# Aviva Cyber
## Risk assessment questionnaire

## 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.

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

## Your Business

| | |
|---|---|
| *Business Name*[1]*:* | |
| *Registered Company number if applicable* | |
| *Main Address including Post Code* | |
| • *Number of employees*<br>• *Number of employees with access to computer systems* | |
| *Year Established* | |
| *Website (s)* | |
| *Please provide the name and contact information of the person within your organisation responsible for IT security.* | |

[1] Please 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'.

**Do you require cover for any subsidiary or associated companies?** Yes ☐ No ☐

If **yes** provide details of the subsidiary and associated companies below, and if outside the UK the country of registration/incorporation.

.....

.....

**All information in this questionnaire should include these companies including revenue, number of employees and claims information**

**Please provide a full description of the business activities including any subsidiary or associated companies to be covered.**

.....

.....

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

| | Last year | 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 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:

.....

.....

## Coverage required

**When do you require cover to start?** D D M M Y Y Y Y

Please select the cover and limit you require:

£100,000 ☐ £250,000 ☐ £500,000 ☐ £1,000,000 ☐ £2,000,000 ☐

£5,000,000 ☐ Other ☐

Cyber Cover includes the following as standard

- Data Security Breach Cover
- Virus, Hacking and Denial of Service Attack Cover
- Extortion Cover
- Business Interruption Cover
- Network Security Liability
- Data Privacy and Confidentiality Liability
- Payment Card Industry Liability
- Multimedia Liability

Excess Period 8 hours ☐ 12 hours ☐ 24 hours ☐ Other

**External Cyber Crime and Telecommunication Services** Yes ☐ No ☐

£50,000 ☐ £100,000 ☐ £250,000 ☐

**Policy Deductible**

£2,500 ☐ £5,000 ☐ £7,500 ☐ £10,000 ☐ £25,000 ☐ Other

# Further Information

## Identify

**1. What is your total annual IT security budget?**

**2. Do you have a dedicated individual responsible for IT security?** Yes ☐ No ☐

**3. Are you accredited to any of these standards?**

Cyber Essentials ☐ Cyber Essentials Plus ☐ NIST Frameworks ☐

ISO27001 ☐ Other

**4. Are you compliant with the most recent applicable payment card industry data security standard (PCS-DSS)?** Yes ☐ No ☐ N/A ☐

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

**5. Do you have an up to date inventory of all hardware and software?** Yes ☐ No ☐

**6. Do you complete an annual Cyber risk assessment?** Yes ☐ No ☐

**7. Do you complete penetration testing?** Yes ☐ No ☐

If **yes**, how frequently?

**Do you complete internal vulnerability scans?** Yes ☐ No ☐

If **yes**, how frequently?

**8. How many servers do you have?**

**9. Do you gather advanced threat intelligence?** Yes ☐ No ☐

**10. Do you use end of life software?** Yes ☐ No ☐

**software that is unsupported by the manufacturer*

If **yes**, how is this protected? (select all that apply)

Air-gapping ☐ Limited Access ☐ Ongoing maintenance agreement ☐ Other

**11. How many PII records are held or processed annually?**

**personal identifiable information*

Up to 50,000 ☐ Between 50,001-100,000 ☐ Between 100,001-500,000 ☐ Between 500,001-1,000,000 ☐

Between 1,000,001-5,000,000 ☐ Between 5,000,001-20,000,000 ☐ Over 20,000,000 please specify

**12. How many sensitive records are held or processed annually?**

**sensitive records are special category data under data protection legislation, such as personal health information*

Up to 50,000 ☐ Between 50,001-100,000 ☐ Between 100,001-500,000 ☐ Between 500,001-1,000,000 ☐

Between 1,000,001-5,000,000 ☐ Between 5,000,001-20,000,000 ☐ Over 20,000,000 please specify ☐

**13. Please list your main IT service providers:**

**E.g. Microsoft Azure, Amazon webservices etc*

## Protect

**1. How do you control access to systems and information? (select all that apply)**

Role based/Least privileged ☐ Business unit ☐ Geographically ☐ None ☐ Other ☐

**2. How often do you review user access?**

Quarterly ☐ Every 6 months ☐ Annually ☐ Never ☐ Other ☐

**3. How often do you carry out phishing tests?**

Quarterly ☐ Every 6 months ☐ Annually ☐ Never ☐ Other ☐

**4. Do you provide annual training to appropriate staff on cyber risks?** Yes ☐ No ☐

**5. Where do you utilise Multifactor Authentication (MFA)? (select all that apply)**

All remote access ☐ Email access ☐ Admin access ☐ Backups ☐ None ☐

**6. When do you encrypt data? (select all that apply)**

In transit ☐ At rest ☐ On portable devices ☐ Backups ☐ None ☐

**7. What is your patching process for standard patches and High or Critical vulnerabilities (CVSS 7 and above)?**

**8. How do you segregate your network? (select all that apply)**

Logically ☐ Geographically ☐ Business unit ☐ Sensitivity ☐ No segregation ☐

**9. How are any automated manufacturing systems protected? (select all that apply)**

Air-gapping ☐ Manual override ☐ Whitelisting ☐ Other ☐

**10. Do you use two-step verification before any change is made to a third party's payment account details?** Yes ☐ No ☐

**two step verification is obtaining secondary authorisation via an authentication method which is different to the original method used to request the change or transfer*

**Do you use two-step verification before transferring funds into an account that you have not paid before?** Yes ☐ No ☐

**11. Are default passwords for all your systems changed immediately after purchase or development?** Yes ☐ No ☐

**Are your administrative passwords separate from your user account passwords?** Yes ☐ No ☐

**12. Do you have a strong password policy across your business e.g. long and complex passwords** Yes ☐ No ☐

**13. Do you use anti-virus, anti-spyware or similar malware protection software, which are automatically updated and manually updated when necessary?** Yes ☐ No ☐

**14. Do you use perimeter firewalls to protect your network and computer systems?** Yes ☐ No ☐

## Detect

1. **Do you use Intruder Detection/Prevention Systems?** Yes ☐ No ☐
2. **Do you use Endpoint Detection and Response?** Yes ☐ No ☐
3. **Do you have Security Incidents and Events Management (SIEM) in place?** Yes ☐ No ☐
4. **Do you use a Security Operations Centre?** Yes - Working hours only ☐ Yes - 24/7 ☐ No ☐
5. **Do you apply secure baselining and conduct ongoing checks of network activity?** Yes ☐ No ☐

## Respond

1. **Do you have a written Disaster Recovery Plan?** Yes - Untested ☐ Yes-Tested Annually ☐ Yes-Tested (Other) ☐ No ☐
2. **Do you have a written Security Response Plan?** Yes - Untested ☐ Yes-Tested Annually ☐ Yes-Tested (Other) ☐ No ☐
3. **Do you have a written Incident Response Plan?** Yes - Untested ☐ Yes-Tested Annually ☐ Yes-Tested (Other) ☐ No ☐
4. **Do you have a written specified communication plan in the event of an outage?** Yes - Untested ☐ Yes-Tested Annually ☐ Yes-Tested (Other) ☐ No ☐

## Recover

1. **How regularly do you take system backups?**

   Daily ☐ Weekly ☐ Monthly ☐ Other ☐

2. **How are your backups managed? (select all that apply)**

   Offline/Onsite ☐ Immutable ☐ Protected by MFA ☐ Tested ☐

3. **What is your failover capability? (select all that apply)**

   **The ability to switch to a reliable backup system*

   Hot site ☐ Warm site ☐ Cold site ☐ Bandwidth Increase ☐ Other ☐

4. **What is your Recovery Time Objective?**

   **The maximum length of time it should take to restore normal operations following an incident*

   Below 4 hours ☐ Between 4 and 8 hours ☐ Between 8 and 12 hours ☐ Between 12 and 24 hours ☐ More than 24 hours ☐

# Declaration

I/We declare that the information given is correct and complete, to the best of my/our knowledge and belief. If the risk is accepted I/We undertake to pay the premium when called upon to do so. I/We understand that my/our information may also be disclosed to regulatory bodies for the purposes of monitoring and/or enforcing the insurer's compliance with any regulatory rules/codes.

Signature: ..... Name: .....

Date: ..... Position: .....

E-mail: .....

## 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.

### 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.

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

| Retirement | Investments | Insurance | Health |



BCOCR14999 03.2024

AVIVA