



Ministry of Defence

Cyber Security Model Supplier Assurance Questionnaire (SAQ) Level 1

Last updated: December 2025

This preview of the Cyber Risk Profile Level 1 SAQ is a point-in-time version of the SAQ, accurate as of its publication date.

Any subsequent changes or updates will not be reflected in this preview.

Version	Date	Amendment
1.0	03/12/25	Publication

Please refer to the published applicant guides for the Defence Cyber Certification on the IASME website which provides guidance on a control-by-control basis.

Contents

General information.....	4
Cyber Essentials scheme.....	5
Governance.....	6
Risk management.....	7
Asset management.....	8
Supplier management.....	9
Physical management.....	11
Planning for resilience.....	13
Identity and access 1.....	14
Identity and access 2.....	16
Data security 1.....	19
Data security 2.....	21
Data security 3.....	26
System security 1.....	28
System security 2.....	33
System security 3.....	37
Network and system resilience.....	41
Awareness, Behaviours and Culture.....	44
Personnel and the environment.....	46
Security monitoring.....	49
Proactive detection.....	53
Incident response.....	54
Recovery and improvements.....	56

General information

1. How many people work in the organisation?

- Fewer than 10
- 10 to 99
- 100 or more

2. What is the name of the organisation's head of cyber security?

This could be a Chief Information Security Officer (CISO) or other role with responsibility for cyber security.

3. What is the best e-mail address for the organisation's cyber security function?

This could be a team or individual able to receive questions on cyber security.

Cyber Essentials scheme

1. Does the organisation hold Cyber Essentials (CE) certification that covers the required scope for this activity?

Yes No

2. Does the organisation commit to maintaining CE certification for the duration of any contract relating to this activity?

Only answer if Cyber Essentials scheme Q1 = Yes

Yes No

Governance

1. Does the organisation have documented management policies and processes in place that govern network and information system security?

Yes No

2. Are the organisation's management policies and processes:

Only answer if Governance Q1 = Yes

- Reviewed at least annually
- Assigned an owner for ongoing maintenance and review
- Communicated to all staff, including contractors
- Approved by management
- None of the above

3. Does the organisation have clearly defined roles and responsibilities for network and information system security at all levels, with established communication and risk escalation channels?

Yes No

Risk management

1. How often does the organisation actively manage cyber security risks across the entire organisation?

- At least quarterly
- Less than quarterly
- No risk management in place

2. Does the organisation assign dedicated risk owners to all identified risks?

Only answer if Risk management Q1 = NOT "No risk management in place"

- Yes No

3. How often does the organisation assess the risks to operations, assets, and individuals arising from the operation of its systems and the associated processing, storage, or transmission of data?

Only answer if Risk management Q1 = NOT "No risk management in place"

- At least annually
- Ad-hoc
- No risk assessment in place

4. Does the organisation maintain up-to-date network diagrams that illustrate network boundaries, internal and external connections, and operational systems?

- Yes No

Asset management

1. Does the organisation have a documented policy for asset management in place?

Yes No

2. Does the organisation have an asset classification process in place?

An asset classification process shall include defining asset types and value.

Yes No

3. Are all resources necessary for the operation of network and information systems documented in an asset inventory?

This includes people, systems and supporting infrastructure.

Yes No

Supplier management

1. Does the organisation have policies and procedures in place to manage the cyber security requirements of its supply chain?

Yes No

2. Does the organisation assess the security risks associated with its dependencies on suppliers?

Yes No

3. When does the organisation assess security risks related to its suppliers?

- Before selecting a supplier
- At least annually, for existing suppliers
- None of the above

4. Which of the following does the organisation do to ensure suppliers maintain appropriate security measures?

- Determine appropriate security requirements for the supply chain
- Review supplier contracts to ensure security requirements are met
- Monitor third-party security arrangements
- None of the above

5. What actions does the organisation take if a supplier fails to meet security requirements?

- Manage the risk through the organisation's risk management process
- Implement corrective actions or terminate the contract, where appropriate
- No defined process for addressing non-compliance

6. Are Service Level Agreements (SLAs) with IT infrastructure suppliers clearly documented?

Yes No

7. Do the organisation's agreements with suppliers include information security, confidentiality, and data protection requirements?

Yes No

8. Does the organisation impose restrictions on all subcontractors handling customer data to prevent unauthorised data sharing?

Yes No

Physical management

1. Does the organisation have a documented physical security policy in place?

Yes No

2. Does the organisation ensure physical access to facilities where sensitive data is stored or processed is restricted to authorised personnel?

Yes No

3. Does the organisation ensure records are retained of all physical access to facilities where sensitive data is stored or processed?

Yes No

4. Does the organisation perform any Functions or process Data from its own physical premises?

Yes No

5. Does the organisation maintain an inventory of all physical access devices used at its premises?

e.g. RFID cards, access fobs, door keys, keypads, biometric scanners.

Only answer if Physical management Q4 = Yes

Yes No

6. Does the organisation restrict physical access to sensitive areas of its premises to authorised personnel?

Only answer if Physical management Q4 = Yes

Yes No

7. Does the organisation maintain an up-to-date inventory of personnel authorised to access sensitive areas?

Only answer if Physical management Q6 = Yes

Yes No

8. Does the organisation manage visitor access to non-public areas of its premises, including logging their entry and exit?

Only answer if Physical management Q4 = Yes

Yes No

9. Does the organisation require visitors to always wear approved identification badges while on its premises?

Visitor badges should be different to staff badges.

Only answer if Physical management Q8 = Yes

Yes No

Planning for resilience

1. Does the organisation have documented policies and procedures in place that cover both cyber security and cyber resilience?

Yes No

2. Does the organisation review its cyber security and cyber resilience policies and processes at least annually?

Only answer if Planning for resilience Q1 = Yes

Yes No

Identity and access 1

1. Does the organisation have documented policies and procedures in place that cover identity management?

Yes No

2. Does the organisation have documented policies and procedures in place that cover access control?

Yes No

3. Before granting access to non-public resources, does the organisation ensure that the following are in place:

User identities are verified

Users are authorised

Users are authenticated

None of the above

4. Does the organisation remove, disable or restrict non-essential functions within its information systems?

Non-essential functions can include programs and services.

Yes No

5. Does the organisation provide user access to resources based on business need and the principle of least privilege?

Yes No

6. Does the organisation's access control policy include a separation of duties methodology?

Yes No

7. Which of the following does the organisation's separation of duties methodology consider:

Only answer if Identity and access 1 Q6 = YES

- Cover for duties during staff absence
- How user accounts (standard and privileged) will be provisioned to facilitate separation
- The criteria for when separation is needed
- None of the above

8. Does the organisation limit access to system audit and security logs to privileged users with a confirmed need for access?

- Yes No

Identity and access 2

1. Does the organisation have a documented process for issuing, managing, verifying, revoking, and auditing identities and credentials for authorised users, processes and transactions?

Yes No

2. Has the organisation implemented measures to ensure that only authorised individuals and processes can access systems using issued identities and credentials?

Yes No

3. Does the organisation secure the storage, transmission and management of first-time and one-time passwords?

Yes No

4. Does the organisation require that first-time and one-time passwords be changed immediately upon first login?

Yes No

5. Does the organisation's password policy require that standard user passwords have a minimum length of 8 characters?

Yes No

6. Does the organisation's password policy prevent users from reusing their last 5 passwords?

Yes No

7. Does the organisation have policies and procedures in place for managing unsuccessful login attempts?

Yes No

8. Are there automated mechanisms in place to detect and respond to multiple unsuccessful login attempts?

Yes No

9. Are unsuccessful login attempts regularly monitored and reviewed for signs of suspicious activity?

Yes No

10. Are there designated individuals or teams responsible for managing unsuccessful login attempts?

Yes No

11. How many incorrect password attempts are allowed before a standard user account is locked?

No more than 10 incorrect attempts

More than 10 incorrect attempts

No limit set

12. How long are user accounts locked out for after failed login attempts?

Only answer if Identity and access 2 Q11 = NOT "No limit set"

Less than 15 minutes

15 minutes or longer

13. Does the duration of the account lockout increase on further unsuccessful login attempts?

Only answer if Identity and access 2 Q11 = NOT "No limit set"

Yes No

14. Does the organisation implement technical controls to prevent replay attacks?

Yes No

15. Does the organisation maintain an inventory of all generic, service, and system accounts?

Yes No

16. Are generic and system accounts assigned a named individual responsible for the account and its usage?

Yes No

17. Does the organisation have a method of identifying system accounts and processes acting on behalf of actual users?

Yes No

Data security 1

1. Has the organisation identified and documented where data meets the following criteria?

- The data is critical to the operation of Functions
- The data could assist an attacker, such as network or system design details
- If the data were modified, deleted or accessed without authorisation it could lead to adverse impacts
- None of the above

2. Does the organisation have policies in place to ensure only authorised users, devices, and systems have access to this data?

Only answer if Data security 1 Q1 = NOT "None of the above"

- Yes No

3. Does the organisation have technical and procedural controls in place to protect this data from unauthorised access, modification, or deletion?

Only answer if Data security 1 Q1 = NOT "None of the above"

- Yes No

4. Does the organisation require network connections to be terminated under the following conditions?

- After a defined period of inactivity no greater than 24 hours.
- At the end of sessions.
- None of the above.

5. Does the organisation require all trusted organisational wireless networks to authenticate users and devices and authorise them before granting access?

- Yes No

6. Do all trusted organisational Wi-Fi networks require Wi-Fi Protected Access 2 (WPA2) or newer encryption standards?

Yes No

7. Does the organisation require visitors without trusted devices to use separate wireless networks which are segregated from trusted organisational networks?

Yes No

8. Does the organisation require Multi-Factor Authentication (MFA) for users connecting remotely to its networks and systems?

Yes No

9. Does the organisation encrypt all data transmitted through Virtual Private Network (VPN) connections?

Yes No

10. Does the organisation disable split-tunnelling for users connecting remotely to its networks and systems, to ensure all Data is only transmitted via organisation-controlled channels?

Yes No

11. Does the organisation use cryptography to protect remote access sessions?

Yes No

12. Does the organisation route all remote access connections through managed access control points?

Yes No

Data security 2

1. Does the organisation maintain an inventory of all its managed Removable Storage Media & Devices (RSM&D)?

Yes No

2. Which encryption algorithm(s) does the organisation implement for its managed Removable Storage Media & Devices (RSM&D)?

- Those approved by FIPS-140-2 or later
- Those approved by a national authority
- Advanced Encryption Standard (AES) 256
- Other

3. Does the organisation prevent the use of unauthorised Removable Storage Media & Devices (RSM&D) by taking the following actions?

- Maintaining records of authorised RSM&D
- Prohibiting staff and visitors from using unauthorised RSM&D
- Granting read/write permissions only to authorised RSM&D
- None of the above

4. Does the organisation maintain and update a list of authorised working locations (outside of the organisation's premises) and inform all staff of these locations?

Yes No

5. Does the organisation provide privacy protectors for devices when staff work in environments with an unacceptable risk of oversight from bystanders?

Yes No

6. Does the organisation's user awareness training cover the cyber security risks of working outside the organisation's premises?

Yes No

7. Does the organisation enforce the use of "always-on" Virtual Private Network (VPN) for endpoints where remote users are at risk?

Yes No

8. Does the organisation manage and restrict the connection of peripherals/media to USB ports, except when authorised by policy?

Yes No

9. Does the organisation risk assess and, unless required, disable the USB and other physical ports on laptops and portable devices?

Yes No

10. Has the organisation implemented full disk encryption on all devices used by employees when working outside the organisation's premise?

Yes No

11. Does the organisation have documented policies and procedures to ensure compliance with obligations under the UK General Data Protection Regulation (GDPR)?

Yes No

12. Does the organisation implement Domain-based Message Authentication, Reporting and Conformance (DMARC) for all internet-facing email services?

Yes No

13. Does the organisation implement DomainKeys Identified Mail (DKIM) to enhance trust in all internet-facing email services?

Yes No

14. Does the organisation implement the Sender Policy Framework (SPF) to protect internet facing email domains against spoofing?

Yes No

15. Does the organisation have procedures in place to identify and authorise the flow of the following types of information?

Personal information provided or produced during a contract.

Government information provided or produced during a contract.

None of the above.

16. Does the organisation require the flow of personal and government information to be controlled in accordance with the following?

Contractual requirements

Applicable legislation

Approved authorisations

None of the above

17. Does the organisation maintain documentation/diagrams of authorised personal and government information flows between the following?

Jurisdictions

Networks

Systems

Users

None of the above.

18. Does the organisation employ systems to control the authorised flow of personal and government data?

Yes No

19. Does the organisation employ systems to monitor personal and government data flows to ensure compliance with its authorisations?

Yes No

20. Does the organisation implement and maintain full disk level encryption on all endpoints?

Yes No

21. Which encryption algorithm(s) does the organisation implement for endpoint full disk encryption?

Only answer if Data security 2 Q20 = Yes

Those approved by FIPS-140-2 or later

Those approved by a national authority

AES-256

Other

22. Does the organisation have a policy governing the use of cryptographic methods?

Yes No

23. Which cryptographic methods does the organisation use when protecting Data with encryption?

Methods approved by a national authority

Methods approved in FIPS-140-2 or later

Other

24. Does the organisation's encryption key management policy and procedures cover the following aspects?

- Compliance with local legal and regulatory requirements for cryptography
- Restriction of cryptographic key access to authorised individuals
- Cryptographic key activation and deactivation dates
- Maintenance of cryptographic key backups
- Management of lost, corrupt and expired keys
- Cryptographic keys revocation
- Secure storage, distribution and update of cryptographic keys
- Required key lengths
- None of the above

Data security 3

1. Does the organisation have designated individuals authorised to make information publicly available?

Yes No

2. Does the organisation train designated individuals to ensure that publicly accessible information does not contain non-public information?

Yes No

3. Does the organisation review proposed content before posting it to publicly accessible systems to ensure that non-public information is not included?

Yes No

4. Does the organisation periodically review the content on publicly accessible systems for non-public information and remove such information if discovered?

Yes No

5. Does the organisation ensure all mobile devices accessing its corporate environment/Data are appropriately configured and managed using Mobile Device Management (MDM) or equivalent solutions?

Yes No

6. Does the organisation have a process to disable or wipe organisation data if the mobile device is stolen or lost?

Yes No

7. Has the organisation implemented procedures to ensure that all Data is securely destroyed when no longer required?

Yes No

8. Does the organisation ensure any third parties engaged to process Data securely dispose of such Data when no longer required?

Yes No

System security 1

1. Does the organisation identify the systems and technologies critical to the operation of its Functions and protection of Data?

Yes No

2. Does the organisation protect critical systems from cyber-attacks by implementing system security measures based on its understanding of risks to Functions and Data?

Yes No

3. Does the organisation securely configure the network and information systems that support its Functions and protect Data?

Yes No

4. Does the organisation have a vulnerability management process in place?

Yes No

5. Does the organisation ensure systems are scanned for vulnerabilities:

Only answer if System security 1 Q4 = Yes

- Following major system or application updates
- At least monthly
- None of the above

6. Does vulnerability scanning include all:

Only answer if System security 1 Q4 = Yes

- Infrastructure / Networks
- Applications
- Web services
- None of the above

7. Does the organisation develop risk treatment plans to address (remediate or mitigate) identified vulnerabilities promptly?

Only answer if System security 1 Q4 = Yes

Yes No

8. Does the organisation have defined timelines for addressing vulnerabilities?

Only answer if System security 1 Q4 = Yes

Yes No

9. Is the organisation's timeline for addressing critical severity vulnerabilities (as defined by the Common Vulnerability Scoring System v3):

Only answer if System security 1 Q8 = Yes

- Within 15 days
- Outside 15 days

10. Is the organisation's timeline for addressing high severity vulnerabilities (as defined by the Common Vulnerability Scoring System v3):

Only answer if System security 1 Q8 = Yes

- Within 30 days
- Outside 30 days

11. Is the organisation's timeline for addressing medium severity vulnerabilities (as defined by the Common Vulnerability Scoring System v3):

Only answer if System security 1 Q8 = Yes

- Within 90 days
- Outside 90 days

12. Is the organisation's timeline for addressing low severity vulnerabilities (as defined by the Common Vulnerability Scoring System v3):

Only answer if System security 1 Q8 = Yes

- Within 180 days
- Outside 180 days

13. Does the organisation ensure that penetration testing is conducted on externally facing systems at least every 12 months?

- Yes
- No

14. Is the organisation's penetration testing programme based on industry standards and conducted by subject matter experts?

- Yes
- No

15. Which of the following does the organisation's penetration testing records include?

- Remedial action plan with timelines
- Testing date
- Name of the tester (organisation / individual)
- Findings by severity
- Test scope and methodology
- None of the above

16. Does the organisation have formal change management policies, processes and procedures in place?

- Yes
- No

17. Are the organisation's change management policies, processes and procedures reviewed at least annually?

Only answer if System security 1 Q16 = Yes

- Yes No

18. Which of the following are included in the organisation's change management policy?

Only answer if System security 1 Q16 = Yes

- Required processes and procedures
- The types of change (e.g. standard, normal, emergency)
- Roles and responsibilities for change management
- None of the above

19. Prior to implementing a change, which of the following are undertaken?

Only answer if System security 1 Q16 = Yes

- Stakeholder approval is obtained
- Back-out procedures are documented
- Any security mitigations required are documented
- Security impact of change is analysed and recorded
- Business impact of change failure is analysed
- A change record is kept in a central repository
- Acceptance criteria are established
- None of the above

20. Which of the following are retained as an audit trail of a change?

Only answer if System security 1 Q16 = Yes

- Change outcome
- Approvals

Test history & documentation

None of the above

21. Does the organisation have a patch management policy and programme in place?

Yes No

22. Does the organisation monitor its technology vendors to ensure timely awareness of updates for its endpoints, network devices, and software?

Yes No

23. Does the organisation assess which vendor updates address vulnerabilities?

Yes No

24. Does the organisation ensure patches are tested before deployment to critical production environments?

Yes No

25. Does the organisation ensure systems are patched promptly, and within 14 days of an update being released which addresses a vulnerability classified by the product vendor as 'critical' or 'high risk'?

Yes No

26. Does the organisation have processes in place to enable out-of-band emergency patching?

Yes No

System security 2

1. Does the organisation ensure users acknowledge warning notices before accessing systems with specific handling requirements, where mandated by the UK and/or international partner nations?

Yes No

2. Which of the following are included within your warning notices for systems which have specific handling requirements imposed by the UK or its International Partners.

Only answer if System security 2 Q1 = Yes

The information system contains information with specific requirements imposed by the UK and/or international partner nations

Use of the information system may be subject to other specified requirements associated with certain types of information, such as that subject to Export Controls or licences.

None of the above

3. Does the organisation ensure that warning notices regarding specific handling requirements are only provided to authorised and authenticated users?

Only answer if System security 2 Q1 = Yes

Yes No

4. Does the organisation automatically lock user sessions on all devices after a predefined period of inactivity?

Yes No

5. Is the organisationally defined period of inactivity for normal users:

Only answer if System security 2 Q4 = Yes

15 minutes or less More than 15 minutes

6. Do locked user sessions and lock screens conceal all information previously displayed on the screen?

Yes No

7. Does the organisation maintain an up-to-date list of authorised software?

Yes No

8. Does the organisation implement a 'block by default, permit-by-exception' policy for software not on the authorised list?

Only answer if System security 2 Q7 = Yes

Yes No

9. Does the organisation review its list of authorised software programs at least every 90 days?

Yes No

10. Does the organisation enforce endpoint controls for internet access, in line with its internet access policy, to block the following?

Suspicious traffic and communications

Downloads without sandboxing and anti-malware scanning

Execution of code on the endpoint

Access to undesirable internet resources (e.g. malicious websites, inappropriate content, etc...)

Malware infections from internet browsing

None of the above

11. Where the organisation's policy permits any of the above activities due to business need, does it ensure processes and technologies are in place to mitigate the additional risk?

Yes No

12. Does the organisation ensure auditing is enabled for internet access endpoint controls?

Yes No

13. Does the organisation ensure security operators are alerted to blocked internet activity?

Yes No

14. Does the organisation ensure systems terminate connections to internet resources at the end of sessions or after a defined period of inactivity?

Yes No

15. Does the organisation have a documented policy in place for the use of Voice over IP (VoIP) technologies?

Yes No

16. Has the organisation's Voice over IP (VoIP) policy been informed by a risk assessment of malicious VoIP usage?

Only answer if System security 2 Q15 = Yes

Yes No

17. Are all VoIP technologies in the organisation:

Only answer if System security 2 Q15 = Yes

Yes No

18. Does the organisation define acceptable and unacceptable use of mobile code?

Yes No

19. Does the organisation ensure controls are in place to identify, authorise, monitor, review, and control the use of mobile code within the organisation?

Yes No

20. Does the organisation protect communication sessions requiring authenticity by enforcing secure communication protocols?

Yes No

System security 3

1. Does the organisation ensure that appropriate authorisations and approvals are granted before privileged actions are carried out remotely?

Yes No

2. Has the organisation established baseline configurations for all organisational systems?

Yes No

3. Does the organisation incorporate system hardening procedures into its system baselines?

Only answer if System security 3 Q2 = Yes

Yes No

4. Do the organisation's baseline configurations include restrictions on the following?

Only answer if System security 3 Q2 = Yes

Use of unsupported software and hardware

User actions

None of the above

5. Are the organisation's baseline configurations:

Only answer if System security 3 Q2 = Yes

Reviewed at least annually

Updated when changes are made to the baseline

Implemented

Documented

None of the above

6. Does the organisation have controls in place that obscure authentication information?

e.g. passwords input by users

Yes No

7. Does the organisation minimise feedback information from failed logins to ensure that the system does not provide any information that would assist unauthorised individuals in compromising authentication mechanisms?

Yes No

8. Does the organisation synchronise the time across all devices by using the Network Time Protocol (NTP)?

Yes No

9. Does the organisation enforce physical and logical access restrictions for making changes to organisational systems, including upgrades and modifications?

Yes No

10. Does the organisation ensure that the physical and logical access restrictions for its organisational systems are defined, documented, and approved?

Yes No

11. Does the organisation deploy automated tools to identify, register, and maintain a trusted inventory of its critical system components?

Yes No

12. What data is recorded in these inventories?

Only answer if System security 3 Q11 = Yes

Ownership of assets

- The location of critical system components
- None of the above

13. Has the organisation implemented anti-malware capabilities on its systems?

- Yes No

14. Does the organisation ensure that malware signatures and software are updated promptly when new releases are made available?

Only answer if System security 3 Q13 = Yes

- Yes No

15. Does the organisation regularly audit its anti-malware implementations to ensure they are:

Only answer if System security 3 Q13 = Yes

- Being updated routinely and promptly
- Functional (e.g. performing real-time scans as well as periodic scans)
- Under active management
- Detecting sample malware
- Reporting detections correctly
- None of the above

16. Does the organisation, at its external boundaries and key internal boundaries of organisational systems, do the following?

- Protect communications
- Monitor communications
- Control communications
- None of the above

17. Does the organisation control and limit connections to external systems using an allow-list at the network boundary?

Yes No

18. Does the organisation block all inbound connections from external systems, unless approved in an allow-list?

Yes No

19. Does the organisation ensure firewall rules are managed, approved and documented by an authorised and competent person?

Yes No

Network and system resilience

1. Has the organisation assessed the degree to which its systems must be resilient to cyber-attack and system failure?

Yes No

2. Has the organisation built resilience into its systems to meet its resilience needs?

Only answer if Network and system resilience Q1 = Yes

Yes No

3. Does the organisation design its network and information systems, which support its Functions and protect Data, to be resilient to identified cybersecurity incidents and system failures?

Yes No

4. Do the organisation's resilient designs consider the appropriate level of segregation between systems?

Only answer if Network and system resilience Q3 = Yes

Yes No

5. Do the organisation's resilient designs account for the levels of resources required for systems to operate?

Only answer if Network and system resilience Q3 = Yes

Yes No

6. Does the organisation develop recovery plans for all systems to ensure recovery from cyber attacks and system failures?

Yes No

7. Does the organisation ensure that accessible and secure backups of data are maintained to support the recovery of its functions and protect data?

Yes No

8. Does the organisation secure backups with appropriate encryption technology to prevent unauthorised parties from viewing or tampering with backup data?

Only answer if Network and system resilience Q7 = Yes

Yes No

9. Does the organisation perform backup integrity validation to ensure backups are completed without error and are accessible?

Only answer if Network and system resilience Q7 = Yes

Yes No

10. Does the organisation ensure that firewalls block all network connectivity paths and services by default, unless explicitly authorised by the appropriate Change Advisory Board (CAB) or equivalent?

Yes No

11. Does the organisation ensure that enabled network connectivity paths and services are regularly reviewed and removed if there is no ongoing business need?

Yes No

12. Does the organisation ensure that publicly accessible systems and networks are physically and/or logically segregated from internal systems and networks using network segmentation?

Yes No

13. Does the organisation use tools or methods to detect, block, and report malicious or spam emails attempting to enter the organisation?

Yes No

14. Does the organisation check all media containing diagnostic and/or test programs for malicious code prior to use?

Yes No

15. Does the organisation ensure the tools, techniques and mechanisms used by maintenance personnel are either authorised or provided by the organisation?

Yes No

16. Where non-local maintenance sessions are required to resolve an issue, does the organisation ensure Multi-Factor Authentication (MFA) is enabled to verify the identity of the individual before granting access to the system?

Only answer if Network and system resilience Q15 = Yes

Yes No

17. Once non-local maintenance activity is complete, does the organisation ensure all remote sessions are terminated?

Only answer if Network and system resilience Q16 = Yes

Yes No

18. Does the organisation require authorised, qualified, and experienced staff to supervise any maintenance workers who lack the necessary physical access permissions?

Yes No

Awareness, Behaviours and Culture

1. Does the organisation have a cyber security awareness and training programme that ensures staff possess the appropriate cyber security knowledge, skills, and awareness for their roles?

Yes No

2. Does the organisation review and update the security risks that system users, administrators and managers should be aware of:

- When there are significant change to the threat
- When there is significant organisational change
- At least annually
- None of the above

3. Does the organisation ensure system users, system administrators and management are made aware of relevant:

- System security procedures
- System security standards
- System security policies
- Security risks
- None of the above

4. Does the organisation have a formal Acceptable Use Policy in place?

Yes No

5. Does the scope of the organisation's Acceptable Use Policy include appropriate restrictions on:

Only answer if Awareness, Behaviours and Culture Q4 = Yes

- Use, including remote activation, of any collaborative computing devices (e.g. remote meeting cameras)
- Locations for conducting duties
- Handling of physical corporate assets outside the office environment
- Clear desk and clear screen requirements
- Use of organisation-provided identifiers (e.g., email addresses) and authentication secrets (e.g., passwords) for creating accounts on external sites/applications
- Posting organisational information on public websites
- Use of social media, social networking sites, and external sites/applications
- None of the above

Personnel and the environment

1. Does the organisation conduct appropriate pre-employment background checks for staff who will have access to Data?

Irrespective of employment type or affiliation (employee, owner, partner, director, volunteer, student, intern or contractor)

Yes No

2. Which of the following are included within the organisation's pre-employment background checks?

Only answer if Personnel and the environment Q1 = Yes

- Application or verification of BPSS (Baseline Personnel Security Standard)
- Qualification checks
- Employment history
- Verifying credentials
- None of the above

3. Does the organisation have a defined and implemented policy for applying the UK Baseline Personnel Security Standard (BPSS) and National Security Vetting (NSV) checks, as appropriate, for personnel supporting Functions and for the protection of Data?

Yes No

4. Does the organisation have a joiners, movers and leavers policy in place?

Yes No

5. Does the organisation have procedures for new joiners to ensure the following?

- Understanding of relevant organisational cyber security policies and procedures is measured
- Appropriate cyber security training is undertaken

- Access permissions are assigned based on roles and responsibilities
- None of the above

6. Does the organisation have procedures in place for staff moving roles or departments to ensure the following?

- Cyber security training for new responsibilities or systems is delivered
- Permissions and data are securely transferred
- Access permissions are reviewed
- None of the above

7. Does the organisation have procedures in place for staff leaving the organisation that promptly:

- Change authentication factors known to leavers, including shared credentials and physical door codes
- Recover issued physical assets including laptops, device tokens, keys and physical identification passes
- Revoke access to systems and data
- None of the above

8. Does the organisation conduct exit interviews or otherwise communicate data security responsibilities to departing personnel?

- Yes No

9. Does the organisation encourage staff to report suspicious activities or cyber security policy violations by:

- Providing training on the reporting processes to staff
- Providing processes for staff to report without fear of punishment
- None of the above

10. Does the organisation have a disciplinary process to investigate and take action when personnel are suspected of violating security policies or procedures?

Yes No

11. Does the organisation assess its need for environmental controls, including:

Backup power technologies

Temperature and humidity controls (e.g. within data centre environments)

Fire suppression systems

None of the above

12. Does the organisation implement, install and maintain the environmental controls it has assessed as appropriate?

Only answer if Personnel and the environment Q11 = NOT "None of the above"

Yes No

Security monitoring

1. Does the organisation monitor the security status of networks and systems that support Functions and protect Data?

Yes No

2. Does the organisation use security monitoring to detect potential security issues?

Only answer if Security monitoring Q1 = Yes

Yes No

3. Does the organisation use its security monitoring to track the effectiveness of protective security measures?

Only answer if Security monitoring Q1 = Yes

Yes No

4. Does the organisation have documented policies, procedures and controls in place for security event monitoring?

Yes No

5. Which of the following are included in the organisation's security event monitoring procedures?

- Escalation matrix
- Clearly defined roles and responsibilities
- Frequency of monitoring
- Security events covered
- None of the above

Only answer if Security monitoring Q4 = Yes

6. Does the organisation ensure security event monitoring is implemented in accordance with its established procedures?

Only answer if Security monitoring Q4 = Yes

Yes No

7. Does the organisation generate alerts for potential security events?

Only answer if Security monitoring Q4 = Yes

Yes No

8. Does the organisation have documented policies and procedures in place for the creation, retention and correlation of auditing logs?

Yes No

9. Does the organisation ensure that event logs are generated for all systems supporting the operation of Functions and the protection of Data?

Yes No

10. Does the organisation ensure that it captures logs for all key security event types, as defined by its policies?

Yes No

11. Does the organisation review the event types selected for logging at least every 6 months to ensure they meet business requirements?

Yes No

12. Does the organisation ensure that system event logs capture:

Network ports used

Devices accessed

User ID

Event date/time from Network Time Protocol (NTP) source

None of the above

13. Does the organisation ensure that logs are available on request for analysis?

Yes No

14. Does the organisation ensure system logs are reviewed at least weekly to identify failures, faults and potential security issues?

Yes No

15. Does the organisation ensure that logs are archived for at least 12 months?

Yes No

16. Does the organisation ensure that access to modify system logs is restricted to prevent tampering?

Yes No

17. Does the organisation store audit records in a separate physical system from the audited systems?

Yes No

18. Does the organisation monitor the operational status of logging/auditing systems and alert on any failures?

Yes No

19. Does the organisation have an effective audit reduction and report generation capability?

Yes No

20. Does this capability support the organisation's requirements for on-demand audit review, analysis and reporting?

Only answer if Security monitoring Q19 = Yes

Yes No

21. Does use of this capability preserve the original content and time-ordering of audit records?

Only answer if Security monitoring Q19 = Yes

Yes No

22. Does the organisation integrate audit record review, triage, analysis, and reporting with its governance and incident management structures?

Yes No

Proactive detection

1. Does the organisation have procedures in place to proactively identify malicious activities within its networks and systems, including those that evade signature-based prevention and detection solutions?

Yes No

2. Does the organisation define examples of abnormal system behaviour to aid in detecting malicious activity that is otherwise hard to identify?

Yes No

3. Does the organisation proactively search for known indicators of compromise across its systems and technologies to support detection efforts?

Yes No

4. Does the organisation monitor alerts and advisories from trusted sources to identify new indicators of compromise?

Yes No

5. Does the organisation use tools to detect unauthorised hardware, software, and firmware components in its systems?

Yes No

6. Does the organisation require action to be taken when unauthorised components are detected, including, where appropriate and proportionate:

Notifying systems administrators and/or security operations teams

Isolating such components

Disabling network access by such components

None of the above

Incident response

1. Does the organisation have clearly defined policies and processes in place for cyber security incident management?

Yes No

2. Has the organisation tested its cyber security incident management processes?

Only answer if Incident response Q1 = Yes

Yes No

3. Does the organisation have an incident handling capability that is robust and comprehensive enough to meet its incident management policy and incident response plans?

Yes No

4. Does the organisation's incident handling capability include:

Only answer if Incident response Q3 = Yes

- Reporting incidents to organisational officials and/or authorities
- Documenting incidents
- Tracking incidents
- Communication with users
- Recovery from incidents
- Containment of incidents
- Forensic analysis of incidents
- Detection of incidents
- Preparation for incidents
- None of the above

5. Does the organisation audit the identities of internal users linked to denied communications?

Yes No

Recovery and improvements

1. Does the organisation have procedures in place to conduct root cause analysis following incidents?

Yes No

2. Does the organisation implement lessons learned from incidents into updated incident response procedures, training and testing?

Yes No