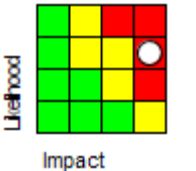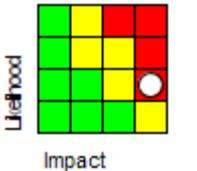| Risk no, title, creation date, owner	Risk Description (Cause, Event, Impact)	Current Risk Rating & Score		Risk Update and date of update	Target Risk Rating & Score		Target Date/Risk Approach	Current Risk score change indicator
CR16 Information Security (formerly CHB IT 030) 10-May-2019 Caroline Al-Beyerty	**Cause**: Breach of City of London Corporation IT Systems resulting in unauthorised access to data by internal or external sources. **Event**: The City Corporation does not adequately prepare, maintain robust (and where appropriate improve) effective IT security systems and procedures. **Effect**: a) Failure of all or part of the IT Infrastructure with associated business systems failures. b) Harm to individuals. c) A breach of legislation such as the Data Protection Act 2018 and UK-GDPR. d) Incurrence of a monetary penalty. e) Corruption of data. f) Reputational damage to City of London Corporation as an effective body.		24	The project to implement a raft of new security improvements is complete. A decision was made to define a minimum-security baseline for all parts of the corporation. The Director of DITS will work with IMS to put this together. The security service provided by Agilisys has now been brought in-house, giving greater control and visibility over Security controls. We are committed to increasing our Secure Score month on month, and this will be reported to Digital Services Committee. **18 Dec 2023**		16	31-Mar-2024 Reduce	 Constant

Action no	Action description	Latest Note	Action owner	Latest Note Date	Due Date
CR16q	Monitoring user activity on the network for any suspicious or unauthorized behaviour	Whilst we have monitoring of activity in place there is no behavioural analytical solution to identify anomalous behaviour. This capability is a significant control in detecting and	Gary Brailsford-	18-Dec-2023	31-Dec-2023

		preventing ransomware attacks.	Hart		
CR16r	Monitoring access control systems and processes to ensure that only authorized users have access to sensitive information	Controls are in place to manage the access control to the estate; improvements have been made in the application of multifactor authentication. However, the escalation and acceptance of privileged accounts remains within the IT department and is not subject to independent scrutiny	Gary Brailsford-Hart	18-Dec-2023	31-Dec-2023
CR16s	Developing and implementing a plan to respond to any security incidents that occur.	We have drafted a Cyber Incident Plan as well as operating cyber testing exercises. However, there is a need to produce further playbooks and develop more testing and exercising events	Gary Brailsford-Hart	18-Dec-2023	31-Dec-2023
CR16t	Using software tools to collect and analyze data from various security sources to detect and respond to security incidents.	This is in place and operating. Microsoft Sentinel is in place and collecting activity from across CoL. This is monitored and managed by the InfoSec team who will detect and investigate incidents highlighted by the SIEM.	Gary Brailsford-Hart	18-Dec-2023	31-Dec-2023
CR16u	Providing regular training to staff and employees on cyber security best practices to prevent security breaches.	We have confirmed that MetaCompliance Learning is currently licensed for CoL but has not been deployed. InfoSec team will be engaging with learning and development to support, refresh and deliver this across CoL. We have developed an awareness plan and produce weekly cyber security articles which are being shared with communications colleagues 03/10/2023 - Launch of Cyber Security awareness training: Module 1, delivered to all staff. October is cyber month and the security team will be distributing practice advice based on a different theme for each week in October.	Gary Brailsford-Hart	18-Dec-2023	31-Mar-2024
CR16v	Security Baseline assessment – COL/COLP/Institutions	Initial assessment complete, work is ongoing to identify trends and a developments plans and updates to the CAF will continue – reviewed bi-annually	Gary Brailsford-Hart	18-Dec-2023	31-Dec-2023