MIDDLESBROUGH COUNCIL	Middlesbrough moving forward

Report of:	Head of Strategy, Information and Governance

Submitted to:	Corporate Audit and Affairs Committee, 7 February 2019

Subject:	Annual Report of the Senior Information Risk Owner (SIRO)

Summary

Proposed decision(s)
That the Committee notes the position in respect of information risk set out in the report, and proposes for consideration any further steps it may wish to see taken to promote good practice in information governance within the Council.

Report for:	**Key decision:**	**Confidential:**	**Is the report urgent?**
Information	No	No	No

Contribution to delivery of the 2018-22 Strategic Plan		
Business Imperatives	**Physical Regeneration**	**Social Regeneration**
The activity outlined in the main body of the report will result in significant improvements in the Council's information governance arrangements.	Improved information governance will underpin the delivery of all strategic priorities.	Improved information governance will underpin the delivery of all strategic priorities.

Ward(s) affected
None.

What is the purpose of this report?

1. To advise the Corporate Affairs and Audit Committee of arrangements in place to ensure the proper governance of information within the Council, progress made within the next past year, risks and issues arising, and priorities for the next 12 months.

Why does this report require a member decision?

2. This report aims to provide assurance to the Committee that information governance (IG) policy and practice within the Council is in line with legal obligations, and consistent with the principles of good governance.

Report background

3. The legal framework under which the Council must protect, manage, share and disclose information includes the Data Protection Act 2018 (DPA 2018), the EU General Data Protection Regulation 2016 (GDPR), the Privacy and Electronic Communications (EC Directive) Regulations 2003 (as amended), the Local Government (Transparency Requirements) (England) Regulations 2015, the Environmental Information Regulations 2004 (EIR), the Freedom of Information Act 2000 (FOI), Reuse of Public Sector Information Regulations 2015 (RoPSI), and the Regulation of Investigatory Powers Act 2000 (RIPA).

4. The Head of Strategy, Information and Governance acts as the Council's Senior Information Risk Owner (SIRO) and advises the Chief Executive and the management team on information risk. The SIRO also reports quarterly to the internal risk management group and annually to this Committee.

5. The Council's activity in this area is regulated by the Information Commissioner's Office (ICO), with the Investigatory Powers Commissioner's Office (IPCO) acting as the regulatory body for RIPA.

Compliance, risks and issues in 2018

6. The last annual report to the Committee (8 February 2018) set out the following priorities for the 2018 calendar year:

   - continuing to improve the Council's cyber security;
   - ensuring plans to comply with the GDPR were effectively implemented, including appointing a statutory Data Protection Officer;
   - reviewing data breach investigations and disseminating lessons learned across the organisation;
   - progressing digital solutions to minimise data protection incidents arising from human error;
   - reviewing how the Council responds to statutory information requests and proactively publishes datasets to ease the burden of response;
   - developing an overarching Information Strategy of the Council; and
   - restructuring the Strategy, Information and Governance service to support the delivery of this strategy.

7. The progress made on these issues during 2018 is set out in the following paragraphs.

Cyber security

8. None of the Council's systems or services were compromised in 2018, and good progress has been made in enhancing the Council's cyber security, including:

    - migrating DNS (Domain Name System) services from Google to the National Cyber Security Centre (NCSC)'s DNS Hosting Servers, managed by Nominet, so reducing the risk of users/devices finding their way to malicious websites;
    - ensuring that 100% of inward-bound emails are scanned and quarantined where appropriate, and that all those receiving emails from middlesbrough.gov.uk are able to verify that these are from the Council and not a third party;
    - adopting the NCSC's Webcheck tool, which scans and reports on whitelisted publically available websites, and immediately brings threats to the attention of the Council for action; and
    - upgrading Microsoft Windows 10 from version 1511 (which left extended support in June 2018) to version 1703, and maintaining a best practice patching cycle for all applications.

9. During the year, the Council used an external CHECK approved assessor as part of its annual Public Services Network (PSN) compliance audit. This highlighted some areas for improvement, which were addressed in-year and the Council retained its PSN compliance certificate in November 2018.

10. The Council also took part in the Local Government Association's (LGA's) 2018 Cyber Security Stocktake and received an overall rating of 'Green'. As a result, the Council may be asked to support other councils in developing their cyber security arrangements. Areas for improvement identified in the stocktake will be progressed during 2019.

11. It should also be noted that significant progress was made in 2018 to strengthen disaster avoidance within ICT. An ICT Disaster Recovery (DR) Plan was developed during the year, integrated with the Council's overall approach to business continuity, and following an internal audit, was found to provide a Strong Control Environment by Tees Valley Audit and Assurance Services (TVAAS). The DR Plan was successfully tested in late 2018.

12. The issue of starters / leavers / movers notifications was discussed and reviewed during the year. Currently ICT modify systems access when notified by managers that, for example, an employee has left the organisation. Sometimes this is not done in a timely fashion, potentially creating a risk of data breach. A plan is now in place for this process to be automated and linked to HR processing of leavers and movers, removing reliance on manager notification.

Data protection

13. The most significant challenge within information risk management that the Council faced in 2018 was the implementation of GDPR and DPA 2018, which came into force on 25 May 2018.

14. During the year the Council put in place robust project governance arrangements to achieve a GDPR compliance baseline, assigning specific activities to workstreams covering policy, contracts, ICT, data audit, and communications.

15. Significant time and effort together with targeted training and facilitation services from an external consultancy were employed to assess the Council's readiness for GDPR, identify any gaps in current compliance, and implement the necessary changes to policies, procedures, and general training. Specialist eLearning modules were procured and mandatory completion requirements for employees were put in place. Elected members (as separate data controllers) were also offered training.

16. A dedicated Data Protection Officer (DPO) was recruited to post in early 2018 and this resource was further supplemented later in the year with the appointment of an Assistant DPO following a review of the resource requirements of the new data protection regime.

17. Work to further enhance the Council's GDPR compliance to exceed the identified baseline standard is on target, as evidenced through the risk treatment documented in the two related strategic risk profiles:

    - Failure to adopt a detailed and documented approach to GDPR.
    - Staff failing to adopt secure working practices.

18. Treatments include the development of a data protection communications plan, training strategy, and the audit work programme is on-going. The main combined focus of this work is to facilitate the necessary cultural change to embed responsibility within the role of the Council's managers for on-going compliance with the new laws. This is a key requirement of the new GDPR principles, specifically accountability – that data controllers are responsible for compliance with the data protection principles, wider than just security, and must be able to demonstrate this.

19. In relation to security incidents, the table below summarises the number of incidents involving personal data breaches or information security incidents and those reported to the ICO in the year to date. The numbers of incidents are slightly higher than the previous year and Quarter Four statistics are not yet compiled. However, these increased numbers are due to the significant changes to personal data breach reporting requirements brought in by GDPR.

Incident Type	**Total**	**Reported to ICO**
Disclosed in Error	40	3
Lost or stolen paperwork	3	2
Unauthorised access/disclosure	4	2
Other - Breach of Confidentiality	1	-
Other - Data Quality Leading to Disclosure	1	-
Other - Building Security	1	-
Total	**50**	**7**

20. As background context, the ICO reported a doubling of incidents nationally notified to them from May to June 2018. Under the previous legislation, there was no legal requirement to report data breaches. However, under GDPR organisations are required to record all personal data breaches and where these present a risk to the rights and freedoms of the individuals affected or likely to be affected, report them to the ICO.

21. Every incident reported to the DPO is logged and investigated. Improvement actions are advised to service areas and implementation monitored. This has resulted in

specific business process improvement to prevent re-occurrences and, where it has been deemed necessary, a number of members of staff receiving sanctions from management where investigations have found that they have breached Council policies.

22. As is typical in local government, the great majority of all reported incidents are due to human error, rather than cyber-attack or common theft. Significant work has been undertaken during 2018 to minimise such human error, including the ongoing reduction in the Council's physical records, eradicating the use of paper diaries and notebooks, and the development of new approaches to mail and print. Discussions have also been held during the year to reduce the risk of unauthorised access to buildings that house physical records during the period of reconfiguration running up to the opening of the Council's new headquarters in 2020. A business change programme is in development that will lead to the effective implementation of the new ways of working that will be required in the new HQ – as well as improving service delivery, this will contribute significantly to the reduction of information risk.

23. In addition to the logging and reporting of incidents, the DPO has a statutory duty to monitor compliance and provide assurance and advice to the Council. The DPO continues to meet regularly with senior managers and their teams and on a quarterly basis with the Chief Executive and the SIRO to provide regular updates and highlight issues for attention where this is necessary.

Information Requests

24. The following table summarises information requests received by the Council in 2018 and trends over the past three years.

Request	2016	2017	2018	% change	% in time	% in time trend
Data Protection Acts 1998 / 2018						
Subject Access Requests	53	42	72	+71%	68%	Down
S.29 requests / Schedule 2, part 1, para 2	65	56	91	+62.5%	N/A	N/A
S.31 requests	0	2	0	N/A	N/A	N/A
S.35 requests / Schedule 2, part 1, para 5	10	10	12	+20%	N/A	N/A
Freedom of Information Act 2000						
FOI requests	1,229	1,266	1,343	+6%	89%	Down
Requests to review initial responses	21	10	23	+130%	87%	Up
Appeals	2	2	5	+150%	100%	Same
Appeals upheld (in MBC favour)	0	2	TBC	TBC	N/A	N/A
Environmental Information Regulations 2004						
EIR requests	75	197	206	+4.6%	94%	Down
Total	**1,455**	**1,585**	**1,752**	**+10.5%**		

25. As anticipated, the numbers of Subject Access Requests received by the Council increased significantly, in line with increased public awareness of data rights arising from GDPR, together with the removal of fees associated with such requests.

26. There is no national benchmarking data on numbers of FOI requests received by local authorities, but as many are sent to all or groups of local authorities, it is reasonable to assume that overall the numbers received by the Council is not uncommon. The

Council continues to receive a high number of EIR requests, largely relating the Council's land and property transactions.

27. Overall, the number of information requests received by the Council rose by 10.5% in 2018, up from 9% in 2017. The volume of requests places a considerable burden on all of those involved in responding to them, and the timeliness of responses fell during 2018, with SARs a particular concern at the present time. By way of comparison, the UK Government average currently stands at 92% in time for FOI. SARs and FOI reviews are historically less timely due to the level of complexity involved. It is however worth noting that (again, based on the most recently published data) the Council fulfils a much greater proportion of FOI requests than the Government average, with 82% of requests granted in full or in part, compared with 42% for Government bodies.

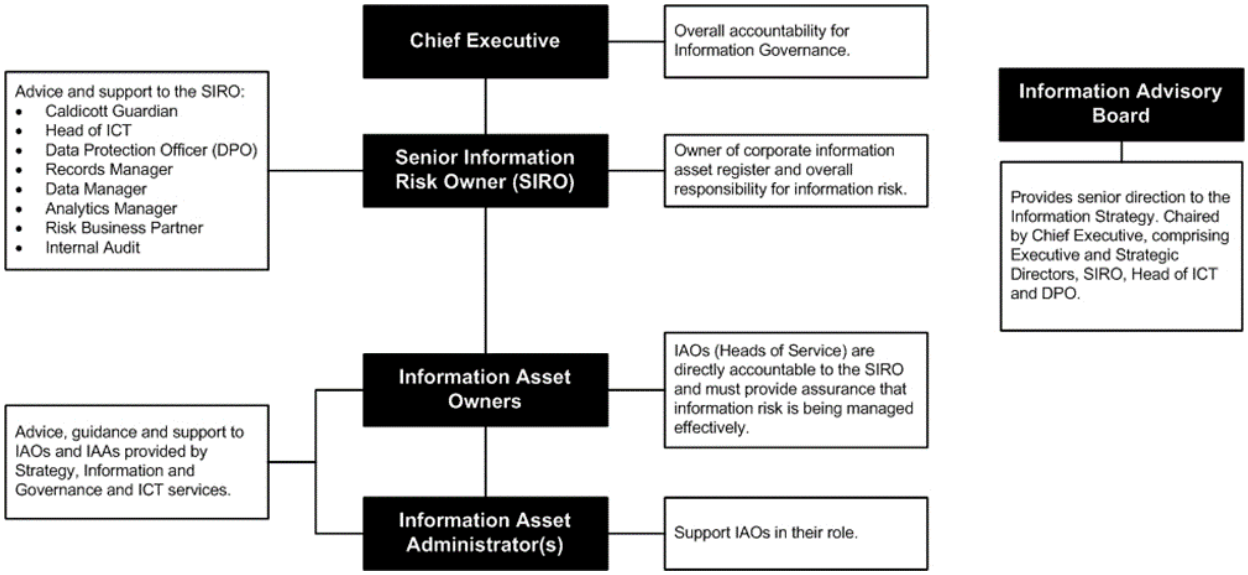
Information Strategy

28. In November 2018, LMT agreed an Information Strategy for the Council for the period 2018-2022. The strategy vision is that *the right information will be available to the right users, at any time, accessible from anywhere, underpinning the achievement of the Council's strategic objectives*.

29. The strategy provides an overall view of the fitness for purpose of information across the Council's service areas, taking into account the following criteria:

- Security
- Confidentiality
- Accuracy
- Completeness
- Timeliness
- Relevance
- Reliability
- Validity
- Availability

30. This assessment will act as the baseline for efforts to improve our information over the next four years, and a means of tracking progress. The strategy will be governed via the following structure.



Restructuring

31. The Information Strategy will allow all those working to improve information and reduce information risk to work in a systematic and integrated manner. During 2018, the Strategy, Information and Governance service was restructured to better support the implementation of the strategy. This restructure provides for dedicated posts of Data Protection Officer, Records Manager, Data Manager and Analytics Manager. Each officer is appropriately supported and training plans are in place for these employees.

Other issues of note during the year

32. RIPA is the law governing the use of surveillance techniques by public authorities, including local authorities. RIPA requires that when public authorities need to use covert techniques to obtain private information about someone, they only do so if surveillance is necessary, proportionate, and compatible with human rights. Typically this relates to suspected criminal activity that is likely to result in a custodial sentence of six months or more.

33. In such instances, surveillance (either covert or directed) can be undertaken, subject to magistrate approval, if it is not possible to gather sufficient evidence to secure a prosecution without this.

34. In late 2018, the Council was subject to a (periodic) documentary inspection by the IPCO regarding its use of RIPA powers. This resulted in a letter stating that the Council had 'demonstrated a level of compliance that removes, for the present, the requirement for a full inspection'. The letter singled out training and the draft RIPA policy that will shortly be considered by the Executive Member for Finance and Governance for praise.

35. As part of the inspection the Council advised that RIPA statistics would from now in be included within the SIRO's Annual Report. The table below sets out the number of applications the Council has made to use RIPA in recent years, including the nature of the surveillance and the reasons why it was undertaken.

Year	Applications	Nature of surveillance	Suspected offence
2015/16	3	2 x Directed 1 x Directed & Covert	1 x Copyright Infringement 1 x Counterfeit Goods 1 x Illicit Tobacco Sales
2016/17	6	6 x Directed	4 x Illicit Tobacco sales 1 x Counterfeit goods 1 x Underage e-cig sales
2017/18	1	Directed	1 x counterfeit goods
2018/19	2	Directed	2x counterfeit goods

Assessment of information risk

36. The Council continues to take steps to implement effective information governance arrangements across the organisation, and activity undertaken during 2018 has

significantly enhanced these arrangements. Taking into account progress in the past year, the revised short-form version of the Council's information risk register is attached at Appendix 1.

Priorities for 2019

37. Priorities for 2019 to move risks towards the targeted scores set out above are as follows:

- Implementing actions from the 2018 LGA Cyber Security Stocktake, specifically providing specialist cyber security training for professionals in IT, implementing an intrusion alert system, and nominating a council member with lead responsibility for cyber security.
- Implementing a revised process for starters / leavers / movers notifications, removing reliance on manager notification, and reducing the risk of data breach.
- Implementing the Information Strategy and revised policies for Secure Working, Data Protection, Records Management, Data Management, Access to Information and RIPA that will underpin it.
- Continuing to enhance the functionality and securing of email, improving integration with Objective to allow email records to be better captured, and ensuring that the Council's system is able to offer the same level of security as the Government's GCSX accounts, when these end in March 2019.
- Digitising and / or archiving historic paper records as appropriate, minimising the creation of new paper records through revised approaches to print and mail, and shifting the majority of electronic records to our Enterprise Content Management System (Objective), to improve their accessibility and usefulness.
- Implementing a business change programme to ensure our managers and employees understand our IG framework and how to make it work for them. We will ensure that this integrates with other work being undertaken to modernise working practices in the run-up to our moving into our new headquarters in 2020.
- Automating data sharing where practicable, and ensuring that employees, and where appropriate partners and contractors, are provided with the tools to share information securely and effectively.
- Reducing the number of information requests reduce by proactively publishing commonly requested information via new Open Data portal, and establishing an arrangement within Children's Services to improve the responsiveness to SARs.

38. Future activity relating to data protection in particular will be influenced by Brexit, and progress on this will be monitored closely to ensure that the Council remains compliant with the future legal framework.

What decision(s) are being asked for?

39. That the Committee notes the position set out in the report, and proposes for consideration any further steps it may wish to see taken to promote good practice in information governance within the Council.

Why is this being recommended?

40. To support the Committee in discharging its responsibilities in relation to corporate governance, which includes information governance.

Other potential decisions and why these have not been recommended

41. Not applicable.

Impact(s) of recommended decision(s)

Legal

42. IG is governed by European and UK legislation, regulation, statutory guidance and case law. This report sets out, at a high level, the steps the Council is taking and plans to take in order to ensure compliance with this legal framework and minimise information risk.

Financial

43. It is anticipated that all activity set out in this report is achievable within existing and planned budgets.

Policy Framework

44. Current and planned activity outlined is consistent with the direction of travel set out in the 'Business Imperatives' section of the Strategic Plan, so this report does not vary the Council's Policy Framework.

Equality and Diversity

45. Not applicable.

Risk

46. This report sets out the Council's information risks and current arrangements and future plans for their management.

Actions to be taken to implement the decision(s)

47. Not applicable, as the report advises the Committee and seeks comment. The activity outlined in the main body of the report will result in significant improvements in the Council's information governance arrangements.

Appendices

Not applicable.

Background papers

08/02/18	Corporate Audit and Affairs Committee	Annual Report of the SIRO

Contact: Paul Stephens, Head of Strategy, Information and Governance
Email: paul_stephens@middlesbrough.gov.uk

Appendix 1: Information Risk Register at end 2018

Category	Risk	Current score[1]	Trend	Target score
Internal	**NEW** Breach of data rights due to untimely response to information requests	20	-	10
Internal	Breach caused by third party processor	15	Same	10
Internal	Internal misuse of data	15	Same	10
Communication	Loss of sensitive data by human error	15	Same	6
External	Loss of personal data from cyber attack	15	Same	5
Technical	**NEW** Unauthorised access due to ICT not being notified of movers / leavers	15	-	5
Internal	Non-compliance with information law, including GDPR	14	Same	7
Internal	Non-compliance with Baseline Personnel Security Standard	14	Same	7
Internal	Non-compliance with Payment Card Industry standard	10	Same	5
Internal	Insecure disposal of records	10	Down	5
Internal	Lack of employee golden record	9	Same	6
Internal	Ineffective staff training	9	Same	6
Internal	**NEW** Unauthorised access due to tailgating / break-in	9	-	3
Internal	Non-compliance with NHS IG Toolkit	5	Same	5
Technical	Disaster recovery	5	Down	5
Technical	Vulnerabilities in third party applications	5	Down	5
Technical	Unsupported infrastructure / applications	5	Down	5

[1] Scoring is in line with the Council's Risk Management Framework. Low risks = <8, Medium = 9-15, and High = >20.

Category	Risk	Current score	Trend	Target score
Technical	Unauthorised access due to incorrect security settings	5	Same	5
Technical	Patching failure	5	Same	5
Technical	Insecure disposal of hardware	5	Same	5
Internal	Non-compliance with Public Services Network standard	5	Same	5
Technical	Encryption failure	2	Same	2