Aviva Cyber Insurance (including Cyber Complete)
Target Market Statement

This document has been prepared by Aviva UK General Insurance to provide an overview of our Commercial Lines Cyber Insurance product. It is intended to help distributors understand the target market for this product, at new business and at point of renewal. In addition, distributors should consider whether any changes in circumstances may result in some features of the product no longer being suitable (for example distribution channel, features/covers, communication method and payment method).

Aviva Insurance Limited will overlay some eligibility and risk acceptance criteria which will be applied and shown through the quote process. This will result in some customers for whom the product is suitable not being eligible due to our current risk appetite.

Aviva Insurance Limited is the Product Manufacturer for this product and may source elements of cover from third parties. Full details are contained within the policy documentation.

Eligibility Criteria?

- Is available for customers with turnovers up to £500m.

Who is Aviva Cyber Insurance (including Cyber Complete) suitable for?

- Aviva's Cyber Insurance product is designed for customers who require insurance protection against the financial impact of cyber risks, such as hacker attacks, ransomware, social engineering fraud, denial of service attacks, reputational damage or compensation claims made against the business for failing to keep personal or commercial data secure.
- This product is designed for businesses, large and small, that depend on their digital technology to operate or have an online presence or store and handle sensitive user and customer data.

Who is this product not suitable for?

- Customers that do not:
  - use a computer or mobile device for their day-to-day work; or
  - store private or sensitive data such as employee, customer or payment card information on a network or cloud.
- Customers involved in E-service providers, E-commerce risks, Financial Institutions, Software Developers, Media, Health and Social Care, Call Centres and Utility Companies.
- Customers who are not involved in running a commercial business.
- This product is not suitable for consumers as defined by the FCA. A consumer is classed as any person who is acting for purposes which are outside their trade or profession.
- Customers that require short term non-renewable cover.
- Customers who cannot afford the annual or monthly premiums.

How can Aviva Cyber Insurance be sold?

- Aviva's Cyber Insurance product is suitable to be sold face to face, via telephone or digitally.
- This product can be sold with or without advice depending on your preference and in line with FCA regulations.

What features should you be aware of when considering this product?

- We recognise that some individuals have additional support needs, such as alternative formatted documents, when purchasing or understanding our products. Aviva Insurance Limited is committed to helping meet these needs. If additional support is required, please contact us to discuss how we can assist the customer.
- Sales journeys must identify customer eligibility and ensure that key information and choices to be made are presented to customers in a way that supports a customer through the process of understanding core cover and configuring optional elements of insurance to suit their specific demands and needs.

- Whilst there is a degree of complexity driven by the need to select appropriate optional additional covers and tailor configurable elements of insurance, each element, limit or choice is sufficiently simple for customers to understand without advice as the underwriting method frees customers to engage with their cover selection. This alongside the annual renewal process, enables familiarity in order to support their decision making.
- Having a comprehensive cyber-insurance policy not only provides financial protection if the worst happens, but also provides access to expert advice and support when an incident occurs, such as, IT, legal, forensic and media relations to minimise the disruption to the business and any reputational damage.
- To make sure the Cyber insurance policy operates fully a certain level of IT security and controls must be in place e.g. data must be backed-up on a frequent basis, up-to-date anti-virus software must be in place and critical software updates must be carried out within prescribed timescales.
- The Cyber insurance product gives access to our Cyber incident response team which provides immediate support 24/7, coordinating all the specialist support required to:
  - identify, contain and repair a breach and restore data.
  - provide legal and PR consultancy to help safeguard the customer's reputation.
  - notify those individuals affected by a breach and co-ordinate credit or identity theft monitoring for those affected.
  - provide consultancy to prepare for any regulatory notification.
- This product does not cover things such as:
  - Losses deliberately carried out by an employee or if they work in collusion with a third party.
  - Failure of infrastructure including the internet, utilities, telecommunications, domain name service, certificate authority or content delivery network.
  - Errors or omissions in any professional advice or services.
  - Infringement of patents or misappropriation of trade secrets, or licence fee or royalties in respect of intellectual property.
- Customers who pay their premiums monthly are more than likely to pay a higher premium than those who pay their premium annually, therefore consideration needs to be given regarding affordability.

Optional additional covers/Extensions which are available with this product:

Ways to enhance cover - These options come at an additional cost and can be added to core cover to provide more comprehensive benefits			
Product cover option	**This product is designed to provide financial protection if**	**Who could this option be suitable for?**	**Who is this product not designed to support, or are there any features that you should be aware of when offering this product to your customers?**
External Cyber Crime	• A financial loss has been incurred due to unauthorised access to the customer's IT network or if a third party deceives an employee into paying or transferring money by impersonating another person.	• Customers requiring cover for potential financial losses incurred due to unauthorised access to their computer systems or if a third party deceives an employee into paying or transferring money by impersonating another person.	To ensure these cover extensions operate fully, customers must: • be trained in the dangers of social engineering fraud and how to spot these attempts and they must keep a record of such training. • have a documented policy in place, which states that details of any new payee requests or amended payment instructions are always checked verbally by using details held on file or a published website and do not solely rely on the new instruction. This policy must be accepted by all Partners, directors and Employees, with such acceptance recorded.

Optional additional covers/Extensions which are available with this product continued:

Ways to enhance cover - These options come at an additional cost and can be added to core cover to provide more comprehensive benefits			
Product cover option	**This product is designed to provide financial protection if**	**Who could this option be suitable for?**	**Who is this product not designed to support, or are there any features that you should be aware of when offering this product to your customers?**
Telecommunication Services (Optional cover for Digital customers only. Included as standard for SME/Mid-Market customers)	• Costs of unauthorised telephone calls and charges, made by an external hacker, have been incurred.	• Customers requiring cover for potential costs associated with unauthorised telephone calls and charges made by an external hacker.	To ensure these cover extensions operate fully, customers must: • be trained in the dangers of social engineering fraud and how to spot these attempts and you must keep a record of such training. • have a documented policy in place, which states that details of any new payee requests or amended payment instructions are always checked verbally by using details held on file or a published website and do not solely rely on the new instruction. This policy must be accepted by all Partners, directors and Employees, with such acceptance recorded.
Extortion (Optional cover for Digital customers only. Included as standard for SME/Mid-Market customers)	• Payments have been made in respect of ransom payments if a hacker holds the customer's business to ransom or threatens to reveal sensitive data until a ransom is paid.	• Customers wanting protection for any payments made for random payments if a hacker holds the customer's business to ransom or threatens to reveal sensitive data until a ransom is paid.	• We will only reimburse ransom payments where we determine that it is legally permissible to do so. To ensure these cover extensions operate fully, customers must: • On receiving a cyber extortion demand you must immediately notify and comply with the requirements of our Claims Service Provider. They will also need to report the crime to Action Fraud, the UK's national fraud cyber crime reporting centre.
Multimedia Liability (Optional cover for Digital customers only. Included as standard for SME/Mid-Market customers)	• Costs are incurred as a result of the customer mistakenly infringing the copyright or trademark of a third party due to the customer's use of online media.	• Customers requiring cover for potential costs incurred if the customer mistakenly infringes the copyright or trademark of a third party due to the customer's use of on line media.	• Cover for defamatory comments made on line. This could be in an email or social media.

| Retirement | Investments | Insurance | Health |

BCOAG16946 06.2024