



Introduction

Welcome to the Aviva Cyber Risk Assessment Questionnaire. The questions are designed to provide a view of the maturity and set-up of your IT and data security within your organisation. Your answers will assist our risk assessment and underwriting process in order to provide cyber insurance to you. Please ensure they are accurate, comprehensive and understandable, otherwise it could affect the extent of cover provided or invalidate your policy. We would suggest that someone within your organisation who is responsible for IT security should answer and sign the Questionnaire or support the person who is doing so and be a counter-signatory.

This cyber risk proposal form, based on the NIST Cybersecurity Framework 2.0 (CSF), is structured around the core functions of Govern, Identify Protect, Detect, Respond, and Recover to comprehensively assess and manage your cybersecurity risks. To find out more, please visit: <https://www.nist.gov/cyberframework>

The Questionnaire is not exhaustive and after evaluating your answers we might have additional questions.

Your Business

Business Name¹ Registered Company Number
(if applicable)

Business Activities

Do you require cover for any subsidiary or associated companies?²

Main Address including Post Code

Number of Employees Number of Employees with access to computer systems

Website(s) Year Established

Name and contact information of the person within your organisation responsible for IT security

¹ Enter the full legal entity of your business. Sole traders and unincorporated partnerships should enter personal names in full along with any trading name. Limited companies, limited partnerships and limited liability partnerships should include 'Limited', 'Ltd', 'LP' or 'LLP'.

² If outside the UK include the country of registration/incorporation. All information in this questionnaire should include these companies including revenue, number of employees and claims information.

Total revenue, including any subsidiary or associated companies to be covered

	Current Year	Estimated revenue for next year
Total revenue	£	£
Revenue generated in UK	£	£
Revenue generated in EEA	£	£
Revenue generated in USA/Canada	£	£
Revenue generated in Rest of the World	£	£

Percentage of revenue generated online such as e-commerce, web sales and e-service %

Do you currently have or have you ever had cyber insurance? Yes No

If **yes**, please complete the following table for each such insurance:

Expiry date	Premium	Deductible	Limits	Insurer	Retroactive Date

Previous losses or incidents

1. Have you had a personal data breach, other security breach or other cyber related incident (such as loss of money) in the last 3 years that has, would have or could have led to a claim or notification under any of these cyber covers had they been in place at the time?

Yes No

If yes, please provide details below:

2. If you answer yes, please provide details of any measures, including professional advice, that have been taken to prevent the recurrence of the situation which gave rise to each claim:

Not applicable

3. Have you ever had any cyber insurance declined, cancelled or withdrawn?

Yes No

If yes, please state the details:

Further Information

1. Govern & Identify (Tick all that apply)

1. What is your total annual IT Security Budget? £

2. Do you have a dedicated individual responsible for IT Security?

Yes No

3. Do you have the following cybersecurity policies in place?

Information Security Privacy Acceptable Use Data Classification
Data Retention & Destruction Access Control Change Management

4. Are you accredited to/Do you follow any of these standards?

Cyber Essentials Cyber Essentials Plus NIST CSF
ISO 27001 Other

5. Do you have an up to date inventory of all hardware and software?

Yes No

If yes, how frequently is this reviewed and updated?

6. Do you conduct an annual or more frequent cyber risk assessment?

Yes No

7. Do you conduct internal vulnerability scans?

Yes No

If yes, how frequently?

8. Do you conduct external/internal penetration tests?

Yes No

If yes, how frequently?

9. Do you actively gather threat intelligence relevant to your organisation?

Yes No

10. Do you use any End-of-Life Systems, if so how do you mitigate the risks?

Yes No

Isolated/Air-Gapped from critical systems Limited Access/Functionality Extended security updates
Disconnected from the internet Other

11. How many Personally Identifiable Information (PII) records does your organisation currently hold?

12. How many Sensitive Personally Identifiable Information (SPII) does your organisation currently hold?

13. Are you (or your service provider) compliant with the latest version of PCI-DSS? Yes No N/A

If yes, to what certificate level? Level 1 Level 2 Level 3 Level 4

14. List your main IT Service Providers including any MSSP

2. Protect (Tick all that apply)

1. How do you control access to your systems and resources?

Principle of Least Privilege Role Based Geographical Separate Admin/Privileged accounts

2. How often is the access reviewed?

Monthly Quarterly Annually Every 6 months Role Change/Staff Departure No review process

3. Are all default passwords changed for all systems immediately?

Yes No

Describe your password policy

4. Where do you require Multi-Factor Authentication?

Remote Access Email Access Administrator/Privileged Accounts None

5. How do you manage and secure remote access?

6. Where do you require the encryption of data?

At Rest In Transit On Portable Devices None

7. Do you provide annual Cybersecurity training to appropriate staff?

Yes No

8. Do you carry out phishing simulations? If so, how frequently?

Quarterly Every 6 months Annually Never Other

9. Do you maintain a secure baseline configuration for all systems?

Yes No

10. What is your policy for patching your systems based on the CVSS/Risk Rating?

High & Critical (CVSS 7+):

Low & Medium (CVSS 0-6.9):

11. How do you segregate your network to prevent lateral movement of malware or unauthorised access?

Geographical Business Unit Sensitivity BYOD IOT/Device Based Guest Wi-Fi No Segregation

How is this achieved?

VLAN Air-Gapping DMZ Firewall Rules Zero Trust Other

12. If you have Operational Technology/Manufacturing Systems, what security is in place?

VLAN Air-Gapping DMZ Manual Override Other

13. What do you use to help protect against Email based threats (Phishing/SPAM)?

14. Have you implemented the following security tools:

Next Generation Firewall Perimeter Firewalls Web application Firewall DLP Anti-Virus/Anti-Malware SPF
DKIM DMARC External tagging USB blocking Disabled Macros

15. Do you use two step verification before any change is made to a third party's account details? Yes No

16. Do you use two step verification before transferring funds into any new account? Yes No

17. Do you have a formal policy in place for staff to refer to in the payment processing team? Yes No

3. Detect (Tick all that apply)

1. What tools do you utilise to aid in the detection of malicious/suspicious activity on your network:

Tool	Yes	No	Vendor
Intrusion Detection System (IDS)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>
Intrusion Prevention System (IPS)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>
Endpoint Detection and Response (EDR)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>
Managed Detection and Response (MDR)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>
Security information and Event management (SIEM)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>

2. Do you utilise a Security Operations Centre?

24/7 Working Hours Only No Internal Outsourced - Vendor

4. Respond (Tick all that apply)

1. Do you have a written Cyber Focused:

Disaster Recovery Plan? Yes - Tested Annually Yes - Untested No

Business Continuity Plan? Yes - Tested Annually Yes - Untested No

Incident Response Plan? Yes - Tested Annually Yes - Untested No

Communication Plan in the event of a cyber incident? Yes - Tested Annually Yes - Untested No

Playbooks for cybersecurity incidents e.g Ransomware? Yes - Tested Annually Yes - Untested No

2. Do you include your Outsourced Service Providers in your response plans? Yes No

5. Recover (Tick all that apply)

1. How often do you take Backups of all mission critical systems, databases & applications?

Continuously Daily Weekly Bi-Weekly Monthly Other

2. How are your backups secured/stored?

Cloud Service Provider Offsite Offline Air-Gapped Storage Physical Copy Replicated at secondary Data centre

Encrypted Immutable Tested on annual basis Protected by MFA Access Controls Other

3. What is your failover capability?

Hot Site Warm Site Cold Site Uninterruptable Power Supply

Backup Generators Increased Bandwidth Alternative Suppliers Other

4. What is your recovery time objective?

8 Hours 12 Hours 24 Hours 48 Hours Other

How and why we use your information

We (Aviva), and our third parties, collect and use information (including data about health and unspent offences or criminal convictions) about you and, if relevant, somebody else covered under your policy and your vehicle(s), business and property.

We do this so we can:

- verify your identity and help prevent fraud
- calculate our risk to insure you
- calculate your price
- set up, assess and maintain your insurance contract with us
- renew and make changes to your cover
- process claims
- carry out marketing, profiling and analytics.

We share information within the Aviva Group, our reinsurers (our own insurers) and specific other organisations for these purposes.

The information comes from:

- what you've already told us
- data we already hold about you (including from other quotes and policies with us)
- publicly available sources
- other organisations we trust
- data about your device, general location and how you interact with our website.

We carry out a quotation search from a credit reference agency

This will appear on your credit report and will be visible to other credit providers. It will be clear it's a quotation and not a credit application by you. We do this when you ask us for a quote, when we prepare your renewal and sometimes if you change your cover so that we are able to offer you a monthly credit payment option. We use data from our credit reference agency to verify your identity, prevent fraud and carry out risk profiling which allows us to calculate your premium and payment options. For more information about your rights relating to profiling and decisions that are automatically processed such as pricing, see the Privacy Notice for this policy.

The identity of our credit reference agency and the ways they use and share personal information are explained in more detail at www.transunion.co.uk/crain. You can also check the information they hold about you.

We use automated processes to make decisions

This means our software decides whether we can insure you and on what terms, deal with claims and carry out fraud checks. For more information, see the Privacy Notice for this policy.

You have rights about your information

For more about your rights and how and why we use your data, see the Privacy Notice for this policy. There's more detail in our Privacy Policy at www.aviva.co.uk/privacypolicy or you can request a copy by writing to us at Aviva, Freepost, Mailing Exclusion Team, Unit 5, Wanlip Road Ind Est, Syston, Leicester, LE7 1PD.

Data Protection – Privacy Notice

Aviva Insurance Limited is the main company responsible for your Personal Information (known as the controller).

We collect and use Personal Information about you in relation to our products and services. Personal Information means any information relating to you or another living individual who is identifiable by us. The type of Personal Information we collect and use will depend on our relationship with you and may include more general information (e.g. your name, date of birth, contact details) or more sensitive information (e.g. details of your health or criminal convictions).

Some of the Personal Information we use may be provided to us by a third party. This may include information already held about you within the Aviva group, information we obtain from publicly available records, third parties and from industry databases, including fraud prevention agencies and databases.

This notice explains the most important aspects of how we use your Personal Information, but you can get more information by viewing our full privacy policy at aviva.co.uk/privacypolicy or requesting a copy by writing to us at: The Data Protection Team, Aviva, PO Box 7684, Pitheavlis, Perth PH2 1JR. If you are providing Personal Information about another person you should show them this notice.

We use your Personal Information for a number of purposes including providing our products and services and for fraud prevention.

We also use profiling and other data analysis to understand our customers better, e.g. what kind of content or products would be of most interest, and to predict the likelihood of certain events arising, e.g. to assess insurance risk or the likelihood of fraud.

We may carry out automated decision making to decide on what terms we can provide products and services, deal with claims and carry out fraud checks. More information about this, including your right to request that certain automated decisions we make have human involvement, can be found in the "Automated Decision Making" section of our full privacy policy.

We may process information from a credit reference agency, including a quotation search where you are offered an Aviva credit payment facility. More information about this can be found in the "Credit Reference Agencies" section of our full privacy policy.

We may use Personal Information we hold about you across the Aviva group for marketing purposes, including sending marketing communications in accordance with your preferences. If you wish to amend your marketing preferences please contact us at: contactus@aviva.com or by writing to us at: Aviva, Freepost, Mailing Exclusion Team, Unit 5, Wanlip Road Ind Est, Syston, Leicester, LE7 1PD. More information about this can be found in the "Marketing" section of our full privacy policy.

Your Personal Information may be shared with other Aviva group companies and third parties (including our suppliers such as those who provide claims services and regulatory and law enforcement bodies). We may transfer your Personal Information to countries outside of the UK but will always ensure appropriate safeguards are in place when doing so.

You have certain data rights in relation to your Personal Information, including a right to access Personal Information, a right to correct inaccurate Personal Information and a right to erase or suspend our use of your Personal Information. These rights may also include a right to transfer your Personal Information to another organisation, a right to object to our use of your Personal Information, a right to withdraw consent and a right to complain to the data protection regulator.

These rights may only apply in certain circumstances and are subject to certain exemptions. You can find out more about these rights in the "Data Rights" section of our full privacy policy or by contacting us at dataprt@aviva.com

Fraud prevention and detection

In order to prevent and detect fraud we may at any time:

- Share information about you with other organisations and public bodies including the Police;
- Undertake credit searches and additional fraud searches;
- Check and/or file your details with fraud prevention agencies and databases, and if you give us false or inaccurate information and we suspect fraud, we will record this.

We and other organisations may also search these agencies and databases to:

- Help make decisions about the provision and administration of insurance, credit and related services for you and members of your household;
- Trace debtors or beneficiaries, recover debt, prevent fraud and to manage your accounts or insurance policies;
- Check your identity to prevent money laundering, unless you provide us with other satisfactory proof of identity;
- Check details of job applicants and employees.

Claims history

- Under the conditions of your policy you must tell us about any insurance related incidents (such as fire, water damage, theft or an accident) whether or not they give rise to a claim. When you tell us about an incident we will pass information relating to it to a database.
- We may search these databases when you apply for insurance, in the event of any incident or claim, or at time of renewal to validate your claims history or that of any other person or property likely to be involved in the policy or claim.

We can supply on request further details of the databases we access or contribute to. If you require further details please contact us.
Tel: 0800 051 4473

Calls to 0800 numbers from UK landlines and mobiles are free. For our joint protection telephone calls may be recorded and/or monitored.

You should show these notices to anyone who has an interest in the insurance under the policy.

Choice of Law

The appropriate law as set out below will apply unless you and the insurer agree otherwise:

- The law applying in that part of the UK, the Channel Islands or the Isle of Man in which you normally live or (if applicable) the first named policyholder normally lives, or
- In the case of a business, the law applying in that part of the UK, the Channel Islands or the Isle of Man where it has its principal place of business, or
- Should neither of the above be applicable, the law of England and Wales will apply

How do I make a complaint?

If for any reason you are unhappy with the product or service, please get in touch as soon as possible. For contact details and more information about the complaints procedure please refer to your policy documents. Where a complaint cannot be resolved to your satisfaction you may be able to ask the Financial Ombudsman Service (FOS) to carry out an independent review. Whilst firms are bound by their decision you are not. Contacting them will not affect your legal rights. You can contact the FOS on **0800 023 4567** or visit their website at **www.financial-ombudsman.org.uk**, where you will find further information.

| Retirement | Investments | Insurance | Health |

Risks situated within the UK and other countries excluding the EEA are underwritten by Aviva Insurance Limited. Registered in Scotland, No. SC002116. Registered Office: Pitheavlis, Perth PH2 0NH. Authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority. Firm Reference Number 202153.

Risks situated within the EEA are underwritten by Aviva Insurance Ireland Designated Activity Company. Aviva Insurance Ireland Designated Activity Company, trading as Aviva, is regulated by the Central Bank of Ireland. Our firm's reference number is No. C171485. A private company limited by shares. Registered in Ireland, No. 605769. Registered Office: Cherrywood Business Park, Dublin, Ireland D18 W2P5. Registered UK Branch Address: 80 Fenchurch Street, London, EC3M 4AE. UK Branch authorised by the Prudential Regulation Authority. Subject to regulation by the Financial Conduct Authority (FCA reference No. 827591) and limited regulation by the Prudential Regulation Authority. Details about the extent of our regulation by the Prudential Regulation Authority are available from us on request.

