



Digital Services Sub (Finance) Committee

Date: FRIDAY, 5 JULY 2019
Time: 1.45 pm
Venue: COMMITTEE ROOMS - WEST WING, GUILDHALL

Members: Randall Anderson (Chairman)
Deputy Jamie Ingham Clark (Deputy Chairman)
Randall Anderson (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
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 and non-public summary of the meeting held on Thursday 30 May 2019.

For Decision
(Pages 1 - 4)
4. **FORWARD PLAN 2019**
Report of the Chamberlain.

For Information
(Pages 5 - 6)
5. **OUTSTANDING ACTIONS FROM PREVIOUS MEETINGS**
Joint report of the Town Clerk and the Chamberlain.

For Information
(Pages 7 - 8)
6. **PRESENTATION FROM OPEN SPACES - ON THEIR DIGITAL JOURNEY**
Director of the Open Spaces to be heard.

For Information
7. **PRESENTATION FROM MARKETS AND CONSUMER PROTECTION**
Director of Markets & Consumer Protection to be heard.

For Information
8. **CITY OF LONDON CORPORATION INFORMATION MANAGEMENT EXECUTIVE SUMMARY**
Report of the Chamberlain.

For Decision
(Pages 9 - 20)
9. **SOCIAL RESPONSIBILITY**
Report of the Chamberlain

For Information
(Pages 21 - 48)
10. **DRAFT IT BUSINESS PLAN 2019/20**
Report of The Chamberlain.

For Information
(Pages 49 - 58)

11. **IT DIVISION - IT SERVICE DELIVERY SUMMARY**
Report of the Chamberlain.
For Information
(Pages 59 - 62)
12. **IT DIVISION RISK UPDATE**
Report of the Chamberlain.
For Information
(Pages 63 - 74)
13. **CR16 INFORMATION SECURITY RISK**
Report of the Chamberlain.
For Information
(Pages 75 - 96)
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 Thursday 30 May 2019 be approved as a correct record.
For Decision
(Pages 97 - 100)
18. **IT DIVISION - IT DISASTER RECOVERY TEST**
Report of the Chamberlain.
For Information
(Pages 101 - 106)
19. **IT SERVICE 2020 CONTRACT - SOURCING**
Report of the Chamberlain.
For Information
(Pages 107 - 126)
20. **POLICING PROGRAMMES - UPDATE REPORT**
Joint report of the Chamberlain and the Commissioner of the City of London Police.
For Information
(Pages 127 - 134)

21. **CITY OF LONDON POLICE - IT MODERNISATION PROGRAMME**
Joint report of the Chamberlain and the Commissioner of the City of London Police.
For Decision
(Pages 135 - 144)
22. **NON-PUBLIC QUESTIONS ON MATTERS RELATING TO THE WORK OF THE
SUB COMMITTEE**
23. **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

Thursday, 30 May 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)	Jeremy Mayhew
Deputy Jamie Ingham Clark (Deputy Chairman)	Deputy Hugh Morris
Rehana Ameer	
Deputy Keith Bottomley	

In attendance:

Sylvia Moys
John Chapman

Officers:

Rofikul Islam	- Town's Clerk
Melissa Richardson	- Town's Clerk
Peter Kane	- Chamberlain
Sean Green	- Chamberlain
Samantha Kay	- Chamberlain
Matt Gosden	- Chamberlain
Gary Brailsford-Hart	- City of London Police
Graeme Quarrington-Page	- Chamberlain

1. APOLOGIES

Apologies for absence were received from Tim Levene, James Tumbridge. Jeremy Mayhew gave notice that he might be slightly late.

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 5 April 2019 be approved as a correct record.

4. OUTSTANDING ACTIONS

The Sub-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 Sub-Committee's proposed work plan for forthcoming meetings.

The Chairman expressed an interest to have Sylvia Moys, John Chapman and James Tumbridge co-opted onto the Sub-Committee.

RESOLVED – That the Sub-Committee notes the report.

5. **FORWARD PLAN**

The Sub-Committee received a report of the Chamberlain which provided the Members with a horizon scan of the Sub-Committee's work plan for the ensuing municipal year.

RESOLVED – That the Sub-Committee notes the report.

6. **PRESENTATION FROM THE OPEN SPACES ON THEIR DIGITAL JOURNEY**

In consultation with the Chairman, the item has been deferred to a future meeting.

7. **CHANGE AND ENGAGEMENT UPDATE**

The Sub-Committee received a report of the Chamberlain on the Change and Engagement Update. Members were informed that the IT Transformation has delivered £250,000 in cashable storage savings. To deliver further benefits requires increased adoption of the Office 365 toolset that the City of London has already invested in with Microsoft licence agreement. A further example of benefit from adoption of Office 365 is the Freeman's School which is based in Leatherhead and is now able to avoid travel time and cost using Skype for Business video conference with colleagues based at the Guildhall.

A Member asked what will happen to the funds saved from the IT Transformation programme. Members were informed that any saving from the programme will go back to the Corporate Funds of the City of London.

Additionally, a Member sought clarification on the benefits of the business case for the programme. While noting the above benefits, it was agreed that , a review will be carried out to explore the additional financial and non-financial benefits of the programme.

RESOLVED – That the Sub-Committee notes the report.

8. **CITY OF LONDON CORPORATION INFORMATION MANAGEMENT EXECUTIVE SUMMARY**

The Sub-Committee received a report of the Chamberlain on the City of London Corporation on the proposed Information Management Strategy. It is recognised that the City does not currently have clear guidelines for data retention and far too much material is held for too long, increasing storage cost. More importantly, much of this information is not held in a manner that makes it readily accessible. The City intends to adopt best in class management practices while also making more of its information available to the public. Members were further told that there is a communications campaign planned to spread the messaging around this strategy across the City of London in the Autumn of 2019.

Members were assured that a revised paper on the City of London Corporation Information Management Executive Summary will be tabled to the Sub-Committee for approval at the next committee meeting.

RESOLVED – That the Sub-Committee notes the report.

9. **IT DIVISION - IT SERVICE DELIVERY SUMMARY**

The Sub-Committee received a report of the Chamberlain on the IT Division – IT Service Delivery Summary.

A Member asked how the organisation responds to the issues detailed in the report. Officers explained that the City of London has dedicated staff who work with stakeholders to resolve any issues.

RESOLVED – That the Sub-Committee notes the report.

10. **IT DIVISION RISK UPDATE**

The Sub-Committee received a report of the Chamberlain on the IT Division on the IT Division Risk Update. IT currently holds 2 risks on the Corporate Risk Register, whilst feeding into the GDPR Corporate risk which is owned by Comptrollers. There was a discussion around removing the CR16 the IT Security risk from the Corporate Risk Register however it was agreed that for the interim the risks should stay on the Corporate Risk Register. It was agreed that a paper would be produced on the current security maturity levels along with an outline of any further investments required to reach the necessary maturity levels.

It was further suggested that all IT Departmental Risks should be brought to the Committee as a regular item.

RESOLVED – That the Sub-Committee notes the report.

11. **IT DIVISION - IT DISASTER RECOVERY SUMMARY**

The Sub-Committee received a report of the Chamberlain on the IT Division – IT Disaster Recovery. There was a discussion on widening the Disaster Recovery processes to address business continuity issues. The wider test is planned for once the transformation programme is completed. A Member enquired when the next Disaster Recovery test is planned and why the annual test was missed. Officers explained that it was unfortunate that the annual test was missed, due to technical issues but every effort is being made to address this for as soon as possible. A member also requested that the Deputy IT Director consider how we can simulate a Disaster Recovery/Business Continuity exercise with a Denial of Service Scenario. This will be reported back at the next DSSC.

Members asked for a future report on the Disaster Recovery test.

RESOLVED – That the Sub-Committee notes the report and another report provided to a future committee meeting.

12. **CR 16 INFORMATION SECURITY RISK**

The Sub-Committee received a report of the Chamberlain on the CR 16 Information Security Risk. Officers informed Members that they are exploring ways to understand how the new Cyber Board toolkit can be adopted by the DSSC.

RESOLVED – That the Sub-Committee;

- Note the report.
- Consider the use of the Cyber Security Board Toolkit.
- Agree the recommendation to adopt the National Cyber Security Toolkit and a deep dive workshop run by the IT Security Director to customise the toolkit for the City of London Corporation.

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 3.18.

Chairman

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

Forward Plan – July 2019

Report Title	Report Month	Category	Who
IT Security Future Projects	September 2019	Strategic	GBH
Police National Enabling Programme Deep Dive	September 2019	Strategic	AB
Web Project Update	September 2019	Strategic	BR
Digital Services Strategy Update	September 2019	Strategic	SG
Print Policy and Members IT Policy	September 2019	Operational	SG
IT Operating Model Implementation Review	September 2019	Strategic	SG
Data Protection (GDPR) Policy Review	September 2019	Strategic	MC
Post 2020 Strategic IT Partner Procurement Update	September 2019	Strategic	KM
Smart Working Review	September 2019	Strategic	SC
IT Applications Roadmap	September 2019	Strategic	MG
Presentation from City Surveyors and DCCS	November 2019	Strategic	PW and AC
Denial of Service DR Test	November 2019	Operational	MG
2020 Procurement Sign off	November 2019	Strategic	KM
Update on Information Management	November 2019	Strategic	SG
2020 Sourcing Contract Award Contract and Progress Reports at each meeting	January 2020	Strategic	SG
IT Service Benchmarking Review	January 2020	Strategic	SG
IaaS to Cloud Migration	January 2020	Strategic	SG
Presentation from DBE and CoLP	January 2020	Strategic	TBA
Presentation from Economic Development	March 2020	Strategic	TBA
Presentation from Town Clerks	May 2020	Strategic	TBA
Presentation from Remembrancer	July 2020	Strategic	TBA
Presentation from Comptroller	September 2020	Strategic	TBA
Presentation from Barbican	November 2020	Strategic	TBA

Contributors

Sean Green – SG

Sam Collins - SC

Matt Gosden – MG

Andrew Bishop - AB

Kevin Mulcahy – KM

Sam Kay – SK

Gary Brailsford-Hart – GBH

Steven Bage – SB

Bob Roberts – BR
Jon Averbs – JA
Paul Wilkinson – PW
Andrew Carter - AC

Digital Services Sub (Finance) Committee– Public Outstanding Actions

Item	Meeting Date	Action and target for completion	Officer responsible	To be completed/ Next stage	Progress update
1	30/05/2019	Presentation from the Open Spaces on their Digital Journey Presentation to be rearranged for the next meeting.	Director of the Open Spaces	05/07/2019	Presentation on the agenda for the July meeting of DSSC
2	30/05/2019	Change and Engagement Update Member sought clarification on the benefits of the business case for the programme. It was agreed that a review will be carried out to explore the additional financial and non-financial benefits of the programme.	Director of IT	30/08/2019	Reported back at the September meeting of DSSC
3		City of London Corporation Information Management Executive Summary Members were assured that a revised paper on the City of London Corporation Information Management Executive Summary will be tabled to the Sub-Committee for approval at the next committee meeting.	Director of IT	05/07/2019	Paper on the agenda for the July meeting of DSSC
3		The IT Division – IT Disaster Recovery A member also requested that the Deputy IT Director consider how we can simulate a Disaster Recovery/Business Continuity exercise with a Denial of Service Scenario. This will be reported back at the next DSSC.	Deputy Director of IT	05/07/2019	Paper on the agenda for the July meeting for DSSC

Committee(s)	Dated:
Digital Services Sub Committee	5 th July 2019
Subject: City of London Corporation Information Management Executive Summary	Public
Report of: The Chamberlain	For Decision
Report authors: Sean Green – IT Director	

Summary

Following the presentation of the Information Management (IM) Strategy in December 2018, Summit requested that an IM Executive Summary should be developed that explained the benefits and principles removing any specialist terms.

It is accepted that IM is not in a good state at the City of London Corporation (CoLC). For example, we keep information for too long in silos that makes it more difficult to find the information we need easily and costs money in storing information for longer than is required or useful.

IM is a whole organisation responsibility with IT, HR, Corporate Strategy and Performance and Comptrollers have a lead function in enabling the achievement of the IM Strategy in the organisation.

In the current climate of financial constraint and the fundamental review the pace of delivering the IM strategy may need to be reviewed later in the year.

The strategy is summarised by the following key principles:

- Information acquired by any part of the City Corporation becomes an asset for all the organisation;
- Information is stored securely once and kept up to date while needed and safely disposed of afterward;
- We share information appropriately across the organisation, with partners and with the public;
- Authorised people have easy access to information and to the tools and skills to get the most out of it;
- We promote the culture and leadership needed to look after, share and use information wisely.

This paper provides Members of this Committee with the Executive Summary version of the Strategy agreed by Summit in March 2019 (See Appendix A – IM Strategy Executive Summary attached).

Recommendation(s)

Members are asked to:

- Agree the IM Executive Summary – Appendix A

Main Report

Background

1. In October of 2017 Summit agreed the proposal presented to carry out an Information Management (IM) review at CoLC to gain an understanding of the current state of IM strengths and weaknesses for CoLC and provide a roadmap to become a mature IM organisation through completion of an agreed set of deliverables.
2. When the IM Strategy was presented to Summit in December 2019 a request was made that an IM Executive Summary should be produced.
3. The IM Executive Summary is attached as Appendix A.
4. A new Corporate risk associated with the delivery of the IM Strategy was agreed by the Audit and Risk Committee at their May meeting.

IM Definition

5. For the purposes of the IM Strategy, information management is defined as the collection, storage, dissemination/sharing, archiving and destruction of information both electronic and paper. Good information management underpins good information, which in turn underpins good intelligence, which in turn underpins good decision-making.

IM Current State

6. Some of the IM problems identified from a review carried out last year that we need to resolve are:
 - CoLC keeps too much information that we don't really need
 - CoLC keeps too much information in (obscure) silos and struggle to share and reuse it
 - CoLC has poor quality of information, including lack of consistency, unnecessary duplication, out-of-date information and large amounts of unstructured data, resulting in no "single version of the truth" and no "one source" for each data set
 - CoLC focuses on management information and performance reporting rather than analysis and performance improvement. "Hindsight".
7. This has negative impacts on the CoLC, its departments and individual staff and customers:
 - cost – of storage, both electronic and physical

- quality – of decisions and actions based on incomplete or out-of-date information
- time – of people spent looking for the information they need
- risk – of information breaches leading to regulatory sanctions and bad publicity. We also risk losing valuable information that is poorly organised when staff leave our organisation.

Information Management Strategy Summary

8. We want to be in a position where the right people have the right access to the right information, in the right way, for the right reason at the right time.
9. This strategy is not just about compliance with legislation. The main driver behind this strategy is the realising of the value of our information and data estate. To this end, we will ensure that we create and collect the right information for the right purpose and reuse that asset where possible.
10. The information needs to be of high quality, correct, complete, reliable, up to date and accessible and we will put in place and develop the relevant skills, tools and behaviours to make sure this is achieved.

Delivering the IM Change

11. No single team can achieve the vision set out in this strategy alone. We all need to have a commitment to improving information management and the use of information in CoLC, working together and learning from areas of good practice and innovation from within both the private and public sectors.
12. To be successful in delivering outcomes and priorities detailed in the IM Strategy there are many different strands which will have different leading service areas:
 - IT for infrastructure, tools and engagement;
 - HR for training and behaviours;
 - Corporate Strategy and Performance for data use and change management;
 - Comptrollers for compliance with information management legislation.
13. Strong governance and oversight are needed if we are to land the positive changes outlined in the strategy and avoid continued replication of the current state. This will be provided by the Digital Task and Finish Group and the Information Governance Group.
14. We will measure our progress towards the vision through a set of activity and performance measures; as well as through softer measures derived from surveys and interviews.
15. We will develop a plan to deliver the IM Strategy and mitigate the actions detailed in the IM Corporate risk.

Corporate & Strategic Implications

16. This strategy will be a key driver behind Corporate Plan outcome 10 'We inspire enterprise, excellence, creativity and collaboration' and outcome 9 'We are digitally and physically well-connected and responsive' whilst also contributing to outcomes 1,2,3,4,8,12.

Financial Implications

17. The capital investment funding to deliver and IM programme will be considered via the Medium-Term Financial Strategy and in year projects through bids for Transformation funds. It estimated capital funding in the order of £2-3m will be required to deliver a 4-year roadmap of IM improvements. If funding is not available there are some incremental changes the organisation can make in the areas of culture, skills and the use of shared drives; however, the changes will be incremental rather than transformational to the organisation.

Conclusion

18. Improving information management practices should be a key focus for CoLC as it is for most organisations, across both the public and private sectors.
19. This is driven by a range of factors, including a need to improve the efficiency of business processes, the demands of compliance regulations (General Data Protection Regulations) and the opportunities for better decision making with better quality, easy to consume and timely information.
20. Next steps during the next 12 months include the following:
 - a. Develop and agree relevant IM Metrics
 - b. Introduce IM Coding and Classification
 - c. Introduce and implement an updated records management policy
 - d. Introduce standard file naming convention
 - e. Migrate from shared drives to Microsoft Sharepoint/Teams
 - f. Implement new business intelligence infrastructure, reporting and analytics
 - g. Set up and implement new information governance and reporting training for all staff across the CoLC.

Sean Green

IT Director
Chamberlain's Department

E: Sean.Green@cityoflondon.gov.uk

Appendices

Appendix A - IM Strategy Executive Summary
Appendix B - Draft IM Plan

Appendix A - Information Management Strategy - Executive Summary 2018-23

What is information management?

Information management is the formalised collection, storage, analysis, use, sharing and disposal of all types of information, from data through to knowledge. This can mean gathering, creating, filtering and disseminating information, using it to support decisions and actions, or conserving or disposing of it. Recent research across the City of London Corporation shows that the way in which information is managed varies significantly. Poor information management incurs significant costs in terms of ill-informed decision-making, missed opportunities and missed threats. Even where the right information is used properly, there is often effort and delay in obtaining and verifying it.

Why information management matters

The more we know and understand, the better we can decide and act, particularly for our stakeholders. Improper gathering, disseminating and analysing of information can put those people at risk. That's why data protection legislation has been passed to regulate this, with stiff penalties for contraventions.

Good information management provides benefits across the City Corporation and for our stakeholders. Its principles are relatively straightforward, but its implementation is made complex by the breadth and depth of its applicability and interdependencies. This is why a strategic approach is required, as set out in the City Corporation's Information Management Strategy Principles (Appendix 1).

How good information management help us

Good information management improves all aspects of designing and delivering services to our stakeholders, but particularly:

- Identifying and measuring service need – what is the problem and how widespread is it?
- Determining service options – what can be done to solve/mitigate the problem, what is the best service solution?
- Designing services for efficiency and effectiveness – making services easier to understand and navigate; encouraging service uptake; minimising blockages and delays; minimising rework;
- Service performance management – is the service working as intended? what are the right performance measures? what can be improved?
- Joined-up approach – what other services might a recipient need and how can these be best co-ordinated?
- Working with partners – getting them the right information; measuring their performance;
- Identifying who isn't being served – identifying gaps in offerings and uptake.

Below are some examples of good information management in action:

- Tell us once – by using information gathered and verified already;
- Pre-filling information on forms - saves customers time and gives them the opportunity to update it;
- Identifying multiple occupancy in a supposedly single-person home;

- Improving property and asset utilisation - so spare capacity can be put to good use or disposed of;
- Improving preventative maintenance - recognising the most effective/ efficient type and timing of maintenance for assets;
- Reducing homelessness - identifying early those people at risk;
- Identifying children at risk early - allowing less intrusive interventions and preventing issues escalating to care orders;
- Better managing shipping of animals across borders - easing reuse of information for high-volume shippers;
- Increasing revenue from visitors to Tower Bridge, Barbican and Monument through acceptable cross-selling based on allowed analysis of visitor and demographic data.

The next steps (See Appendix 2 and 2a)

Technical: Implement the required information management infrastructure.

Policy and skills: Implement skills training for improved information and data literacy, identifying champions in each department/team.

Culture and ways of working: Work with Senior Officers to see how objectives can be translated to departmental business plans and individual's objectives.

Maximise the benefit: Using central analytical resources and working with departments on requirements and priorities where this can be of benefit e.g. preventative measures, saving money, and making better informed decisions.

In summary

The key to information management success is making it an intrinsic and beneficial part of everyday behaviour, rather than treating it as an afterthought or overhead.

The City Corporation will use the principles above alongside recognised good practice standards to develop policies, processes, technologies and leadership that support and encourage the behaviours we need. The built-in continual improvement ethos will ensure that these keep pace with changing business needs.

Appendix 1 - What good information management entails

The right people have the right access to the right information, in the right way and for the right reason at the right time.

To achieve this will need a combination of the right culture, tools and processes, guided by five key information management principles that have been defined for the City of London Corporation:

- **Information acquired by any part of the City Corporation becomes an asset for all of the organisation**
Information will be open, transparent and available across the organisation. Our staff are custodians of our information assets. We only restrict information for legal, commercial or privacy reasons.
- **Information is stored securely once and kept up to date while needed and safely disposed of afterward**
We will educate, encourage and enable staff to store a single version of information that can be added to and amended. We will discourage duplication and encourage information reuse and repurposing. We will insist on safe disposal of information when no longer needed.
- **We share information appropriately across the organisation, with partners and with the public**
We will enable staff to easily share our information by developing common standards and processes.

- **Authorised people have easy access to information and to the tools and skills to get the most out of it**

We will provide the information required – securely, quickly, easily, accurately, conveniently, consistently, and transparently. Systems will be procured, designed and developed to enable effective information sharing, analysis and presentation.

- **We promote the culture and leadership needed to look after, share and use information wisely**

We will develop and nurture new information management values and behaviours, including a drive to continually improve based on experience and research. We will encourage an approach of curiosity and challenge in the use of our information. Departments will be given the skills and capability to lead and champion this ambition.

Appendix B – High Level Activities Plan

IM Outcome 1: CoL has the necessary awareness, tools, skills and culture to promote a set of behaviours and values which understands and manages good information management practice.

CP Outcome 4: Communities are cohesive and have the facilities they need.

These activities focus on developing the values, behaviours and culture we need to deliver good information management. Each activity shows what we need to achieve if the change is to be long lasting and positively landed.

This is based on the ADKAR model¹:

- **A**wareness of the need for change
- **D**esire to support the change
- **K**nowledge of how to change
- **A**bility to demonstrate skills and behaviours
- **R**einforcement to make the change stick

Activities:

Activity Number	Goals and outcomes of successful change	Activity
1.01	Awareness	Research best practice across the private and public sectors – and benchmark against the performance of organisations providing similar functions.
1.02	Awareness	Introduce a tool to check and monitor compliance with GDPR, mapping information flows across CoL and to external stakeholders.
1.03	Awareness / Desire	Promote the importance and benefits of good information management to Chief Officers and Senior Leadership Teams. Identify data owners across the organisation who will be responsible for the quality, management and use of data.
1.04	Desire	Develop prototype analyses and self-service dashboards to show the “art of the possible” to service managers and Chief Officers.
1.05	Knowledge	Existing support offers for these tools to be refocused on “when” and “why” to use the tools rather than just “how” to use them.
1.06	Knowledge	Develop a training offer across CoL – identify gaps in knowledge and skills and develop a training plan for staff and Chief Officers.
1.07	Ability	Widen the adoption of the tools required for collaboration, with a focus on existing Office 365 tools such as Sharepoint and Teams, reducing volumes of information stored on unstructured H ad W drives, duplication, collaboration via email and time spent

¹ <https://www.prosci.com/adkar/adkar-model>

Activity Number	Goals and outcomes of successful change	Activity
		looking for information. Widen the use of Power BI to develop self-service capabilities.
1.08	Ability	Provide detailed training, guidance and ongoing support for all staff in the use of information management tools.
1.09	Reinforcement	Identify champions or super users across Information Management disciplines from within existing services. Develop a “community of interest” where officers can discuss problems, share and develop skills and solutions; as well as develop solutions to problems.
1.10	Reinforcement	Determine the change management resources and requirements, ongoing support and training needed to positively land the strategy.

IM Outcome 2: CoL’s information estate is safe, relevant, accurate, reliable, used and trusted.

CP Outcome 12: Our spaces are secure, resilient and well-maintained.

These activities focus on the information lifecycle stages -

Activities:

Activity Number	Information Lifecycle Stage	Activity
2.01	Initiate	Design and build an information asset register for CoL and implement a security classification approach. Define access permissions and retention criteria for our information.
2.02	Initiate	Develop an approach where analytical products identify intelligence gaps which inform future application development.
2.03	Initiate	Form Digital Services Steering Board to oversee and prioritise the business intelligence project pipeline; considering both ethics and statutory compliance.
2.04	Populate	Implement information classification tools across CoL and develop a search facility of our information asset.
2.05	Retain	Identify data and information owners across CoL, and support and train them in their roles and responsibilities. Complete annual information asset audit.
2.06	Retain	Complete migration of unstructured data
2.07	Maintain	Develop a single source of information; including an integration layer of our data sources. This will include transforming and standardising our data to ensure it is amenable for analysis.
2.08	Maintain	Ensure all staff have completed Data Protection training. Implement information tracking tool to identify flows of information throughout the CoL and beyond.
2.09	Maintain	Implement Annual Data Protection compliance audit, and best practice in terms of information management and sharing.
2.10	Maintain	Develop information security function for CoL.

Activity Number	Information Lifecycle Stage	Activity
2.11	Share	Develop communications plan about information sharing. Develop Corporate Register of Information Sharing Protocols and agreements (with owners and review dates).
2.12	Share	Develop protocols and mechanisms to receive (and share) data with external parties.
2.13	Dispose	Review and revise information disposal policies and identify safe routes for this to happen.
2.14	Dispose	Develop a consistent approach to records management across the Corporation and develop tools to identify information that can be safely disposed of.

IM Outcome 3: CoL derives real value and benefits from the use of information, data, analysis and modelling.

CP Outcome 7: We are a global hub for innovation in financial and professional services, commerce and culture.

The activities in this outcome focus around the exploitation and *use* of data and using innovative tools and techniques to drive value, open collaboration and innovation.

Activities:

Activity Number	Activity
3.01	Put tools in place to automate manual data processes, improving efficiency and productivity.
3.02	Widen the roll out of self-service visualisation tools across the Corporation. Develop dashboards and analyses for services and support them in their use.
3.03	Develop a pipeline of dashboards and analytical products to be developed. Identify the benefits of each project.
3.04	Develop an approach to prioritisation of analytical projects to be overseen by the Digital Services Steering Board.
3.05	Develop an approach to benefits realisation and monitoring. Identify potential secondary benefits of projects.
3.06	Develop problem articulation skills across the Corporation (business requirements) – This will help the culture shift from performance to intelligence with a focus on a culture of enquiry and asking “why?” Problem solving needs to focus on the underlying condition not the presenting symptoms.
3.07	Develop prototypes illustrating how advanced analytics such as prediction, prescription and system modelling can drive improvements, realise benefits and improve service delivery.
3.08	Form an analyst network to reinforce the change, develop and share skills, collaborate and innovate.

IM Outcome 4: CoL has sufficient checks, balances and oversight to ensure the successful implementation of this strategy.

CP Outcome 5: Businesses are trusted and socially and environmentally responsible.

The focus of activities in this outcome centre around compliance, assurance and monitoring. The programme needs to have effective governance and oversight mechanisms in place if we

are to positively land the change required and reinforce it to make sure continual improvements are made.

Activities:

Activity Number	Activity
4.01	Ongoing programme of consolidating applications and reducing the fragmentation of our data and information.
4.02	Programme of identifying legacy systems which require renewal and upgrades, assessing options for integration with existing systems or procurement of new solutions.
4.03	Identification of organically grown spreadsheets and databases within services – and develop a programme of incorporation into main applications. Ad hoc systems to be disposed of.
4.04	Development of an ongoing mechanism to catalogue and manage our information asset, identifying data owners and applying security classifications where relevant. Provide a mechanism to search through the asset.
4.05	Ensure that procurement is informed, and where necessary enforced by the IT and Information Management strategies – ensuring compliance with general direction, data standards, security and sharing protocols.
4.06	The Information Management Board will develop a CoL wide register of all Information Sharing Agreements and Protocols, identifying owners and review dates; and oversee the development of any new sharing mechanisms.
4.07	Develop a standard approach to the development of information sharing protocols and agreements between CoL and external partners.
4.08	Develop a mechanism to review what information and datasets can be openly (publicly) published over and above the existing requirements of the Transparency Code.
4.09	Create a Digital Services Steering Board to prioritise and oversee the development of the analytical capability, ensuring that benefits are realised, compliance, and coherence of all related strategies and policies; as well as the implementation of the Information Management Strategy.
4.10	Inform wider procurement - ensure that our contractors comply with our standards, policies and strategies; and ensure that we have direct access to performance and activity data and information about that provision – clauses in contracts (including exit provision).

This page is intentionally left blank

Committee(s)	Dated:
Digital Services Sub Committee – For Information	5th July 2019
Subject: Social Responsibility	Public
Report of: The Chamberlain	For Information
Report authors: Eugene O’Driscoll, Agilisys Client Services Director	

Summary

Driven by the City Corporation’s responsible business commitments and as part of the Responsible Procurement Strategy 2016-19, social value and ethical sourcing requirements were integrated into the terms of the contract renewal between City of London Corporation and Agilisys Limited in March 2018. This formed part of the overall Social Responsibility commitment.

Social value outcomes include work-related opportunities targeted towards local residents and/ or socially excluded groups, training workshops to support digital inclusion, a report on increasing the representation of women in tech and school visits to promote IT as a career.

The ethical sourcing deliverable was a supply chain mapping exercise, the first of its kind undertaken for the City Corporation, which examined human and labour rights due diligence procedures and relative risks up the supply chain of our Lenovo laptops, to the point of manufacturing at locations in China.

This report provides an update on progress in delivering on promises made regarding Corporate and Social Responsibility when the contract was renewed in March 2018.

The report is a reminder on the scope of the areas that were agreed to be covered and the activities delivered for each area of responsibility.

Recommendations

Members are asked to note this report

Main Report




1.0 Social Inclusion Agilisys Commitments




The groups that we agreed that would be covered and the targets we set were as follows:

- Apprenticeships - Maintain minimum of three Level 4 Apprentices (back-end/technical) working on CoL’s contract over the remaining two years of the contract.

- Work Experience (14-18 years) - Minimum of three-person weeks per year to provide work experience. Aimed at CoL academies in Islington, Southwark, Hackney and/or youth organisations in London 10% most deprived boroughs.
- Work Experience (19+ years) - Minimum six person-weeks per year 19yr + work experience placements targeted towards socially excluded groups in London's 10% most deprived boroughs, including Barking, Dagenham and Tower Hamlets.
- Women in IT - A 4-page summary report on key findings from Agilisys' existing initiative, which aims to increase interest in the IT sector amongst women, that CoL can use to generate ideas on addressing any similar internal issues within STEM specialties. The Report should be clear and simple, focusing on transferable information, success factors, overcoming barriers and lessons learned.
- School visits - 2 visits per year to schools/ colleges, to provide career insights, raise awareness about vocational and academic career paths into the IT industry particularly raising awareness about areas where there are skills gaps.
- Training Workshops - Two training workshops per year to support digital inclusion, targeted towards socially excluded groups
- Responsible IT Procurement - A supply chain map to be produced identifying where and to what extent ethical sourcing risks exist within the supply chain of ICT equipment (Lenovo) being used on CoL's contract (see appendix A – Supply Chain Sustainability). Specifically, to identify highest risk of the infringement of UN International Labour Organisation (ILO) fundamental conventions. Please refer to Appendix A - attached presentation 'Supply Chain Sustainability Study'.

2.0 Progress Update 2018-2019 and 2019-2020

Commitment	Update	RAG status
Apprentices	Level 4 Network Engineers (18-month apprenticeships) <ul style="list-style-type: none"> • 1 started October 2018 • 2 started 12th November 2018 	Green 
Work experience 14-18 years	<ul style="list-style-type: none"> • Year 1 delivered March 2018 • Year 1 delivered July 2018 • Year 1 March 2019 (cancelled due to candidate illness) • Year 1/2 March to July 2019 at CoLP • Year 1/2 March to July 2019 at CoLP • Year 2 delivered May 2019 • Year 2 delivered June 2019 • Year 2 pending July 2019 • Year 3 pending May 2020 	Green 
Work experience 19+ years	<ul style="list-style-type: none"> • Year 1, 6-week placement took place between February and March 2019 • Year 2, planned November 2019 • Year 3, planned March 2020 	Green 

Commitment	Update	RAG status
Training Workshops	<ul style="list-style-type: none"> Year 1 First workshop delivered 3rd December 2018 Year 1 Second workshop delivered 15th April 2019 Year 2 planned September 2019 Year 2 planned February 2020 Year 3 planned July 2020 	Green 
Women in Technology	Report submitted February 2019. Being reviewed by Responsible Procurement Manager. An offer of a workshop has also been made to City of London colleagues.	Green 
School visits	<ul style="list-style-type: none"> Year 1 visit completed on 5th November 2018. Year 1 visit completed 2nd May 2019. Year 2 visit arranged June 2019 but cancelled by school. To be rearranged Nov 2019 Year 2 planned Mar 2020 Year 3 planned June 2020 	Green 

3.0 Work experience Testimonials

Work experience 14-18

“Thank you so much for hosting Kito on work experience. He found his week very interesting and rewarding and it has clearly improved his confidence. Yesterday, he told me that he was very sad it was coming to an end so soon and did not want to go back to school!

I hope he did well and showed initiative and good communication skills, do let me know if you have any feedback.

Thank you again and have a lovely week-end”

School visit

“Thank you for the apprenticeship talk and the museum visit this afternoon. We appreciate your warm welcome and the students were very positive about the possibility of pursuing an apprenticeship.”

Work experience 19+ years

“Today is my last day in Agilisys and I have learned a lot. I want to seize this opportunity to say thank you very much for your kindness.”

4.0 Women in Technology report

4.1 Agilisys are committed to producing a 4-page summary report outlining the initiatives within Agilisys aimed at increasing more women in technology roles, which City of London could use to generate ideas to tackle low female representation.

4.2 A summary of the salient points in the report are as follows:

- The number of young women opting for STEM subjects is traditionally low, and whilst this is increasing, they do not then often choose a career in these areas. This restricts the talent pool and means low female representation in the technology sector.

- The Agilisys Women’s Empowerment (AWE) Group was formed in November 2017 to tackle the issue within Agilisys.
- The AWE sponsored a survey in March 2018 to identify the key issues to focus on, with 10% of the organisation completing this.
- The survey highlighted the following themes which should be tackled in order to increase female representation in technology roles:
 - Education and Schools – as a result Agilisys have created several opportunities for work experience and celebration events and taken part in careers fairs.
 - Promoting role models – as a result Agilisys have participated in awards and recognition
 - Mentoring – Agilisys will be ensuring those we are able to recruit, remain within the organisation.
 - Reviewing recruitment practices and policies.
- Whilst Agilisys work experience opportunities may have some local impact, they will need to go further to have a real impact within the organisation and effect change.
- The awareness that has been created from these initiatives has created momentum within the organisation to the extent that Agilisys are considering a series of commitments Agilisys can sign up to, particularly with regard to recruitment practice, to increase female representation. Agilisys have secured their Senior Leadership buy-in to these currently.
- Agilisys would be delighted to host a follow-up workshop with City of London colleagues which discusses these initiatives and explores opportunities for sharing knowledge/joint working.

Eugene O’Driscoll
 Client Services Director
 Agilisys

E: Eugene.Odriscoll@cityoflondon.gov.uk

Appendices

Appendix A – Supply Chain Sustainability



Page 25

Supply Chain Sustainability Study

By Douglas Moore

For the Corporation of the City of London

Commercial in confidence

Agenda

1. About the laptop
2. Key components
3. Summary
4. Recommendations

The laptop in question

Page 27



Item	Manufacturer
CPU	Intel
RAM	Samsung
Storage	Samsung
Sound	Realtek
Chipset	Intel

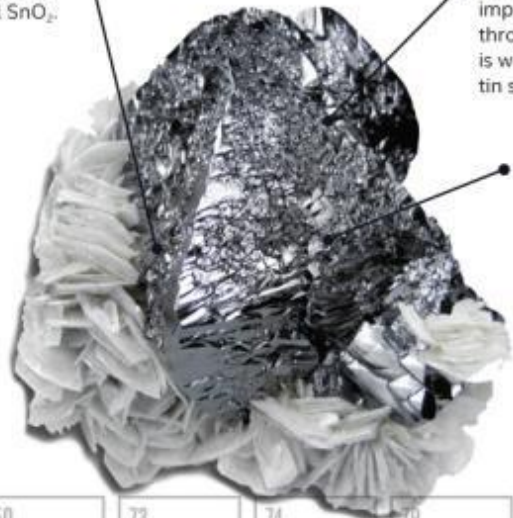
From your desktop to mine



FROM THIS

CASSITERITE

Tin oxide mineral with the symbol SnO_2 .



It has been the most important source of tin throughout history, and is where most of today's tin still comes from.

It can also be used as a gemstone, with its beautiful and unique crystals.

50 Sn Tin	73 Ta Tantalum	74 W Tungsten	79 Au Gold
------------------------	-----------------------------	----------------------------	-------------------------

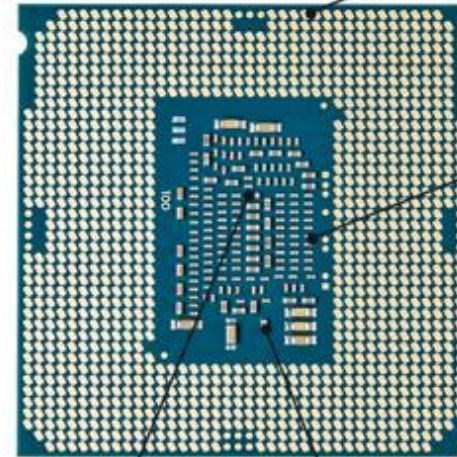
TO THIS

GOLD

Pins in processors are often made of gold, because it's conductive but not corrosive.

TIN

Often used as a replacement for lead in printed circuit boards and processors, and used to solder pieces together with devices.



TANTALUM

The key ingredient in tantalum capacitors, which can be used in devices that require high performance in a small amount of space, like laptops.

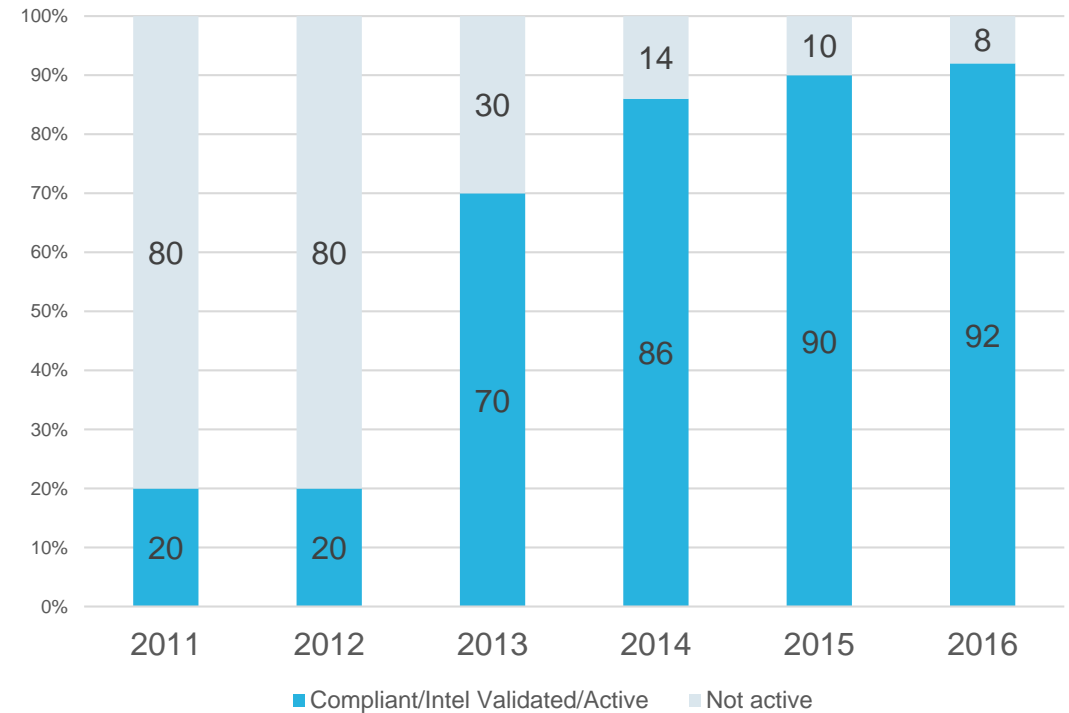
TUNGSTEN

Because of its chemical properties, it's used to conduct electricity in integrated circuits and metallic films.

263 (approximately 92%) of the smelters and refiners in Intel's supply chain have either:

- (i) received a conflict-free designation from an independent third party audit programme,
- (ii) begun participating in such a programme or;
- (iii) have been determined to be conflict-free (through our own due diligence).

Smelters and Refiners Compliance Summary

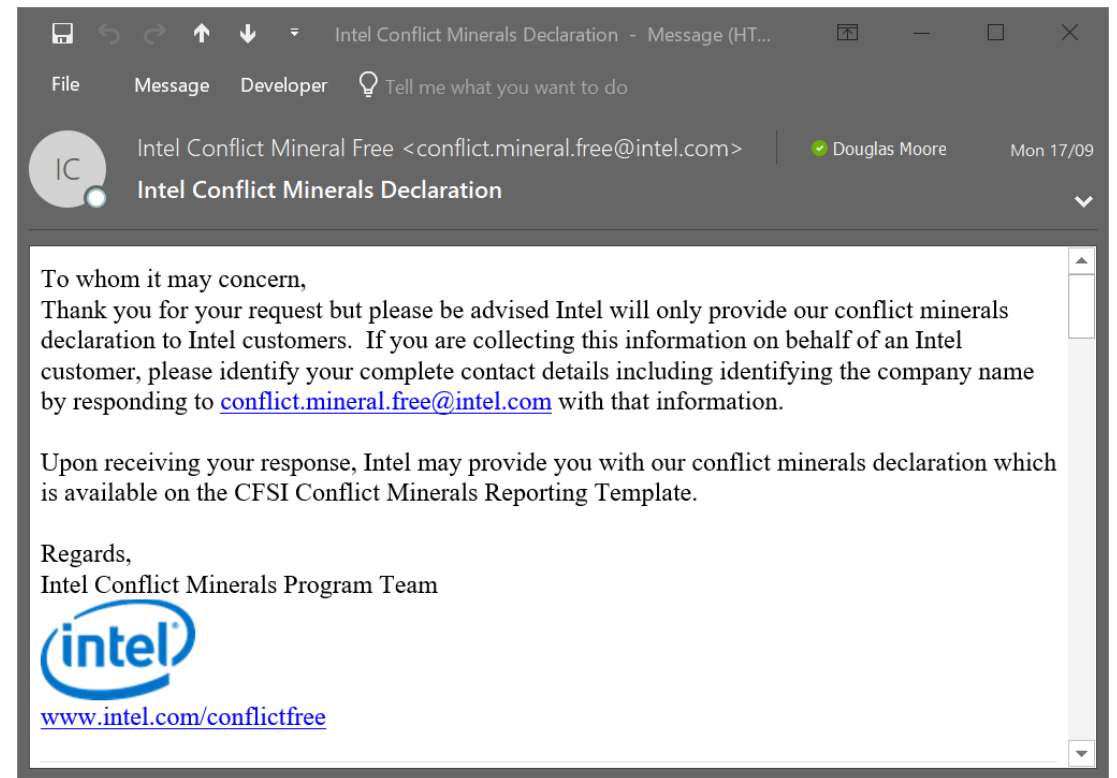


Intel

Intel's 14 nm process and lead system-on-a-chip (SoC) product are now qualified and in volume production, with fabrication facilities in Oregon (2014), Arizona (2014), and Ireland (2015).

Page 31

Intel don't release details about the source of the minerals involved in the manufacturing of their chips, unless you are a direct customer of Intel.

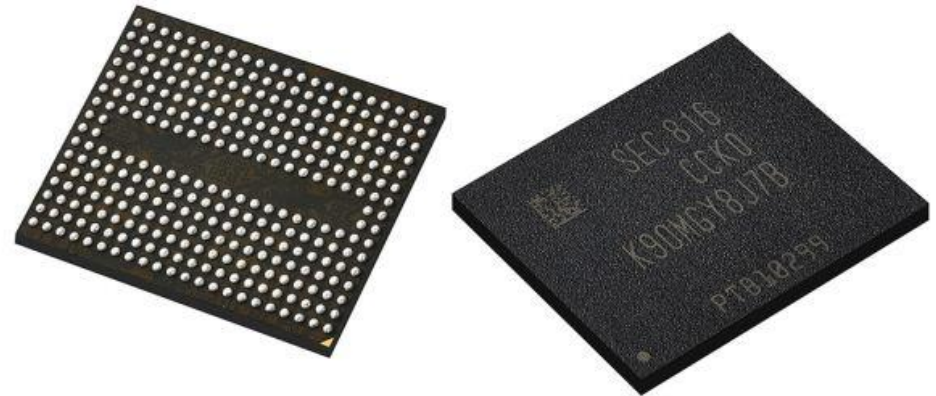


Samsung

The chips manufactured by Samsung that are used in the laptop form two key components;

- Solid State Disks
- DDR RAM

The manufacturing process and functions of the semiconductors are similar to those used by Intel.



Samsung

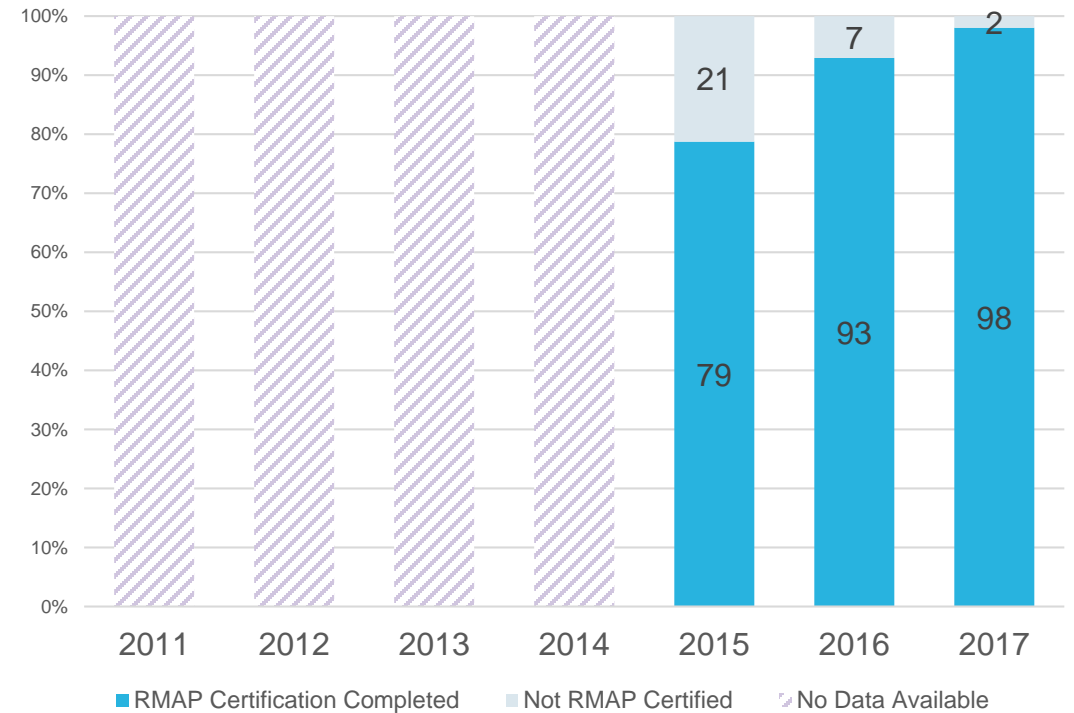
Conflict Mineral Smelters and Refiners Compliance

255 of the smelters and refiners in Samsung's supply chain, approximately 98%, have either;

- received a conflict-free designation from an independent third party audit program
- begun participating in such a program,
- or through our own due diligence been determined to be conflict-free.

Page 33

Smelters and Refiners Compliance Summary



Realtek

Realtek are the worlds largest manufacturer of on-board audio semi-conductors. They have an estimated market share of 50-60%.

Page 34 We encountered difficulty in confirming any information about Realtek, and the company is less transparent in its Conflict Mineral sourcing than its peers.

They do not appear to be following the Responsible Minerals Assurance Process and we suspect they should use more robust auditing to ensure their supply chain is sustainable.

“Realtek's suppliers are required to provide a Conflict Mineral Policy Statement and written certificate that no minerals from conflict-affected locations are used in the manufacture of Realtek products, thereby assuring that Realtek products contain no conflict minerals.”

Lenovo

All Lenovo global manufacturing locations are ISO 9001 (quality), ISO 14001 (environmental) and OHSAS 18001 (health and safety) certified.

Page 35 In addition to this, Lenovo states “all key procurement personnel are trained semi-annually on sustainability concerns” to ensure that sustainability risks are removed from the supply chain.



Lenovo

Conflict Mineral Smelters and Refiners Compliance

82% of the smelters and refiners in Lenovo's supply chain have either received a conflict-free designation.

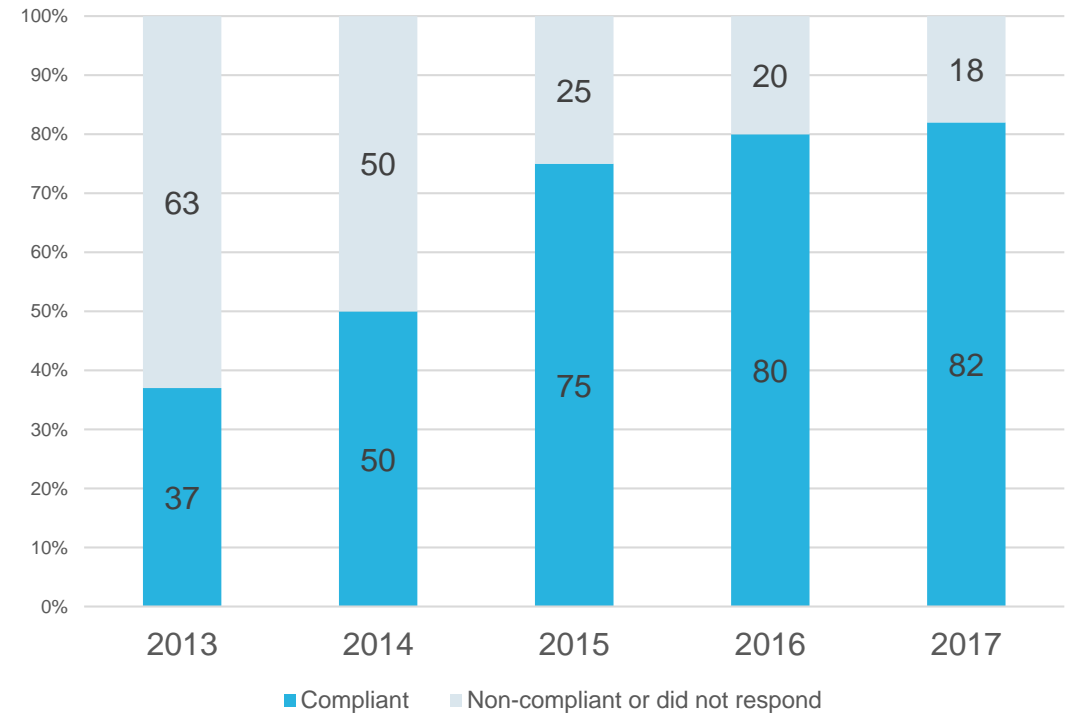
Page 36
Lenovo stated that;

“2017 was limited due to two causes;

- First, we on-boarded several new suppliers who did not have robust conflict mineral DD programs.*
- Second, several previously compliant SORs became non-conformant during the year.*

Lenovo will take further steps in calendar year 2018 to improve our efforts and to continue our results. We have a goal of improving our overall conflict-free posture to 90% by end of CY2018.”

Smelters and Refiners Compliance Summary



Lenovo

ILO Declaration on Fundamental Principles and Rights at Work

Lenovo is a signatory to the U.N. Global Compact, committing to the [10 principles](#) of human rights, labor, the environment and anticorruption.

Page 37

Lenovo states that it manages all operations consistent with the spirit and intent of the U.N. Universal Declaration of Human Rights and the International Labor Organization (ILO) [Declaration on Fundamental Principles and Rights at Work](#).

Audit data on performance against these commitments was not made available or in the public domain. Agilisys cannot confirm compliance with these statements.

Lenovo

Occupational Safety and Health

All Lenovo manufacturing locations are OHSAS 18001 certified by [Bureau Veritas](#).

Page 38
Lenovo also conducts regular site and corporate self-assessments using [Responsible Business Alliance](#) (RBA) templates. The results of the risk assessments are documented on this page.

Agilisys was unable to review any of the actual audit data, and our visibility was limited.

Facility Name	Score (%)	Risk Rating
Lenovo Corporate	94.4	Low
LCFC (Hefei, China)	86.8	Low
Wuhan Plant	90.4	Low
Beijing Plant	93.6	Low
Chengdu Plant	95	Low
Huiyang Plant	94.1	Low
Shanghai Plant	93.7	Low
LIPC (Shenzhen, China)	94.1	Low
LSTC (Shenzhen, China)	94	Low
USFC (Whitsett, N.C., U.S.A.)	85.1	Low
Monterrey, Mexico	88.2	Low
Pondicherry, India	91.4	Low
Indaiatuba, Brazil	89.2	Low
NEC (Yonezawa, Japan)	90.8	Low

Lenovo Risk Assessment Data for FY 2017/18

SCC

The distributor of this laptop was SCC. Laptops may be shipped direct from the manufacturer, or from the distributor warehouse in the UK. We reviewed their delivery supply chain to identify any risks.

Company	Overview	Risk
TNT	Part of the FedEx group. Documented corporate social responsibility policies. However, lacks detail on carbon footprint, and emissions.	Very Low
Bonds Worldwide	Small UK company, based in Birmingham.	Low
UK Mail	Part of DHL. Target of “zero emissions” by 2050. Offers suppliers training in 26 languages on DHL’s Global Code of Conduct that covers human rights.	Very Low
Paul Ponsonby Limited	Small UK company, based in Birmingham.	Low



Page 40

Summary

Report Summary

Should the City of London be concerned about the supply chain sustainability of Lenovo laptops and the sourcing of minerals?

Page 41

Not at this time.

Following the procurement responsibility programme, we can confirm that Lenovo and key component manufacturers (such as Intel) use international standards to maximise their supply chain sustainability. This doesn't mean we should be complacent, or that improvements can't be made. There is a general lack of transparency beyond the key component manufacturers. Third party auditing might highlight issues that are not visible to Agilisys at this time.

Contents Summary

- What we've learnt from this investigation.
- Areas that the industry could improve upon.
- Recommendations for further supply chain reviews.
- How intelligent procurements could drive sustainability.

What we've learnt

Growing Importance

Supply chain sustainability is important to the producers of commodity IT goods.

Manufacturers are increasingly pro-active, and self reporting forms a significant element of their annual disclosure to investors.

Standardised Reporting

The embrace of programs such as the Responsible Minerals Initiative Assurance Program (RMAP) allows buyers to compare the supply chain of electronic manufacturers, without the need for bespoke auditing.

Further to go...

The information provided by manufacturers has limited depth, and true transparency is not available at this time.

Areas that could be improved upon

Toxic Chemicals

The chemicals used to fabricate semiconductors are toxic. 43% of Intel's waste is classified as hazardous.

There is very little information published by manufacturers (Intel, Samsung, AMD).

Water Wastage

Semiconductors fabrication also uses a large volume of water.

Fabrication technologies that reduced the amount of water used in the manufacturing process would benefit the environment.

Recommendations for further supply chain reviews

- Undertaking a detailed supply chain review can be resource intensive and requires a combination of specialist skills, knowledge and proficiency in foreign languages.
- Business relationships are required to get access to detailed information that will support an investigation relating to a specific enquiry.
- If the authority wished to conduct its own review of other IT equipment, Agilisys recommends they use a combination of personnel who have the following skills;
 - an understanding of the finished product, possibly with a background in manufacturing,
 - an understanding of chemistry, the chemicals and raw materials used in the product components,
 - and knowledge of which chemicals and raw materials are at a higher risk of sustainability issues.

How could intelligent procurements drive sustainability?

Page 45



Score the tenders based on supplier RMAP compliance

The use of the RMAP standards across suppliers allows comparison between vendors. As these often form part of SEC filings, you can be confident of the information.



Refresh cycles and flexible working has an impact on the environment

Not all laptops are not designed to be upgraded or fixed. Awarding points for modular designs, and longer warranties will reduce waste.



Request carbon neutral shipping

While the end buyer can't directly influence the distant supply chain shipping methods, it can specify the last mile. Make it a requirement for carbon neutral shipping.



Leverage buying power

Each manufacturers was keenest to support this investigation when they believed it might lead to a sale. In the absence of an immediate purchase opportunity they become disinterested.

Page 46



AGILISYS


Third Floor, One Hammersmith Broadway
London, W6 9DL

☎ +44 (0)845 450 1131

✉ info@agilisys.co.uk

www.agilisys.co.uk

 Agilisys

 @Agilisys

What are RMAP Conformant Smelters & Refiners

Smelters and refiners on the Active list are participants in the RMAP and have committed to undergo a Responsible Minerals Assurance Process (RMAP) assessment. Smelters and refiners are identified as Active in the RMAP once they have scheduled the assessment date.

Page 47 Smelters and refiners on the Active list are at various stages of the assessment cycle, anywhere from scheduling the assessment date to undergoing the assessment enacting corrective actions in the post-audit phase. The time it takes a smelter to complete an assessment cycle varies, the average time is approximately nine months. During this time, RMI will not share details about a smelter's progress, in accordance with provisions in the AECI.

Companies can be removed from the RMAP Active List for a number of reasons: if the company is deemed by the RMAP to be delaying an assessment, corrective action completion, or re-assessment for more than 90 days; not progressing to the next steps in the assessment process within a reasonable timeframe; or unresponsive for 45 days.



[Link to all Conformant Smelters](#)

This page is intentionally left blank

Committee(s)	Dated:
Digital Services Sub Committee – For Information	5th July 2019
Subject: Draft IT Business Plan 2019/20	Public
Report of: The Chamberlain	For Information
Report authors: Sean Green – IT Director	

Summary

The IT Division Draft business plan for 19/20 details our objectives and priorities to ensure that we continue to deliver secure and stable IT services whilst supporting our customers across the City of London Corporation (CoLC) and the City of London Police (CoLP) in the delivery of more efficient and effective services.

Our top line objectives are summarised to:

- Act as an enabler for efficiency and value for money across all service areas
- Ensure safe, secure, stable and responsive Digital and Information solutions
- Develop our “One Team” focus to strengthen the links between teams and the provision of a joined-up service

The IT Division have summarised our priorities for 19/20 in the attached plan (see appendix A).

The plan also includes actions to support the further capability and development of staff who work within the IT Division.

The IT Division plan will be updated annually.

Recommendations

Members are asked to note this report

Main Report

1.0 Objectives

Our top line objectives for the IT Division are to:

- Act as an enabler for efficiency and value for money across all service areas
- Ensure safe, secure, stable and responsive Digital and Information solutions
- Develop our “One Team” focus to strengthen the links between teams and the provision of a joined-up service

Our objectives will be delivered through training, projects and developing the capabilities of our staff.

2.0 Summary of the IT Division Priorities

Our priorities for 19/20 can be summarised as follows:

- Drive forward digital adoption
- Optimise operational efficiency
- Deliver safe, secure and stable IT/Digital Services
- Deliver technology enabled business change and transformation
- Continue to create and engage a supportive environment for all our staff

We will be able to deliver the priorities through several projects, programmes and supporting new initiatives defined by the fundamental review.

3.0 Summary of IT Key Deliveries for 19/20

3.1 IT Deliverables in relation to departmental / service programmes and projects

- Help Departments to achieve their efficiency savings through adopting digital ways of working and the provision of finance and commercial support
- Deliver our own 2% savings as per our departmental efficiency plan (or more depending on the outcomes of the Fundamental Review)
- Implement improved processes to enable more efficient and effective working across the IT Division

3.2 Deliverables within corporate programmes and projects

- Work with Corporate Strategy and Performance to develop and implement the Digital and Information Management Strategies
- Provide expert IT direction to corporate programmes and projects
- Provide Technology support to departments to help them deliver their fundamental review of services and operations

How we plan to develop our capabilities this year

- Delivery of an in-house programme of training and secondments to build future capability
- Engage with our customers to better understand their business requirements

4.0 IT Metrics

Our key performance indicators:

4.1 Service Delivery

- Customer Satisfaction – 80%
- IaaS (Compute and Storage) – 99.9%
- P1 Incident Resolution – 98%
- P2 Incident Resolution – 87.5%

4.2 Savings and Efficiencies

Benefits Enabled in 19/20

- £250,000 of transformation savings realised from the 19/20 IT Budget.
- £100,000 (annualised) estimated of storage savings from the use of cheaper Azure savings.

Non-Cashable

- Enable travel savings from the use of Skype and staff time used up in travelling
- Enable reduced office footprint with staff working from different locations easily having the same office experience (higher staff to desk ratio).
- Enabling time saving for staff in being able to access information stored in shared drives more easily by using Sharepoint.

4.3 Increased adoption of digital ways of working

- We aim to have at least 500 regular users of Skype for Business by the end of the financial year.
- We will be rolling out further phases of CRM with the Events and Innovation and Growth teams
- We will be implementing information management tools to enable easier access, collaboration and reduce Data Protection risks
- We will be researching use of Robotics Process Automation for further roll out in teams across the CoL and CoLP following the pilot in Finance.
- We will be researching the use of Artificial Intelligence and Machine Learning with the Action Fraud system to improve the efficiency of crime resolution
- We will be supporting Corporate Strategy and Performance team with the enabling business analytics platform to improve preventative decision making in CoLC and CoLP.

5.0 Conclusion

The IT Business Plan for 19/20 helps the IT Division to focus our scarce resources on delivering our business as usual IT Services and Change activities in the most efficient and effective way.

The attached plan with the detailed priorities has been developed into a Gantt Chart (timeline) to help the Senior IT Management team monitor progress and consider the resource impact of any additional activities that the IT team may be required to undertake.

There are additional activities that will be added to reflect the support of CoLP projects and programmes.

The IT Business plan will be reviewed and updated on an annual basis.

Sean Green

IT Director

City of London Corporation

E: Sean.Green@cityoflondon.gov.uk

Appendices

Appendix A – IT Division Business Plan

Appendix A – Draft IT Division Business Plan 2019/20

Ensure safe, secure, stable and responsive Digital and Information Solutions

Key to the Corporate Outcomes that we aim to have an impact on:

1 – People are safe and feel safe,
 4. Communities are cohesive and have the facilities that they need
 9, We are digitally and physically well connected and responsive

What we do is:

Digital and Information Technology

Working with partners to implement appropriate and innovative technology and business processes to support our customers across the Corporation and Police in the delivery of more efficient and effective services.

Our budget is:

Expenditure	£m
CoLP IT	£9.7m
CoL IT	£7m

Less: Income

IT (London Councils)	£190k
----------------------	-------

Our top line objectives for the Chamberlain's Department are to:

- Act as an enabler for efficiency and value for money across all service areas
- Ensure safe, secure, stable and responsive Digital and Information solutions
- Develop our "One Team" focus to strengthen the links between teams and the provision of a joined-up service

Supported by a range of detailed performance indicators we will measure the following:

- Increased customer satisfaction by 5%

IT Deliverables in relation to departmental / service programmes and projects

- Help Departments to achieve their efficiency savings through adopting digital ways of working and the provision of finance and commercial support
- Deliver our own 2% savings as per our departmental efficiency plan (or more depending on the outcomes of the Fundamental Review)
- Implement improved processes to enable more efficient and effective working across the IT Division

Deliverables within corporate programmes and projects

- Work with Corporate Strategy and Performance to develop and implement the Digital and Information Management Strategies
- Provide expert IT direction to corporate programmes and projects
- Provide Technology support to departments to help them deliver their fundamental review of services and operations

How we plan to develop our capabilities this year

- Delivery of an in-house programme of training and secondments to build future capability
- Engage with our customers to better understand their business requirements

- Delivery of our current Service Targets:
 - Customer Satisfaction – 80%
 - IaaS Availability – 99.9%
 - P1 Incidents Resolution – 98%
 - P2 Incidents Resolution – 87.5%
- Achievement of on-going departmental efficiencies of at least 2% in year subject to new targets from the Fundamental Review
- Increased adoption of digital ways of working – 500 regular users of skype for business by year end
- Opportunity Outline for New IT Projects response – TBC
- Solution Proposals for New IT Projects response – TBC
- Projects delivered to budget – X%
- Projects delivered to plan – X%

What we're planning to do in the future:

- Deliver innovative digital and information solutions that are safe, stable and secure to enable efficient and effective working
- Equip staff with the skills and capabilities to maximise the benefit of the solutions provided
- Deliver the 2020 Sourcing Programme successfully
- Deliver the CoLP Modernisation Programme
- Deliver the IT commitments for the Fundamental review

Summary of our priorities:

1. Drive forward digital adoption
2. Optimise operational efficiency
3. Deliver safe, secure and stable IT/Digital Services
4. Deliver technology enabled business change and transformation
5. Continue to create and engage a supportive environment for all our staff

Priorities for 2019/20:

Priority Theme	Priorities	Owner
Drive forward digital adoption	Deliver CoLP single online home on the National Police Platform	AB
Drive forward digital adoption	Put in place a reference architecture	KM/MG
Drive forward digital adoption	Updating Digital Services Strategy	KM/SC
Drive forward digital adoption	Updating the Technology Roadmap	MG
Drive forward digital adoption	Applications Roadmap Implementation	MG
Drive forward digital adoption	Implement the Technology on the road every 2 weeks	SC
Drive forward digital adoption	Review an Enterprise Bus to enable system/forms integration	MG
Optimise operational efficiency		

Optimise operational efficiency	Automate service management metrics	SK/SC
Optimise operational efficiency	Continue SML improvements Self Service Portal Updated	MG
Deliver safe, secure and stable IT/Digital Services	Safe, secure and efficient IT	MG
Deliver safe, secure and stable IT/Digital Services	Asset Management Policy Review	SK
Deliver safe, secure and stable IT/Digital Services	Ensure tighter patching to avoid health-check surprises – health-checks twice a year	MG
Deliver safe, secure and stable IT/Digital Services	Radio replacement interim solution	AB
Deliver safe, secure and stable IT/Digital Services	PSN, DWP and HSCN compliance	MG
Deliver safe, secure and stable IT/Digital Services	Review and improve connectivity and public Wi-Fi in remote sites	MG
Deliver safe, secure and stable IT/Digital Services	Standardise public Wi-Fi offering and support in Libraries	MG
Deliver safe, secure and stable IT/Digital Services	Deliver new Digital Recording Solution	AB
Deliver safe, secure and stable IT/Digital Services	Replace aged CoLP solution to provide more resilience and ensure CoLP complies with Statutory responsibilities	AB
Deliver technology enabled business change and transformation	Implement enhancements and changes to Action Fraud including API's for integration to enable data sharing with Financial	AB

	institutions and the case management system	
Deliver technology enabled business change and transformation	CoLP 365 Modernisation	KM/AB
Deliver technology enabled business change and transformation	CoL Digital adoption and Transformation	KM
Deliver technology enabled business change and transformation	Dealing with unstructured data	SG/MG
Deliver technology enabled business change and transformation	Enabling infrastructure for Business Intelligence	KM
Deliver technology enabled business change and transformation	Deliver the next Phases of CRM	KM
Deliver technology enabled business change and transformation	Unified Communications Project	KM
Deliver technology enabled business change and transformation	Mobile Policing Model including replacement solution for Toughpads	AB
Deliver technology enabled business change and transformation	Transition from IaaS to Public Cloud	KM
Deliver technology enabled business change and transformation	Develop a Stakeholder Map for the Division	SG
Optimise operational efficiency	Applications replacement – <ul style="list-style-type: none"> ○ 2003 Server estate ○ SQL consolidation 	MG

Deliver technology enabled business change and transformation	<ul style="list-style-type: none">○ Statutory systems and Planning○ HR and Payroll○ Housing○ Libraries○ Wastes and Licensing○ Property System○ Oracle upgrade	
Continue to create and supporting and engaging department for our staff	Deliver the Staff Survey Action Plan	All

This page is intentionally left blank

Committee(s)	Dated:
Digital Services Sub-Committee – For Information	5th July 2019
Subject: IT Division – IT Service Delivery Summary	Public
Report of: The Chamberlain	For Information
Report author: Matt Gosden Deputy IT Director Eugene O’Driscoll Agilisys	

Summary

During May customer satisfaction with IT Services that Agilisys support and are responsible for remained high although there was a total of 5 high priority incidents for the City of London Corporation and City of London Police in May. 4 of these were caused by external factors such as supplier failures outside of the direct control of the IT service.

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

- There were **4** P1 incidents for City of London Corporation and **0** for City of London Police.
- There were **0** P2 incidents for the City of London Corporation and **1** for City of London Police.
- The Net Promoter Score average for the City of London Corporation/City of London Police for the last 3 months is **67.6**. Any score over **50** is considered very good.
- **91.5%** of users reported a good or very good experience of the City of London Service Desk – qualitative sampling will be undertaken to understand how to further improve satisfaction of CoL customers.
- **100%** of users reported a good or very good experience of the City of London Police 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 0 P1 incidents

P2 Incidents

There was 1 P2 incident

Affected Service	Reason	Resolution	Problem Management plan
Network outage	4th floor GYE network outage	UPS was reset to restore power	UPS/power management audit

With regards to the P2 incident for the 4th floor GYE network outage, monitoring indicated that a router was reported as being down which affected one floor of GYE. The uninterrupted power supply unit had to be restarted due to power loss, which re-established the power supply and service.

2. City of London (CoL)

P1 incidents

There were 4 P1 incidents

Affected Service	Reason	Resolution	Problem Management plan
Network services to London Councils, Epping Forest The Warren and Barbican Estate.	The initial outage was due to a fibre break on the BT network affecting 3 POP sites (5x 100Gb circuits). BT repaired the fibre to restore service. The subsequent outages were due to an ARP storm in the BT Open Reach core network following the repair. Total outage time was 20 hours.	BT cleared the ARP storm on their network to permanently restore service by 07:13 on 29th May 2019.	To be discussed at the next CoL/BT service review.

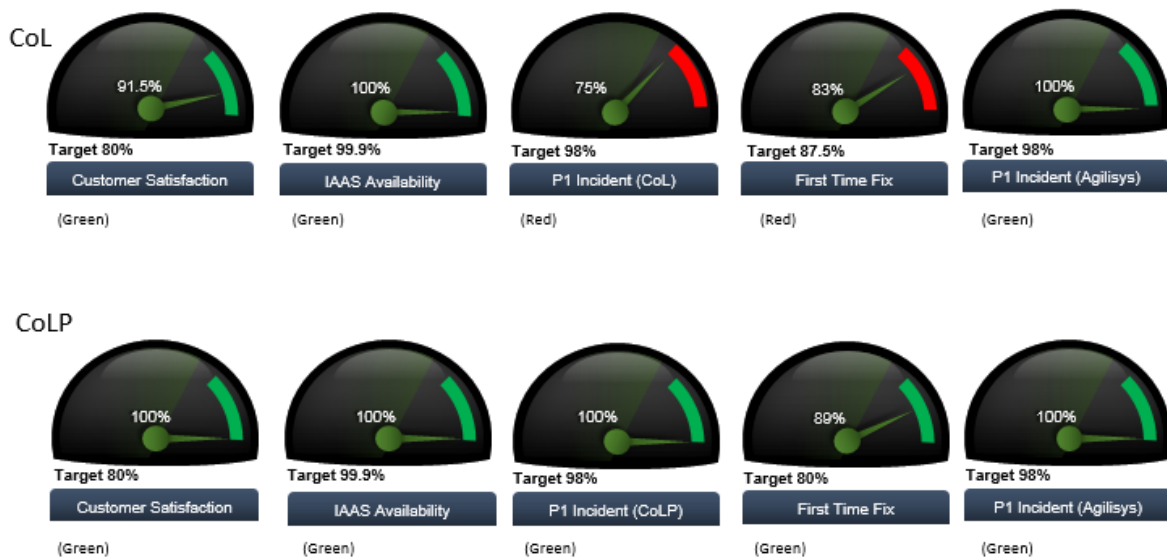
Pubnet at Barbican Library Shoe Lane Library Artizan Library	A 5-minute outage was observed and raised with the supplier.	Service resumed without intervention in City of London.	Incident report provided to CoL IT from 3 rd party supplier.
Gower Epilog	The application was unavailable. This is a known issue for the application.	Services were immediately restarted (outage time <1 minute) to restore service.	Root cause under investigation as part of Problem Management by CoL IT Applications.
Airconditioning failure	No IT services were unavailable, but multiple services were at risk of failure due to overheating equipment in a communications room.	The air-conditioning units were repaired by the Facilities team and temperatures were reduced to safe levels within 1 hour and 20 minutes.	CoL Director of IT engaging with Facilities to highlight the issue, review service levels and improve support model.

P2 Incidents

There were no P2 incidents

Service performance summary is detailed in the dashboard below.

Gauges to monitor performance – May 2019



3. Service improvements

- Agilisys ISO27001 Information Security Management System reaccreditation audit took place in May 2019 for both City of London and City of London Police and was successfully achieved with no actions.
- Senior Officers from the States of Guernsey visited City of London and met business stakeholders from City of London and City of London Police to assist them with their transition to a managed IT service provided by Agilisys. The officers were extremely impressed by the people they met and were very grateful for the time taken to meet them.

4. Police Improvements include:

- Hardware has been replaced on a security zone firewall. This has eliminated unexpected restarts which had adversely affected the Pronto service.
- Improvements are being made to the monitoring and alerting of CoLP systems.

5. Corporation improvements include:

- A Starters, Movers and Leavers tool is being developed by Agilisys to improve all related IT processes associated with user onboarding/offboarding. Requirements gathering workshop planned for mid-June with estimated completion by end of July.
- A DR test is planned for end of June which will test the resilience of the infrastructure under adverse circumstances including partial power failure and loss of connectivity to the internet and to IaaS datacentres. Stage 1 verification processes have already been successful at identifying points of weakness which are being addressed.
- Excellent feedback from London Councils Senior Management at the recent monthly performance meeting, reflecting high level of satisfaction following their IT Transformation project moving to new laptops, implementing office 365 and moving off an aged on-premise estate to the IaaS Cloud..

Eugene O'Driscoll
Client Director
Agilisys

Matt Gosden
Deputy IT Director

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

Committee(s)	Dated:
Digital Services Sub Committee – For Information	5 th July 2019
Subject: IT Division Risk Update	Public
Report of: The Chamberlain	For Information
Report author: Samantha Kay – IT Business Manager	

Summary

All IT Risks are now in the Risk Management System, with actions included, for the ongoing improvement and continuing assessment to the Management of Risk within the IT Division. The IT Division currently holds 4 risks, a reduction of one from the previous period. There are currently no RED risks. 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, whilst feeding in to the GDPR Corporate risk which is owned by Comptrollers.

Summary of the Corporate Risks

CR 16 – Information Security - Following review with A&R com and DSSC it was agreed that further steps were required to achieve maturity level that could bring the score to its target

CR 25 – GDPR Regulation Compliance – Will continue to be monitored following the closure of the formal project.

CR 29 – Information Management – The Information Management strategy has been agreed subject to a more detailed action plan and metrics to track performance. Progress is being made in developing a draft retention and disposal policy

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 and assists to mitigate one other Amber Corporate Risk. The IT Division currently holds 4 risks, none of which are scored as Red. All risks have owners, clear actions, with target dates to enable focussed management, tracking and regular and consistent reviews.

Current status

3. Since the last report the IT Risk Register has seen the following activity:
 - 3 Risks have been reduced from Departmental to Divisional level.
 - 1 Risk has increased from Divisional to Departmental level.
 - 1 Risk has been deactivated
 - 2 New risks have been identified

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

Movement of Risks

4. Risks reduced from Departmental to Divisional Level

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

- **CHB IT 020 – PSN Compliance** – the PSN Compliance certificate was granted, risk will now be monitored a Divisional Level
- **CHB IT 026 – Failure to commence CoLP IT Modernisation** - Following initial funding approval this was reduced to divisional level.
- **CHB IT 029 - 2020 Contract Planning and Procurement** – Following initial funding approval this was reduced to divisional level.

5. Risks increased from Divisional to Departmental Level

- **CHB IT 001 – Resilience – Power & Infrastructure** - following the failure of UPS devices this risk has been increase to departmental level

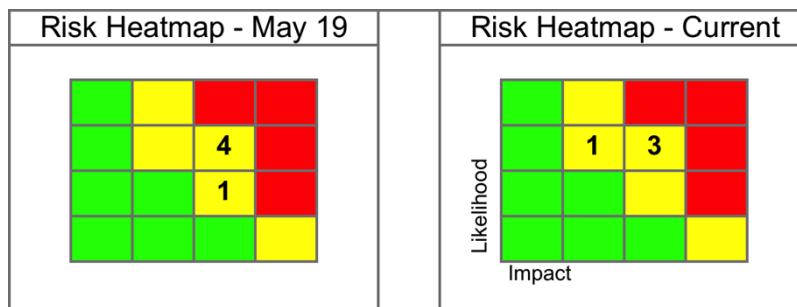
6. Risks that have been deactivated.

- **CHB IT 027 – IP Telephony – Cessation of dependant Service** - following the successful migration and cessation of services this risk has been deactivated.

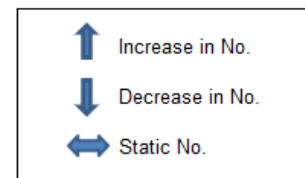
7. New Risks

- **CHB IT 028 – Air-conditioning Failure in Datacentres** – Following the failure of air conditioning units within data centres a new risk was identified due to critical IT systems being at threat.

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



8. Further breakdown of current Division risks:



Major Impact:

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

Serious Impact:

Risks with “likely” likelihood and “serious” impact:	0	0	↔
Risks with “possible” likelihood and “serious” impact:	0	1	↑
Risks with “unlikely” likelihood and “serious” impact:	1	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

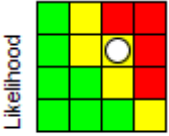
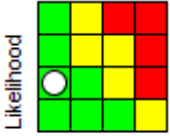

E: samantha.kay@cityoflondon.gov.uk




T: 07817 411176

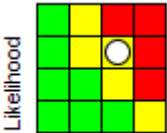
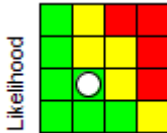

APPENDIX A - CHB IT All DEPARTMENTAL risks

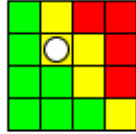
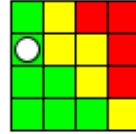



Rows are sorted by Risk Score

Risk no, title, creation date, owner	Risk Description (Cause, Event, Impact)	Current Risk Rating & Score	Risk Update and date of update	Target Risk Rating & Score	Target Date	Current Risk score change indicator
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>	<p>12</p> <p>Recent failures with UPS equipment have led to this risk being escalated to departmental level.</p> <p>Guildhall has been prioritised as part of audit.</p> <p>Audit on track. Reporting will commence over coming weeks.</p> <p>18 Jun 2019</p>	 <p>Likelihood</p> <p>Impact</p>	<p>2</p> <p>31-May-2020</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
CHB IT 004 Business Continuity / Disaster Recovery - planning and management. 30-Mar-2017 Sean Green	Cause: A lack of clear understanding of Business need for Services and Applications. No procedure in place for regular reviews with business. 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. 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.	 Likelihood Impact	12 DR test set for 25th June. With results and lessons learnt paper to be available by 2nd July 14 Jun 2019	 Likelihood Impact	4 15-Sep-2019	 Constant

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 028 Air Conditioning Failure in Datacentres 10-Jun-2019	Cause: The air conditioning units are failing in a number of the Guildhall Communication Equipment Rooms (CER's) / Datacentres. The existing air conditioning units are circa 12 years old and are being reset on a daily basis by the facilities team to keep them functional Event: There will be intermitted / prolonged service disruptions across the IT service provision. Effect: <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 	 Likelihood Impact	12 Temporary portable air conditioning unit has been placed in CER. The site assurance audit will produce recommendations on security, management and reliance of all CoL and CoLP comms rooms on a tiered basis. The scope has been increased to include environmental services (air conditioning) 18 Jun 2019	 Likelihood Impact	4 31-Mar-2020	 Constant


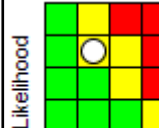

Risk no, title, creation date, owner	Risk Description (Cause, Event, Impact)	Current Risk Rating & Score		Risk Update and date of update	Target Risk Rating & Score		Target Date	Current Risk score change indicator
CHB IT 029 iTrent Contract 18-Jun-2019	<p>Cause: Extension of contract passed the envisaged 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 exemption of 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>Project planning has commenced</p> <p>18 Jun 2019</p>	 <p>Likelihood</p> <p>Impact</p>	<p>3</p>	<p>31-Mar-2020</p>	<p></p> <p>Constant</p>


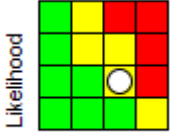

Three Corporate risks

Report Author: Paul Dudley
Generated on 18 June 2019



Rows are sorted by Risk Score

Risk no, title, creation date, owner	Risk Description (Cause, Event, Impact)	Current Risk Rating & Score		Risk Update and date of update	Target Risk Rating & Score		Target Date	Current Risk score change indicator
CR29 Information Management Page 70 08-Apr-2019 John Bardwell	<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 	 Likelihood Impact	12	The Information Management strategy has been agreed subject to a more detailed action plan and metrics to track performance. Progress is being made in developing a draft retention and disposal policy alongside reviewing roles to support good information management in the organisation and the business case for investment in tools required to help us manage and use our information more effectively. A draft Information Metrics model has been developed and discussed with the Information Management Board this now needs a final review with the Corporate Strategy and Performance team before being shared with SRG and Summit 08 Jun 2019	 Likelihood Impact	6	31-Mar-2020	
								Constant

Risk no, title, creation date, owner	Risk Description (Cause, Event, Impact)	Current Risk Rating & Score		Risk Update and date of update	Target Risk Rating & Score		Target Date	Current Risk score change indicator
CR16 Information Security (formerly CHB IT 030) 10-May-2019 Peter Kane	Cause: Breach of IT Systems resulting in unauthorised access to data by internal or external sources. Officer/ Member mishandling of information. Event: Cybersecurity attack - unauthorised access to COL IT systems. Loss or mishandling of personal or commercial information. Effect: Failure of all or part of the IT Infrastructure, with associated business systems failures. Harm to individuals, a breach of legislation such as the Data Protection Act 2018. Incur a monetary penalty of up to €20M. Compliance enforcement action. Corruption of data. Reputational damage to Corporation as effective body.	 Likelihood Impact	6	Following review with A&R committees and DSSC it was agreed that further steps were required to achieve maturity level that could bring the score to its target 14 Jun 2019	 Likelihood Impact	8	31-Oct-2019	 Decreasing

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
CR25 General Data Protection Regulation Compliance 01-Dec-2017 Michael Cogher	Cause: Inadequate departmental systems and procedures are in place which meet the additional requirements of GDPR legislation. Event: CoL is unable to comply with GDPR requirements - poor, non-secure and non-compliant processing of personal data. Effect: CoL exposed to adverse publicity, reputational damage, financial penalties imposed by the Information Commissioners Office. Increased volume of Subject Access Requests.	 Likelihood Impact	6	1. C&CS Information Compliance Team continues to advise departments on GDPR compliance issues and on embedding GDPR generally. 2. The Mazars GDPR compliance audit is awaited which will provide an assessment of the level of compliance. 21 May 2019	 Likelihood Impact	4	31-Jul-2019	 Constant

This page is intentionally left blank

Committee(s)	Dated:
Digital Services Sub Committee (DSSC)	5 th July 2019
Subject: CR 16 Information Security Risk	
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 as means to capture and mitigate the risks a ‘cyber breach’ would present to the City Corporation. It is evident that dependent on the nature of the breach the impact can vary from very low to critical. Cyber threat is often viewed as a complex, dynamic and highly technical risk area. However, what is often at the root of a breach is a failure to get the basics right, systems not being patched, personnel not maintaining physical security, suppliers given too much information.

The National Cyber Security Centre (NCSC) 10 Steps to Cyber Security framework has been adopted to strengthen the controls in this risk area; this framework is now used by the majority of the FTSE350. The control scores are developing well and are reflective of the ongoing adoption across the City Corporation, all risk areas continue to be actively monitored and risk managed. Scores will continue to increase as improvements to people, process and technology are delivered.

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

Recommendation(s)

Members are asked to:

- Note the report.

Main Report

Background

1. Cyberspace has revolutionised how many of us live and work. The internet, with its more than 3 billion users, is powering economic growth, increasing collaboration and innovation, and creating jobs.
2. Protecting key information assets is of critical importance to the sustainability and competitiveness of businesses today. The City Corporation needs to be on the front foot in terms of our cyber preparedness. Cyber security is all too often thought of as an IT issue, rather than the strategic risk management issue it actually is.
3. Corporate decision making is improved through the high visibility of risk exposure, both for individual activities and major projects, across the whole of the City Corporation.
4. Providing financial benefit to the organisation through the reduction of losses and improved “value for money” potential.
5. The City Corporation is prepared for most eventualities, being assured of adequate contingency plans. We have therefore adopted the NCSC Ten Steps to Cyber Security framework to assist and support our existing strategic-level risk discussions, specifically how to ensure we have the right safeguards and culture in place.
6. The creation of CR16 demonstrates the City Corporations commitment to the identification and management of this risk area.

Current Position

7. The development and implementation of an Information Security Management System (ISMS) was seen as an essential requirement to permit the measurement and assurance of the CR16 risk. A number of frameworks were considered, and the NCSC Ten Steps to Cyber Security framework, supported by the NCSC 20 Critical Security Controls, was chosen as the most appropriate for the City Corporation.
8. The first step of the ISMS is the “risk management regime“, as the NCSC describe it, this is the strategy that glues different controls and processes together. This ensures we do not fragment the approach to cyber security and identify hidden vulnerabilities and potential for compromise, ensuring the ability to measure the risk profile. The remaining nine steps are broken down into four clear delivery areas: Establish, Manage, Enhance, and Deliver.

Information Risk Management

	% Complete	Target Score	Actual Score	Trend
Information Risk Management	86%	4	4	-

Risk appetite statement is the next applicable piece of work in this area. Involves an overarching agreement with the SIRO and then a cascade framework for application in each of the business areas across the City. In addition, a code of connection has been developed to support institutional departments connecting to and consuming core IT services from City.



Establish

	% Complete	Target Score	Actual Score	Trend
Monitoring	72%	4	3	-
Incident Management	93%	4	4	↑
Secure Configuration	86%	4	3	-

The deployment, throughout October/November, of the Security Information and Event Management collector has taken place. However, connection work remains outstanding and once in place this will establish direct improvements to the monitoring and secure configuration across the City infrastructure.

Manage

	% Complete	Target Score	Actual Score	Trend
Network Security	69%	4	3	-
Managing User Privileges	75%	4	3	-

Network security will directly improve following the implementation of the Security Information and Event Management collector was deployed throughout October/November. The issues of managing user privileges is currently being managed manually and a technical solution has been purchased and is awaiting implementation across the infrastructure – this is a complex piece of software and whilst installation is simple, the application and management will take time to develop and tune.

Enhance

	% Complete	Target Score	Actual Score	Trend
Malware Prevention	68%	4	3	-
Removable Media Controls	89%	4	4	-

A project is underway to review the existing anti-malware solution and determine if enhancements are required, this has highlighted the need for anti-malware solutions for mobile devices. The removable media controls have recently been reviewed and the deployment of controls have been confirmed. To improve the removable media control score requires further work in respect of policies and user education, this is currently being included within the procedural refresh for removable media across IT, and this will include a sign-off process for receipt of device and responsibilities.

Deliver

	% Complete	Target Score	Actual Score	Trend
Home and Mobile Working	71%	4	3	↑
User Education and Awareness	75%	4	3	-

The next steps for the Home and Mobile Working control area are for a thorough review of user acceptance policies and guidance. In addition, the aging Citrix infrastructure is being replaced, once complete this will improve the scores in this area. A developed schedule of awareness and training is being rolled out across the organisation with a different theme each month.

- 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 June 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	3	-
9. Home and Mobile Working	71%	4	3	↑
10. User Education and Awareness	75%	4	3	-

Options

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

Proposals

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

Implications

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

Health Implications

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

Conclusion

16. There is an extensive programme of work underway to mitigate the risks identified within CR16. This report articulates the work in progress and clearly identifies where we will be directing continuing effort to manage this risk to an initial acceptable level and then monitoring as the controls mature across the organisation.
17. The breadth and scope of the necessary controls are cross-organisational and should not be entirely seen as a technical issue to be solved by the IT department. For example if users leave the door open and their computers logged on then technical controls cannot in themselves defend the organisation.
18. The realisation of this risk would certainly have a severe impact on technical systems and directly impact the operational effectiveness of potentially the entire City Corporation. It is therefore imperative that the underlying issue of developing a security culture is supported through the delivery of risk controls for CR16. There is positive support for this work across the organisation and senior management understand and are supportive of the necessary changes to ensure the City Corporation's security.

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

Appendices

Detailed Appendices available on request:

- Appendix 1 – CR16 Information Security
- Appendix 2 – 10 Steps to Cyber Security Dashboard & Breakdown
- Appendix 3 – Statutory Requirements Summary
- Appendix 4 – Maturity Scoring Matrix
- Appendix 5 – Critical Security Controls Mapping

Gary Brailsford-Hart

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

Appendix 1 - CR16

Report Author: Paul Dudley

Generated on: 10 May 2019



Rows are sorted by Risk Score

Risk no, title, creation date, owner	Risk Description (Cause, Event, Impact)	Current Risk Rating & Score		Risk Update and date of update	Target Risk Rating & Score		Target Date	Current Risk score change indicator
CR16 Information Security (Formerly CHB IT 030) 10-May-2019 Peter Kane	Cause: Breach of IT Systems resulting in unauthorised access to data by internal or external sources. Officer/ Member mishandling of information. Event: Cybersecurity attack - unauthorised access to COL IT systems. Loss or mishandling of personal or commercial information. Effect: Failure of all or part of the IT Infrastructure, with associated business systems failures. Harm to individuals, a breach of legislation such as the Data Protection Act 2018. Incur a monetary penalty of up to €20M. Compliance enforcement action. Corruption of data. Reputational damage to Corporation as effective body.	 Likelihood Impact	12	A&RMC agreed to add this risk back on to the Corporate Risk register until the July meeting where there will be a full discussion about the status of this risk. 10 May 2019	 Likelihood Impact	8	31-Jan-2019	 Constant

Action no	Action description	Latest Note	Action owner	Latest Note Date	Due Date
CR16j	Now in continuous improvement with monitoring and review at the DSSC	New action	Gary Brailsford-Hart	29-Apr-2019	30-Jun-2019

CR16k	Final stages of completing information security projects which will mean that we can assure Members that the City of London Corporation has implemented all the national government recommended security practices and technology achieving a maturity level of 4.	Information Security projects are being delivered as planned. The Information Security team recommended to the Audit and Risk Committee that this risk is reduced to Amber. Move towards a continuous improvement model is being adopted to ensure the controls in place are embedded, mature and reflective of emergent threats and risks.	Gary Brailsford-Hart	29-Apr-2019	30-Apr-2019
-------	--	--	----------------------	-------------	-------------

This page is intentionally left blank



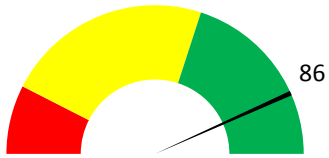
City of London Corporation

10 Steps Maturity Assessment

01 June 2019

10 Steps to Cyber Security: Dashboard

1. Information Risk Management



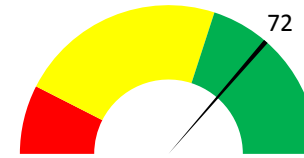
2. Network Security



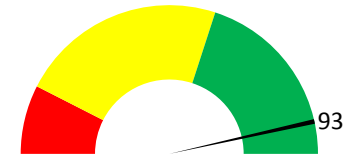
3. Malware Prevention



4. Monitoring



5. Incident Management

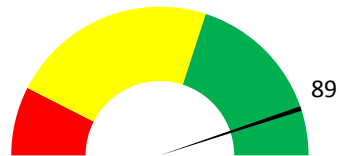


Page 86

6. Managing User Privileges



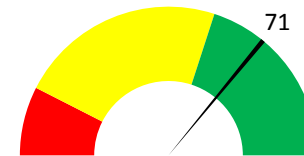
7. Removable Media Controls



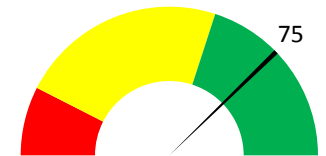
8. Secure Configuration



9. Home and Mobile Working



10. User Education and Awareness



	% Complete	Target Score	Actual Score
Information Risk Management	86%	4	4
Establish a governance framework	100%	4	4
Determine the organisation's risk appetite	25%	4	2
Maintain the Board's engagement with information risk	100%	4	4
Produce supporting policies	100%	4	4
Adopt a lifecycle approach to information risk management	100%	4	4
Apply recognised standards	100%	4	4
Make use of endorsed assurance schemes	100%	4	4
Educate users and maintain their awareness	75%	4	3
Promote a risk management culture	75%	4	3

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

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

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

	% Complete	Target Score	Actual Score
Network Security	69%	4	3
Police the network perimeter	75%	4	3
Install firewalls	100%	4	4
Prevent malicious content	75%	4	3
Protect the internal network	80%	4	3
Segregate network as sets	25%	4	1
Secure wireless devices	100%	4	4
Protect internal IP addresses	25%	4	1
Enable secure administration	25%	4	2
Configure the exception handling process	100%	4	4
Monitor the network	50%	4	2
Assurance process	100%	4	4

	% Complete	Target Score	Actual Score
Incident Management	93%	4	4
Obtain senior management approval	100%	4	4
Provide specialist training	100%	4	4
Define the required roles and responsibilities	100%	4	4
Establish a data recovery capability	100%	4	4
Test the incident management plan	100%	4	4
Decide what information will be shared and with whom	75%	4	3
Collect and analyse post-incident evidence	75%	4	3
Conduct a lessons learned review	100%	4	4
Educate users and maintain their awareness	75%	4	3
Report criminal incidents to law enforcement	100%	4	4

	% Complete	Target Score	Actual Score
Secure Configuration	86%	4	3
Use supported software	80%	4	3
Develop and implement corporate policies to update and patch systems	100%	4	4
Create and maintain hardware and software inventories	80%	4	3
Manage your operating systems and software	100%	4	4
Conduct regular vulnerability scans	75%	4	3
Establish configuration control and management	75%	4	3
Disable unnecessary peripheral devices and removable media access	100%	4	4
Implement white-listing and execution control	100%	4	4
Limit user ability to change configuration	100%	4	4
Limit privileged user function	50%	4	2

	% Complete	Target Score	Actual Score
Malware Prevention	68%	4	3
Develop and implement anti-malware policies	75%	4	3
Manage all data import and export	75%	4	3
Blacklist malicious web sites	100%	4	4
Provide detailed media scanning machines	25%	4	1
Establish malware defences	75%	4	3
End user device protection	50%	4	2
User education and awareness	75%	4	3

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

	% Complete	Target Score	Actual Score
Home and Mobile Working	71%	4	3
Asses the risks and create a mobile working security policy	75%	4	3
Educate users and maintain their awareness	75%	4	3
Apply the security baseline	100%	4	4
Protect data at rest	100%	4	4
Protect data in transit	75%	4	3
Review the corporate incident management plans	75%	4	3

Current status of 10 Step control areas across organisation.
ASSESSMENT DATE: 01 June 2019

Control Area	% Complete	Target Score	Actual Score
Information Risk Management	86%	4	4
Network Security	69%	4	3
Malware Prevention	68%	4	3
Monitoring	72%	4	3
Incident Management	93%	4	4
Managing User Privileges	75%	4	3
Removable Media Controls	89%	4	4
Secure Configuration	86%	4	3
Home and Mobile Working	71%	4	3
User Education and Awareness	75%	4	3

This page is intentionally left blank

Appendix 3: Statutory Requirements Summary

Data Protection Act 2018

<http://www.legislation.gov.uk/ukpga/2018/12/contents>

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

The Act is underpinned by six guiding principles which requires that personal data shall be:

- a) processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency');
- b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes ('purpose limitation');
- c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
- d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');
- e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals ('storage limitation');
- f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')."

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

Freedom of Information Act 2000

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

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

Privacy and Electronic Communications Regulations 2003

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

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

Regulation of Investigatory Powers Act (RIPA) 2000

<http://www.legislation.gov.uk/ukpga/2000/23/contents>

RIPA regulates the powers of public bodies to carry out surveillance and investigation and also deals with the interception of communications.

Copyright, Designs and Patents Act 1988

<http://www.legislation.gov.uk/ukpga/1988/48/contents>

The Copyright, Designs and Patents Act (CDPA) defines and regulates copyright law in the UK. CDPA categorises the different types of works that are protected by copyright, including:

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

Computer Misuse Act 1990

<http://www.legislation.gov.uk/ukpga/1990/18/contents>

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

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

Human Rights Act 1998

<http://www.legislation.gov.uk/ukpga/1998/42/contents>

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

Equality Act 2010

<http://www.legislation.gov.uk/ukpga/2010/15/contents>

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

Terrorism Act 2006

<http://www.legislation.gov.uk/ukpga/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

Top 20 Critical Security Controls - Assessment and Mapping to NCSC 10 Steps

CSC #	Ten Steps	Control Criteria	Technical Controls in place	Technical Gaps Identified	@Investment	Status
1	Secure Configuration Monitoring	Inventory of Authorized and Unauthorized Devices <i>Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.</i>	IBM Endpoint Manager (IEM) undertakes point in time audit of connected devices.	Implementation of Network Access Control (Part of JNRP) will provide identification of unauthorised devices and report into a SIEM for remediation.	@£80k for SIEM	Awaiting connection from CoL to CoLP networks.
2	Secure Configuration Monitoring	Inventory of Authorized and Unauthorized Software <i>Actively manage (inventory, track, and correct) all software on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.</i>	IEM / SCCM should provide this functionality.	Application Whitelisting	Staff Resource	Dependent on outsourcer and monitoring of assets
3	Secure Configuration	Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers <i>Establish, implement, and actively manage (track, report on, correct) the security configuration of laptops, servers, and workstations using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.</i>	Controlled build is in place across all device types as well as an established change management process. Microsoft InTune MDM is being deployed.	Review ITIL implementation and SIEM.	Staff Resource	In place and operating under contract with outsourcer.
4	Monitoring	Continuous Vulnerability Assessment and Remediation <i>Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers.</i>	Contractual security support.	Purchase Nessus vulnerability assessment product and deploy in enterprise mode and feed into SIEM for alerting and reactive remediation.	@£10k	Product in place and being utilised by Infosecurity Analyst
5	Removable Media Controls Malware Protection	Malware Defenses <i>Control the installation, spread, and execution of malicious code at multiple points in the enterprise, while optimizing the use of automation to enable rapid updating of defense, data gathering, and corrective action.</i>	ESET Anti-virus and Anti-Malware in place across Servers and workstations; Different AV products at gateways. However, this has proved ineffective against recent cryptoware attacks.	Consider investing in dedicated anti-malware product - MalwareBytes, proven very effective against Ransomware attacks.	@£80-100k	Requirement to invest in mobile anti-virus solution.
6	Secure Configuration	Application Software Security <i>Manage the security lifecycle of all in-house developed and acquired software in order to prevent, detect, and correct security weaknesses.</i>	Change management process in place, no technical controls. Resource in place to manage process.	Deployed software will be subject to application log inspection into SIEM.		SIEM: Awaiting connection from CoL to CoLP networks.
7	Monitoring Network Security	Wireless Access Control <i>The processes and tools used to track/control/prevent/correct the security use of wireless local area networks (LANS), access points, and wireless client systems.</i>	Not currently applicable as no corporate services provided by direct wireless connection	Addressed within the network refresh project and subject to monitoring by outsourcer.		NOC in place and operating.
8	Incident Management	Data Recovery Capability <i>The processes and tools used to properly back up critical information with a proven methodology for timely recovery of it.</i>	Operated under managed service.	DR/BCP testing and support needed.	Significant Staff Resource Required	Requires testing.
9	User Education & Awareness	Security Skills Assessment and Appropriate Training to Fill Gaps <i>For all functional roles in the organization (prioritizing those mission-critical to the business and its security), identify the specific knowledge, skills, and abilities needed to support defense of the enterprise; develop and execute an integrated plan to assess, identify gaps, and remediate through policy, organizational planning, training, and awareness programs.</i>	Limited scope for awareness, training and policy enforcement	Invest in a policy and awareness product, i.e. MetaCompliance.	@£30k	Product purchased and operating.
10	Secure Configuration Network Security	Secure Configurations for Network Devices such as Firewalls, Routers, and Switches <i>Establish, implement, and actively manage (track, report on, correct) the security configuration of network infrastructure devices using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.</i>	Revised approach to change management process in place aligned with ITIL. No specific technical controls.	Configuration change to be tracked by SIEM.	Staff Resource	SIEM: Awaiting connection from CoL to CoLP networks.
11	Network Security	Limitation and Control of Network Ports, Protocols, and Services <i>Manage (track/control/correct) the ongoing operational use of ports, protocols, and services on networked devices in order to minimize windows of vulnerability available to attackers.</i>	None	Network Access Control will provide this functionality - this is part of the network refresh delivery.		Verification of NAC outstanding with outsourcer.
12	Monitoring	Controlled Use of Administrative Privileges <i>The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.</i>	Procedurally managed no technical monitoring in place.	No automatic monitoring or alerting in place when privilege access is granted or revoked. SIEM should be implemented to provide technical oversight as well as policy enforcement tool to ensure adherence and understanding of required standards.	£100k	Product purchased, awaiting installation by IT.
13	Home & Mobile Working Monitoring Network Security	Boundary Defense <i>Detect/prevent/correct the flow of information transferring networks of different trust levels with a focus on security-damaging data.</i>	Basic firewall controls, no intelligent boundary defence mechanisms in place.	Deploy an Intrusion Detection System; Deploy an Intrusion Prevention System; Data fed into SIEM.	@£50-100k	In place and operating under contract with outsourcer.
14	Monitoring	Maintenance, Monitoring, and Analysis of Audit Logs <i>Collect, manage, and analyze audit logs of events that could help detect, understand, or recover from an attack.</i>	Limited and locally managed, no centralised Syslog.	Implementation of SIEM will address this issue.		SIEM: Awaiting connection from CoL to CoLP networks.
15	Managing User Privileges Network Security	Controlled Access Based on the Need to Know <i>The processes and tools used to track/control/prevent/correct secure access to critical assets (e.g., information, resources, systems) according to the formal determination of which persons, computers, and applications have a need and right to access these critical assets based on an approved classification.</i>	Limited segregation in place.	Following identification and classification of assets the deployment of VLANS. Classification of data is linked to reducing overall cost reduction.	Staff Resource	Network refresh has introduced additional security standards for VLANS across network.
16	Managing User Privileges	Account Monitoring and Control <i>Actively manage the life-cycle of system and application accounts - their creation, use, dormancy, deletion - in order to minimize opportunities for attackers to leverage them.</i>	Currently managed by outsourcer	Process driven, supported by technology.	Staff Resource	In place and operating.

Top 20 Critical Security Controls - Assessment and Mapping to NCSC 10 Steps

CSC #	Ten Steps	Control Criteria	Technical Controls in place	Technical Gaps Identified	@Investment	Status
17	Removable Media Controls	Data Protection <i>The processes and tools used to prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the privacy and integrity of sensitive information.</i>	Limited capability managed by Firewall and gateway filters.	Deploy an Intrusion Detection System; Deploy an Intrusion Prevention System; Deploy DLP controls including the review of Email and Internet gateway rules; Pixalert - content scanner.	@50k	Move to o365 requires review of MS security centre control set and alignment with security controls.
18	Incident Management	Incident Response and Management <i>Protect the organization's information, as well as its reputation, by developing and implementing an incident response infrastructure (e.g., plans, defined roles, training, communications, management oversight) for quickly discovering an attack and then effectively containing the damage, eradicating the attacker's presence, and restoring the integrity of the network and systems.</i>	Recorded within SupportWorks by ServiceDesk no other technical controls in place; Reactive and fragmented processes in place; Currently under review by management.	Create a single incident reporting process across the organisation for all security incident types; Audit technical capability against CESG Cyber Incident Response Scheme.	Staff Resource	In place and operating.
19	Secure Configuration	Secure Network Engineering <i>Make security an inherent attribute of the enterprise by specifying, designing, and building-in features that allow high confidence systems operations while denying or minimizing opportunities for attackers.</i>	Network refresh project is addressing Security by Design including SAVE process.	Ongoing integration into procurement processes.	Staff Resource	Established processes in place and security gateways in place for procurement processes.
20	Incident Management Monitoring Secure Configuration	Penetration Tests and Red Team Exercises <i>Test the overall strength of an organization's defenses (the technology, the processes, and the people) by simulating the objectives and actions of an attacker.</i>	Penetration test takes place against PSN;	Widen scope of Penetration tests to include all risk areas;	@£50-100k	In place and operating.

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