LGA Cyber Security Self-Assessment Tool – Question Set

Introduction

1. Please confirm the type of council.
    1. County council
    2. District council
    3. Single Tier

2. Please confirm the council's region.
    1. North East
    2. North West
    3. Yorkshire and the Humber
    4. East Midlands
    5. West Midlands
    6. East of England
    7. London
    8. South East
    9. South West

3. Please confirm the council's official name.

4. Please confirm your full name.

5. Please confirm your job title at the council.

6. Please confirm your phone number.

7. Please confirm your email address.

Leadership, reporting and ownership

8. Which board is ultimately responsible for cyber security matters?
    1. The most senior executive board (or equivalent)
    2. IT board (or equivalent)
    3. Not reported to a board

9. Do you know who the chair of the board responsible for cyber security matters is?
    1. Yes
    2. No

10. In the last 12 months, how many times has cyber security featured on the agenda of this board?

1. Monthly
2. Quarterly
3. Annually
4. Less than annually
5. Not reported, unless there is a serious incident
6. Not reported, but updates are ad hoc and occur with no fixed timescale
7. Not at all

11. What cyber security matters are reported to this board? (Tick all that apply.)

1. Compliance updates
2. Incident management
3. Risk assessments
4. Cyber security audits
5. Cyber security incidents or 'near misses'
6. Cyber security prevention measures
7. Patching and vulnerability management
8. Internal security policies and procedure (e.g. physical access)
9. External matters on general cyber security issues (e.g. threat landscape and policy developments etc.)
10. Other (please specify):

12. Are there clear lines of responsibility and accountability to named individuals for the cyber security of the council?

1. Yes
2. No

13. How often does the Chief Executive Officer receive cyber security updates?

1. Monthly
2. Quarterly
3. Annually
4. Less than annually
5. No updates, unless there is a serious incident
6. Updates are ad hoc and occur with no fixed timescale
7. Not at all
8. Other (please specify):

14. How often is there reporting on cyber security matters to the senior management team / corporate management team?

1. Monthly
2. Quarterly
3. Annually
4. Less than annually
5. No reporting, unless there is a serious incident
6. Updates are ad hoc and occur with no fixed timescale
7. Never any reporting
8. Other (please specify):

15. Is there a councillor with lead responsibility for cyber security?

1. Yes
2. No

16. How often do councillors receive updates concerning cyber security matters?

1. Monthly
2. Quarterly
3. Annually
4. Less than annually
5. No updates, unless there is a serious incident
6. Updates are ad hoc and occur with no fixed timescale
7. Never any reporting
8. Other (please specify):

17. In the last 12 months, how many times has cyber security featured on the agenda of the cabinet (or equivalent)?

1. Monthly
2. Quarterly
3. Annually
4. Less than annually
5. Not reported, unless there is a serious incident

18. Does the council have a specific cyber security budget?

1. Yes
2. No, it is incorporated into the wider IT budget
3. No, it is part of another budget

19. Does a member of the Senior Leadership Team have the appropriate security clearance to work on an incident with national partners?

1. Yes
2. No

Governance, structures and policies

20. Does the council have a cyber security risk register?

1. Yes
2. No

21. Does the council have an information technology (IT) risk register that references cyber security?

1. Yes
2. No

22. Does the council have an IT disaster recovery plan?

1. Yes
2. No

23. Is the IT disaster recovery plan designed and tested with third parties?

    1. Designed and tested with main suppliers
        1. Yes
        2. No
    2. Designed and tested with shared service partners
        1. Yes
        2. No
    3. Designed and tested with partner organisations (e.g. WARPs or NCSC)
        1. Yes
        2. No
    4. Designed and tested with public sector partners (e.g. CCG, Fire Service, Police)
        1. Yes
        2. No

24. How frequently is the council's IT disaster recovery plan tested, partially or in full?

    1. 0-5 months
        1. In full
        2. Partially
        3. Not tested

    2. 6-12 months
        1. In full
        2. Partially
        3. Not tested

    3. 12+ months
        1. In full
        2. Partially
        3. Not tested

25. Does the council have a board-level agreed ‘critical applications list’ for prioritising IT resilience and recovery planning?
    1. Yes
    2. No

26. Is there a single responsible officer for the council’s IT security policies and procedures (e.g. IT risk register and IT disaster recovery plans)?
    1. Yes
    2. No

27. Is there a minimum cyber security standard laid out and enforced for products and services by the council for third party suppliers?

    1. Laid out for third-party products
        1. Yes
        2. No

2. Enforced for third-party products
   1. Yes
   2. No

3. Laid out for third-party services
   1. Yes
   2. No

4. Enforced for third-party services
   1. Yes
   2. No

28. Does the council have business continuity plans that reference cyber security arrangements?
    1. Yes
    2. No

29. Does the council have civil continuity plans (emergency planning) that references cyber security arrangements?
    1. Yes
    2. No

30. Does the council have a corporate risk register that references cyber security arrangements?
    1. Yes
    2. No

31. Is the IT disaster recovery plan reviewed and agreed alongside business continuity plans, civil continuity plans or corporate risk register by the board responsible for cyber security?

    1. Business continuity
       1. Yes
       2. No

    2. Civil continuity (emergency planning)
       1. Yes
       2. No

    3. Corporate risk register
       1. Yes
       2. No

32. Are there policies and processes in place across the whole council to detect, manage and respond to cyber incidents?

    1. Incident detection policies and processes
       1. Yes
       2. In part
       3. No

2. Incident management and response policies and processes
    1. Yes
    2. In part
    3. No

33. In the event of a complete denial of service attack, could the council access its critical documents and Emergency Response Plan?
    1. Yes
    2. No

Partnerships, information, advice and guidance

34. Is the council aware of the Warning, Advice and Reporting Point (WARP) in the region?
    1. Yes
    2. No

35. Is the council a member of the regional WARP?
    1. Yes
    2. No

36. How often does a representative of the council attend WARP meetings?
    1. All meetings
    2. More than half
    3. Fewer than half
    4. Never

37. How often does the council engage with the WARP in a proactive way (e.g. seek information, advice and guidance?)
    1. Monthly
    2. Quarterly
    3. Annually
    4. Less than annually
    5. No, not unless there is a specific need
    6. Never

38. Is the council aware of the National Cyber Security Centre (NCSC) and the services they offer?
    1. Yes
    2. No

39. Has the council engaged with the NCSC on cyber security matters in the past 12 months?
    1. Yes
    2. No

40. Is the council currently using any of the following NCSC services? (Tick all that apply.)

1. Cyber Security Information Sharing Partnership (CiSP)
2. Domain-based Message Authentication, Reporting & Conformance (DMARC)
3. Web Check
4. Public sector DNS

41. How does the council engage with the NCSC in a proactive way (e.g. seeking information, advice and guidance?)

1. Contact with named NCSC staff
2. Website
3. Mailing list
4. Social media updates
5. Through the CISP
6. Through the WARP
7. No engagement
8. Other (please specify):

Technology, standards and compliance

42. Is the council adopting or compliant with ISO 27001?

1. Full adoption and formal compliance
2. Adopting and working towards formal compliance
3. Adopting but not working towards full compliance
4. Not adopting

43. Is the council adopting ISO 27001 across the whole council or in part across a specific area of service?

1. Yes, the whole council
2. Yes, in part across a specific area of service

44. Does the council have current and full Public Service Network (PSN) compliance?

1. Yes, the council has current compliance
2. The council does not have current compliance but is working towards it
3. The council does not have current compliance and is not working towards it

45. Has the council formally adopted any of the following cyber security measures, regimes or standards?

1. IG Toolkit / Data security and protection (DSP)
    1. Yes, full adoption
    2. Working towards adoption
    3. Not working towards adoption

2. Payment Card Industry Data Security Standard (PCI DSS)
    1. Yes, full adoption
    2. Working towards adoption
    3. Not working towards adoption

3. Cyber Essentials or Cyber Essentials Plus
    1. Yes, full adoption
    2. Working towards adoption
    3. Not working towards adoption

4. If the organisation has formally adopted any other relevant cyber security measures, regimes or standards, please list them below.

46. Is there specific and specialist training for cyber security professionals in IT (whether internally sourced or externally)?

1. Internal training
    1. Yes
    2. No

2. External training
    1. Yes
    2. No

47. Is the head of IT/CIO appropriately trained in Cyber Security (eg CISM, CIPPR etc.)?
    1. Yes
    2. No

Technology and standards - Identify

48. Please respond to the following statements:

1. The council has identified its key operational services.
    1. Yes, fully achieved
    2. Yes, partially achieved
    3. Not currently, but plans are in place to do so
    4. No, and there are currently no plans to do so

2. The council has identified the technologies, services and other dependencies (e.g. power cooling, data, people, etc.) that operational services rely on.
    1. Yes, fully achieved
    2. Yes, partially achieved
    3. Not currently, but plans are in place to do so
    4. No, and there are currently no plans to do so

3. The council has identified and catalogued all sensitive cyber security assets (e.g. devices, data, networks, etc.).
    1. Yes, fully achieved
    2. Yes, partially achieved
    3. Not currently, but plans are in place to do so
    4. No, and there are currently no plans to do so

4. The council has a structured cyber security risk management system in place.
   1. Yes, fully achieved
   2. Yes, partially achieved
   3. Not currently, but plans are in place to do so
   4. No, and there are currently no plans to do so

5. The council has identified and recorded which assets or services are operated by third party supplies.
   1. Yes, fully achieved
   2. Yes, partially achieved
   3. Not currently, but plans are in place to do so
   4. No, and there are currently no plans to do so

6. The council has identified and recorded the security responsibilities related to those third party operated information assets or services.
   1. Yes, fully achieved
   2. Yes, partially achieved
   3. Not currently, but plans are in place to do so
   4. No, and there are currently no plans to do so

Technology and standards - Protect

49. Please respond to the following statements:
    1. The council has identification processes in place to authenticate and authorise users of all IT systems.
       1. Yes, fully achieved
       2. Yes, partially achieved
       3. Not currently, but plans are in place to do so
       4. No, and there are currently no plans to do so

    2. The council has an auditable and robust procedure to verify each user and issue minimum required access rights.
       1. Yes, fully achieved
       2. Yes, partially achieved
       3. Not currently, but plans are in place to do so
       4. No, and there are currently no plans to do so

    3. The council has managed privileged access (e.g. to systems controlling essential or operational services) using separate accounts that are closely managed.
       1. Yes, fully achieved
       2. Yes, partially achieved
       3. Not currently, but plans are in place to do so
       4. No, and there are currently no plans to do so

4. The council tracks and records all hardware and software assets and their configuration.
    1. Yes, fully achieved
    2. Yes, partially achieved
    3. Not currently, but plans are in place to do so
    4. No, and there are currently no plans to do so

5. The council regularly tests for commonly known vulnerabilities or misconfigurations.
    1. Yes, fully achieved
    2. Yes, partially achieved
    3. Not currently, but plans are in place to do so
    4. No, and there are currently no plans to do so

6. The council regularly backs-up data in several different locations with different access controls to ensure the availability of essential services.
    1. Yes, fully achieved
    2. Yes, partially achieved
    3. Not currently, but plans are in place to do so
    4. No, and there are currently no plans to do so

7. The council has sensitive data stored using appropriate encryption mechanisms.
    1. Yes, fully achieved
    2. Yes, partially achieved
    3. Not currently, but plans are in place to do so
    4. No, and there are currently no plans to do so

8. The council has identified and accounted for all mobile devices (e.g. laptops and smartphones) that contain sensitive data.
    1. Yes, fully achieved
    2. Yes, partially achieved
    3. Not currently, but plans are in place to do so
    4. No, and there are currently no plans to do so

9. The council's internet services are segregated from internal systems and services.
    1. Yes, fully achieved
    2. Yes, partially achieved
    3. Not currently, but plans are in place to do so
    4. No, and there are currently no plans to do so

10. The council's networks and information systems (e.g. servers and high value information assets) are segregated into separate security zones.
    1. Yes, fully achieved
    2. Yes, partially achieved
    3. Not currently, but plans are in place to do so
    4. No, and there are currently no plans to do so

Technology and standards - Detect

50. Please respond to the following statements:

    1. The council has a structured vulnerability and patch management system in place.
        1. Yes, fully achieved
        2. Yes, partially achieved
        3. Not currently, but plans are in place to do so
        4. No, and there are currently no plans to do so

    2. The council uses network monitoring tools and programmes in order to detect potential cyber security intrusion.
        1. Yes, fully achieved
        2. Yes, partially achieved
        3. Not currently, but plans are in place to do so
        4. No, and there are currently no plans to do so

    3. The council has data logging practices, which are protected and where any modification is detected and attributed.
        1. Yes, fully achieved
        2. Yes, partially achieved
        3. Not currently, but plans are in place to do so
        4. No, and there are currently no plans to do so

    4. The council has the ability to detect abnormalities in system behaviour that are otherwise hard to identify.
        1. Yes, fully achieved
        2. Yes, partially achieved
        3. Not currently, but plans are in place to do so
        4. No, and there are currently no plans to do so

    5. The council conducts proactive vulnerability assessments or scans to detect threats.
        1. Yes, fully achieved
        2. Yes, partially achieved
        3. Not currently, but plans are in place to do so
        4. No, and there are currently no plans to do so

    6. The council uses threat intelligence feeds from external sources (e.g. Stix, Taxii, etc.) as part of its security management and network monitoring.
        1. Yes, fully achieved
        2. Yes, partially achieved
        3. Not currently, but plans are in place to do so
        4. No, and there are currently no plans to do so

7. The council uses security and event management software products and services (e.g. Security Incident Event Management [SIEM] or Security Operations Centre [SOC] tools) to manage cyber security alerts.

    1. Yes, fully achieved
    2. Yes, partially achieved
    3. Not currently, but plans are in place to do so
    4. No, and there are currently no plans to do so

Technology and standards - Respond

51. Please respond to the following statements:

1. All the council's cyber security incidents reports are recorded.
    1. Yes, fully achieved
    2. Yes, partially achieved
    3. Not currently, but plans are in place to do so
    4. No, and there are currently no plans to do so

2. The council has tested backups, which include all relevant key policies, documents and procedures, that can be restored in the event of a cyber security incident.
    1. Yes, fully achieved
    2. Yes, partially achieved
    3. Not currently, but plans are in place to do so
    4. No, and there are currently no plans to do so

3. The council has a pre-agreed prioritisation of which systems to restore or sustain. (E.g. social care functions first, frontline customer service hubs, etc.)
    1. Yes, fully achieved
    2. Yes, partially achieved
    3. Not currently, but plans are in place to do so
    4. No, and there are currently no plans to do so

4. The council has the capability to enact a cyber-attack response and recovery plan, given limitations to essential services and systems that may be impacted.
    1. Yes, fully achieved
    2. Yes, partially achieved
    3. Not currently, but plans are in place to do so
    4. No, and there are currently no plans to do so

52. Which of the following organisations would the council report a cyber security incident to? (Tick all that apply.)

1. Action Fraud
2. CiSP
3. Information Commissioner's Office (ICO)
4. NCSC
5. Police
6. WARP
7. We would not report it to any external organisation

Technology and standards – Recover

53. Please respond to the following statements:

1. The council performs post-incident assessments to identify and record lessons learned.
    1. Yes, fully achieved
    2. Yes, partially achieved
    3. Not currently, but plans are in place to do so
    4. No, and there are currently no plans to do so

2. The council has a process to ensure that lessons learned from previous incidents are reviewed and integrated into other relevant risk register and cyber security policies and procedures.
    1. Yes, fully achieved
    2. Yes, partially achieved
    3. Not currently, but plans are in place to do so
    4. No, and there are currently no plans to do so

54. Has the council been the subject to any of the following cyber-attacks in the past 12 months? If yes, please specify the total number of attacks and the number of successful attacks in the last 12 months. These can be estimates or actual figures. If no, please enter 'nil' for no attacks, or 'do not know' for do not know.

1. Insider threat or internal system misuse
    1. Yes, total number of attacks
    2. Yes, number of successful attacks
    3. No (nil / do not know)

2. DDoS
    1. Yes, total number of attacks
    2. Yes, number of successful attacks
    3. No (nil / do not know)

3. Malware
    1. Yes, total number of attacks
    2. Yes, number of successful attacks
    3. No (nil / do not know)

4. Phishing
   1. Yes, total number of attacks
   2. Yes, number of successful attacks
   3. No (nil / do not know)

5. Ransomware
   1. Yes, total number of attacks
   2. Yes, number of successful attacks
   3. No (nil / do not know)

6. Web attacks
   1. Yes, total number of attacks
   2. Yes, number of successful attacks
   3. No (nil / do not know)

7. If yes to any of the above, are the number of attacks above estimates or actual figures? Please provide details.

Training and awareness

55. Do all members of staff and councillors receive basic cyber security awareness training?

1. All members of staff
   1. Yes, this is mandatory on induction and refreshed regularly
   2. Yes, it is part of induction, but not formally renewed after that
   3. Yes, through voluntary on-line training
   4. No, there is nothing specific

2. Councillors
   1. Yes, this is mandatory on induction and refreshed regularly
   2. Yes, it is part of induction, but not formally renewed after that
   3. Yes, through voluntary on-line training
   4. No, there is nothing specific

56. Do all members of staff and councillors whose role involves using their own devices to remotely access council IT systems receive specific cyber security training?

1. All members of staff
   1. Yes, this is mandatory on induction and refreshed regularly
   2. Yes, it is part of induction, but not formally renewed after that
   3. Yes, through voluntary on-line training
   4. No, there is nothing specific
   5. No, staff do not use their own devices

2. Councillors
    1. Yes, this is mandatory on induction and refreshed regularly
    2. Yes, it is part of induction, but not formally renewed after that
    3. Yes, through voluntary on-line training
    4. No, there is nothing specific
    5. No, councillors do not use their own devices

57. Does the council conduct email phishing tests to test internal staff and councillor awareness?

1. All members of staff
    1. Yes
    2. No

2. Councillors
    1. Yes
    2. No

58. Which of the following methods does the council use to raise awareness of cyber security? (Tick all that apply.)

1. Email notifications
2. Text notifications
3. After incident email alert
4. Intranet
5. Blogs
6. Newsletters
7. Social media updates
8. Incident updates provided by communications team
9. Printed communications material (e.g. posters, brochures and other promotional items)
10. Online training courses or e-learning courses
11. Email phishing tests
12. Security policy tests
13. The council does not raise awareness of cyber security arrangements
14. Other (please specify):

59. Are you confident all members of staff and councillors are aware of relevant policies and procedures to report cyber security incidents or suspicious emails?

1. All members of staff
    1. Extremely confident
    2. Very confident
    3. Somewhat confident
    4. Not so confident
    5. Not confident at all

2. Councillors
    1. Extremely confident
    2. Very confident
    3. Somewhat confident
    4. Not so confident
    5. Not confident at all

Questionnaire close

60. Is there anything important to add or explain in relation to the council's assessment, or any other general observations?
    1. No
    2. Yes (please explain):

61. Have all questions in all sections in the questionnaire been completed?
    1. Yes

62. Is the information provided accurate to the best of your knowledge?
    1. Yes

63. Is this your final submission?
    1. Yes