2019</p>	 <p>Likelihood</p> <p>Impact</p>	<p>4</p>	<p>31-Aug-2020</p>	<p></p> <p>Constant</p>

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
<p>CHB IT 004 Business Continuity / Disaster Recovery - planning and management.</p> <p>30-Mar-2017 Sean Green</p>	<p>Cause: A lack of clear understanding of Business need for Services and Applications. No procedure in place for regular reviews with business.</p> <p>Event: The IT Division cannot provide assurance of availability or timely restoration of core business services in the event of a DR incident or system failure.</p> <p>Effect: The disaster recovery response of the IT Division is unlikely to meet the needs of COL and COLP leading to significant business interruption and serious operational difficulties.</p>	<p>Likelihood</p>  <p>Impact</p>	<p>8</p>	<p>The likelihood has reduced to unlikely following the installation of the resilient circuit into the Guildhall, the completion of a Disaster Recovery Test has confirmed that the circuit is in place and working as required.</p> <p>A rolling programme of DR tests has been developed and implemented. Risk will be continually reviewed alongside the DR test results.</p> <p>10 Dec 2019</p>	<p>Likelihood</p>  <p>Impact</p>	<p>4</p>	<p>31-Mar-2021</p>	<p>↓</p> <p>Decreasing</p>

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
<p>CHB IT 029 iTrent Contract</p> <p>18-Jun-2019</p>	<p>Cause: Extension of contract passed the envisaged term of 10 years with no permissible grounds. No projects started to procure a replacement.</p> <p>Event: City of London receive a challenge around the contract for iTrent with MHR Ltd around the extension of the contract.</p> <p>Effect: Legal challenge/court proceedings from a competitor to iTrent. CoL could be forced to issues 18 months termination notice before they are ready to implement a replacement product.</p>	 <p>Likelihood</p> <p>Impact</p>	<p>6</p>	<p>Options appraisal is with procurement and a tender working group has been set up with all relevant parties engaged, this is being led by the Deputy Chamberlain.</p> <p>Capital bid for funding has been submitted</p> <p>11 Dec 2019</p>	 <p>Likelihood</p> <p>Impact</p>	<p>3</p>	<p>31-Mar-2020</p>	<p></p> <p>Constant</p>

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
<p>CR16 Information Security (formerly CHB IT 030)</p> <p>10-May-2019 Peter Kane</p>	<p>Cause: Breach of IT Systems resulting in unauthorised access to data by internal or external sources. Officer/ Member mishandling of information.</p> <p>Event: The City Corporation does not adequately prepare, maintain robust (and where appropriate improve) effective IT security systems and procedures.</p> <p>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 €20M. Compliance enforcement action. Corruption of data. Reputational damage to Corporation as effective body.</p>	 <p>Likelihood</p> <p>Impact</p>	<p>12</p>	<p>Following review with A&R committee and DSSC it was agreed that further steps were required to achieve maturity level that could bring the score to its target. As a result of the Deep dive report to A&RMC in September 2019, the risk description has been amended to reflect an emphasis on CoL preparedness.</p> <p>04 Dec 2019</p>	 <p>Likelihood</p> <p>Impact</p>	<p>8</p>	<p>31-Dec-2020</p>	<p></p> <p>Constant</p>

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
<p>CR29 Information Management</p> <p>08-Apr-2019 John Barradell</p>	<p>Cause: Lack of officer commitment and investment of the right resources into organisational information management systems and culture.</p> <p>Event: The City Corporation’s IM Strategy (2018-2023) is not fully and effectively implemented</p> <p>Effect:</p> <ul style="list-style-type: none"> • Not being able to use relevant information to draw insights and intelligence and support good decision-making • Vulnerability to personal data and other information rights breaches and non-compliance with possible ICO fines or other legal action • Waste of resources storing information beyond usefulness 	 <p>Likelihood</p> <p>Impact</p>	<p>12</p>	<ul style="list-style-type: none"> • New business intelligence dashboards continue to be developed for improved decision making by the Corporate Strategy and Performance team • An Information Management Awareness campaign starts from 19 February to 12 March. • Work will begin to review relevant staff roles that should have an information management competency added • A paper covering the benefits and proposed implementation of Protective was agreed by Summit in their December meeting • Capital bids submitted for information management investment to support the mitigation of this risk <p>11 Dec 2019</p>	 <p>Likelihood</p> <p>Impact</p>	<p>6</p>	<p>30-Jun-2020</p>	<p></p> <p>Constant</p>

Committee(s)	Dated:
Digital Services Sub Committee (DSSC)	January 24 th 2020
Subject: CR 16 Information Security Risk	Public
Report of: Chamberlain	For Information
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 to capture and mitigate the risks a 'cyber breach' would present to the City of London Corporation (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 Measurable) 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 CR16 risk is currently Amber. The risk score will remain Amber but should move to 8 from 12 by December 2020 based on delivering the target maturity scores.

Recommendation(s)

Members are asked to:

- Note the report.

Main Report

Background

1. Cyberspace has revolutionised how many of us live and work. The internet, with its more than 3 billion users, is powering economic growth, increasing collaboration and innovation, and creating jobs.
2. Protecting key information assets is of critical importance to the sustainability and competitiveness of businesses today. The City Corporation needs to be on the front foot in terms of our cyber preparedness. Cyber security is all too often thought of as an IT issue, rather than the strategic risk management issue it 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. This is tested annually with the work undertaken with the IT Health check and the National Government PSN accreditation. 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 Corporation’s 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 an essential requirement to permit the measurement and assurance of the CR16 risk. Several frameworks were considered, and the NCSC Ten Steps to Cyber Security framework, supported by the NCSC 20 Critical Security Controls, was chosen as the most appropriate for the City Corporation.
8. To provide an overview of CR16 risk management, the current compliance with the HMG Ten Steps assurance programme is detailed below (table 1) under each of the ten steps areas. The control scores 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 Oct. 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	93%	4	4	-
6. Managing User Privileges	75%	4	3	-
7. Removable Media Controls	89%	4	4	-
8. Secure Configuration	86%	4	4	↑
9. Home and Mobile Working	71%	4	3	-
10. User Education and Awareness	75%	4	3	-

Options

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

Proposals

10. Continue to implement the 10 steps programme across the City Corporation.
11. Continue to monitor threat, risks and harm and make recommendations for changing the risk status accordingly.

Implications

12. Failure to demonstrate appropriate controls in this risk area will expose the City Corporation to unacceptable levels of risk and could hinder several strategic objectives.
13. There are also several statutory requirements to consider for the management of this risk area, these are summarised at Appendix 3.

Health Implications

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

Conclusion

15. 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.

16. 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.
17. 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.
18. 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. The nature of the risk we face is illustrated with Appendix 6 the risk threat report. The risk score will remain Amber but should move to 8 from 12 by December 2020 based on delivering the target maturity scores.

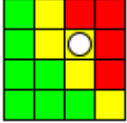


Appendices

- Appendix 1 – CR16 Information Security
- Appendix 2 – Statutory Requirements Summary
- Appendix 3 – Maturity Scoring Matrix
- Appendix 4 – NON-PUBLIC - 10 Steps Detail Report
- Appendix 5 – NON-PUBLIC - 10 Steps Gap Analysis
- Appendix 6 – NON-PUBLIC – Risk Threat Report

Gary Brailsford-Hart

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

Appendix 1 - CR16 – IT Security Risk

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
<p>CR16 Information Security (formerly CHB IT 030)</p> <p>10-May-2019</p> <p>Peter Kane</p>	<p>Cause: Breach of IT Systems resulting in unauthorised access to data by internal or external sources.</p> <p>Officer/ Member mishandling of information.</p> <p>Event: The City Corporation does not adequately prepare, maintain robust (and where appropriate improve) effective IT security systems and procedures.</p> <p>Effect: Failure of all or part of the IT Infrastructure, with associated business systems failures.</p> <p>Harm to individuals, a breach of legislation such as the Data Protection Act 2018. Incur a monetary penalty of up to €20M. Compliance enforcement action. Corruption of data. Reputational damage to Corporation as effective body.</p>	<p>Likelihood</p>  <p>Impact</p>	<p>12</p>	<p>Following review with A&R committee and DSSC it was agreed that further steps were required to achieve maturity level that could bring the score to its target. As a result of the Deep dive report to A&RMC in September 2019, the risk description has been amended to reflect an emphasis on CoL preparedness.</p> <p>04 Dec 2019</p>	<p>Likelihood</p>  <p>Impact</p>	<p>8</p>	<p>31-Dec-2020</p>	<p></p> <p>Constant</p>

This page is intentionally left blank

Appendix 2: 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/2006/11/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 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 awareness of the of the need to act. Management communicates the overall issues.	Similar and common processes emerge, but are largely intuitive because 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 understanding of the requirements. Proactive communication of the issues based on trends exists, mature communication techniques are applied, and integrated communication 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 education support 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

Document is Restricted

This page is intentionally left blank

By virtue of paragraph(s) 1 of Part 1 of Schedule 12A
of the Local Government Act 1972.

Document is Restricted

This page is intentionally left blank

By virtue of paragraph(s) 1 of Part 1 of Schedule 12A
of the Local Government Act 1972.

Document is Restricted

This page is intentionally left blank

By virtue of paragraph(s) 1 of Part 1 of Schedule 12A
of the Local Government Act 1972.

Document is Restricted

This page is intentionally left blank

By virtue of paragraph(s) 3 of Part 1 of Schedule 12A
of the Local Government Act 1972.

Document is Restricted

This page is intentionally left blank

By virtue of paragraph(s) 3 of Part 1 of Schedule 12A of the Local Government Act 1972.

Document is Restricted

This page is intentionally left blank

By virtue of paragraph(s) 3 of Part 1 of Schedule 12A of the Local Government Act 1972.

Document is Restricted

This page is intentionally left blank

By virtue of paragraph(s) 3 of Part 1 of Schedule 12A
of the Local Government Act 1972.

Document is Restricted

This page is intentionally left blank

By virtue of paragraph(s) 3 of Part 1 of Schedule 12A
of the Local Government Act 1972.

Document is Restricted

This page is intentionally left blank

By virtue of paragraph(s) 3 of Part 1 of Schedule 12A
of the Local Government Act 1972.

Document is Restricted

This page is intentionally left blank

By virtue of paragraph(s) 3 of Part 1 of Schedule 12A
of the Local Government Act 1972.

Document is Restricted

This page is intentionally left blank

By virtue of paragraph(s) 3 of Part 1 of Schedule 12A
of the Local Government Act 1972.

Document is Restricted

This page is intentionally left blank

By virtue of paragraph(s) 3 of Part 1 of Schedule 12A
of the Local Government Act 1972.

Document is Restricted

This page is intentionally left blank