Question 1 – Cllr David Wilcox
Re: Cyber Security

I welcome the report, and I'm pleased the council is working on a strategy for compliance.

I do, however, have some questions:

Q1: How many cyber security incidents have BCC logged in the each of the previous four quarters of the current risk report?

We log various types of incidents that are classed as security Incidents. In the last year we have logged 172 incidents – these range from Phishing emails, lost or stolen devices, Scam phone calls, to Malware alerts.

Q2: How long has the council been without a cyber security strategy?

We have a number of policies and frameworks that set out our ways of working and how the Information Governance Service functions and what it is responsible for. I am looking to create an Information Governance Strategy that will include Cyber, currently we are doing a lot of work to identify operational risks which is necessary foundation to inform the Strategy, this is something that we will be working on over the next 12 months.

Q3: What metrics are in place to ensure that the council has an effective strategy ASAP?

All the audit action are being tracked by the Information Governance Board – which has attendance from Audit colleagues.

Q4: Obviously, I do not want to publicise all the areas where BCC's cyber security is weak or non-existent. Is there a mechanism that members can securely view the scale of the issue and the progress?

I will be willing to give members an exempt briefing on the details.

Q5: Risk Report: Please quantify why CRR29 and CRR7 are only classed as Amber Risks? The likelihood of these issues will increase over time, and these risks have been at Amber for the last four quarters, with no change in their scoring.

In both these cases they are classed as High risk (the tolerance level is set to Medium). As with Q4, I will be happy to go into more detail in an exempt briefing.

Q6: What is the timescale to install a feedback loop for security incidents to the IGB, and will members be updated on its progress?

Security incidents are reported monthly to EDM's and also discussed at the IGB.

Q7: How will maintaining Information Asset Registers fields be integrated into every employee and member's day-to-day workflow and when will this project be complete?

Information Governance now includes colleagues from our Modern Records team. We are looking to revisit how we do information management, so that we cover all aspects of the records Lifecyle.

Q8: Shadow IT - applications & hardware that are not managed by central IT - seems to be a huge problem for the Council IT department. What steps being taken to get this under control? This is both a huge security risk and a potential overspend for council.

Information Governance are working closely with IT colleagues to mitigate this. The move to O365, Azure and Windows 10 has given us more visibility and technical tools to manage this. We are also working with colleagues in the PMO and Procurement to try and prevent any new 'shadow IT' being created.

Q9: When will the Windows 10 rollout be complete, so that unencrypted and therefore unauthorised USB disks can be put out of scope?

This is a question for ICT – awaiting a response which I will then pass on.

Q10: When will the formal IT security training rollout be complete for all employees and members?

Security training is mandatory for all staff, as well as annual refreshers. The new Learning and Development portal allows us easier visibility of completion rates. Elected Members are also required to undertake IT security training and this programme is expected to be completed by the end of October 21.