MERCURY

YOUR VISION, OUR DUTY.

IT Security Questionnaire – Guidance for Suppliers

Table of Content

Why do I need to complete the IT Security Questionnaire?

The IT Security Questionnaire is mandatory for supplier onboarding and for being added to the SAP system.
It helps Mercury understand how your organisation protects information that may be shared with us.
Please make sure **all questions are answered** before submission to avoid delays.

How to Complete the Questionnaire

- Provide **clear, honest, and accurate answers**.
- If a question is technical or unclear, **do not guess**.
- Please **ask your IT team or IT service provider** to help you answer correctly.
- The questionnaire should ideally be completed or reviewed by **someone with IT or security knowledge**.

Important Points to Remember

- Some security controls (for example, **Multi-Factor Authentication**) are **basic minimum requirements**.
- If you currently do not have a required control in place, please **explain the reason and any plans to implement it**.
- Simple “Yes” or “No” answers should include **short explanations where requested**.
- Providing accurate information helps ensure **faster review and approval**.

What Happens After Submission

- The responses will be **reviewed by the Mercury Information Security team**.
- We may contact you if **additional information or clarification** is required.
- **Incomplete or unclear answers may delay supplier onboarding or approval**.

Detailed Explanation to Help You Understand and Complete the IT Security Questionnaire

2. Information Security Management System (ISMS)

What is an Information Security Management System (ISMS)?

An Information Security Management System (ISMS) is a set of policies, processes, and controls used to protect company and customer information.
It defines how your organisation manages information security risks and keeps information secure.

2.1 Do you have an established Information Security Management System (ISMS)?

What we are asking:
Do you have a formal or documented approach to managing information security risks within your organisation?

This may include (examples):

- Information Security or IT Security policies
- Access controls (who can access systems and data)
- Risk assessments or risk registers
- Incident or breach handling procedures
- Defined security roles and responsibilities

If **Yes**:

- Please specify the type of certification(s) held, if applicable
- Please upload the relevant certificate(s) (if available)

If **No**:

- Please provide additional information explaining your current approach to information security

2.2 Is your ISMS certified to an industry-recognised standard (e.g. ISO/IEC 27001, Security Essentials, or equivalent)?

What we are asking:
Has your ISMS been formally certified by an independent external organisation against a recognised security standard?

If **Yes**:

- Please specify which industry-recognised standard or framework your ISMS is certified or aligned to

If **No**:

- Please provide more information explaining why your ISMS is not aligned with an industry-recognised framework

2.4 Please specify the type of certification(s) held

What we are asking:

- please specify the certification(s) your organisation holds (e.g. ISO/IEC 27001, Cyber Essentials, Security Essentials) and provide the relevant details for section 2.5.

2.5 Security Certification (e.g. ISO/IEC 27001 Certificate)

What this section is about

This section collects basic details about your security certification so that it can be reviewed and validated.

Please provide the following details:

- **2.5.1 Issuer** – The organisation that issued the certificate
- **2.5.2 Audit Result** – Pass / Approved / Certified
- **2.5.3 Certificate Number** – As shown on the certificate
- **2.5.4 Effective Date** – The date the certificate became valid
- **2.5.5 Expiration Date** – The date the certificate expires
- **2.5.6 Attachment** – Upload a copy of the certificate

2.5.7 Do **you want to add another attachment?**
(Use this if you have additional certificates to upload.)

3. Business Continuity Plan (BCP)

What is a Business Continuity Plan (BCP)?

A Business Continuity Plan (BCP) explains how your organisation continues operating if something goes wrong, such as:

- An IT system outage
- A cyber security incident
- A major disruption or emergency

It typically includes backup arrangements, recovery steps, and key responsibilities.

3.1 Do you have a documented and tested Business Continuity Plan (BCP) that includes IT disaster recovery and cyber security incident response?

What we are asking:

Do you have a written and tested plan that explains how your organisation responds to and recovers from:

- IT system failures
- Cyber security incidents
- Loss of access to critical systems

The plan does not have to be complex, but it must be documented and reviewed or tested.

3.2 Do you test your BCP on an annual basis (at least)?

What we are asking:
Do you review or test your Business Continuity Plan at least once per year to ensure it remains effective?

Testing can include:

- Table-top exercises
- Simulations
- Plan reviews and updates

4. Multi-Factor Authentication (MFA)

Important:
Multi-Factor Authentication (MFA) for email and remote access is considered a basic and mandatory security control.

If MFA is not implemented:

- **Suppliers must provide a clear explanation**
- **Supplier onboarding approval may be rejected by the Information Security team until MFA is in place**
- **If MFA is not implemented, please explain why and outline any plans to implement it**

What is Multi-Factor Authentication (MFA)?
MFA adds an extra layer of protection by requiring more than just a password to sign in (for example, a phone code or authentication app approval).
This helps prevent unauthorised access, even if a password is compromised.

How to Set Up MFA / 2FA

Most email providers offer multi-factor authentication (MFA) at no additional cost:

Microsoft 365 / Outlook – Settings → Security → Two-step verification
Google / Gmail – Settings → Security → 2-Step Verification
Yahoo Mail – Settings → Account Security → Two-step verification

If you use a different email provider, please refer to their support documentation for instructions on enabling MFA or two-step verification.

4.1 Do you enforce Multi-Factor Authentication (MFA) for access to IT systems (e.g. Office 365, VPN, cloud software)?

What we are asking:
Do users need more than just a password to log in, especially for:

- Remote access
- Email systems
- Cloud services

5. Cyber Security Awareness

What is Cyber Security Awareness?
Cyber Security Awareness training helps employees recognise and avoid cyber threats, such as:

- Phishing emails
- Malicious links
- Data breaches

5.1 Do you have an active cyber security awareness training programme in place for employees with IT access?

What we are asking:
Do your employees receive regular security guidance or training on topics such as:

- Phishing emails
- Password security
- Safe internet and email use
- Reporting suspicious activity

Training can be online, in-person, or delivered through regular awareness communications.

For information security clarifications or technical queries: Infosec