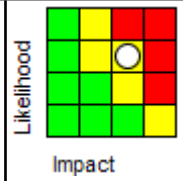
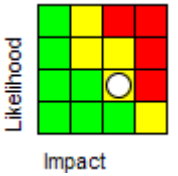
Appendix 1

CR16 Information Security

Report Author: Paul Dudley
Generated on: 05 September 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.		**12**	Following review with A&R committee and DSSC it was agreed that further steps were required to achieve maturity level that could bring the score to its target **29 Aug 2019**		**8**	31-Oct-2019	Constant

Action no	Action description	Latest Note	Action owner	Latest Note Date	Due Date

Appendix 1

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	23-May-2019	30-Sep-2019
CR16l	New toolkit for monitoring and managing the security risk being discussed with the Digital Services Sub-Committee at their meeting on the 30th May 2019.	Recommending that the Digital Services Sub Committee adopts an additional tracking tool called the Cyber Security Board Toolkit This was agreed at last DSSC and a member's workshop is being arranged.	Gary Brailsford-Hart	29-Aug-2019	31-Oct-2019
CR16m	Review of how Cyber risk is identified, analysed and monitored – the expectation is we should be moving beyond compliance measuring (Ten Steps) and seeking to integrate cyber security into organisational risk management processes.	Compliance and security are **not** the same thing. They may overlap, but compliance with common security standards can coexist with, and mask, very weak security practices. **Good risk management should go beyond just compliance.** Good risk management should give insight into the health of the City of London and identify opportunities and potential issues. Many of our organisational risks will have a cyber component to them. Cyber security risk should therefore be integrated with our organisational approach to risk management. Dealing with cyber security risk as a standalone topic (or considering it simply in terms of 'IT risk') will make it hard for us to recognise the wider implications of those cyber security risks, or to consider all the other organisational risks that will have an impact on cyber security	Gary Brailsford-Hart	29-Aug-2019	31-Oct-2019
CR16n	Now in continuous improvement with monitoring and review at the DSSC	Updates to be provided to DSSC committee every two months with a deep dive at the next A&R Committee. Report provided to A&R, monitoring agreed to continue at DSSC.	Gary Brailsford-Hart	29-Aug-2019	28-Sep-2019