

# QBE EO Product Oversight & Governance Information Exchange

The following information has been prepared to meet the FCA's Product Oversight and Governance rules, as set out in the PROD Sourcebook. These require all insurance product manufacturers to share certain information with Distributors following a Product Review and Fair Value Assessment, to ensure the product is sold to the identified Target Market and therefore meets the needs of that intended target market.

This document is intended to support distributors in understanding the key characteristics, target market, and distribution strategy of the product. It should be used to ensure alignment with the intended customer profile and to identify any potential gaps with the customer requirements.

Please note that we have grouped similar products together where this does not detrimentally affect our ability to review each product appropriately. Similar products are those that are intended to deliver similar cover and outcomes for customers, where the target markets are consistent.

If you have any questions in relation to the content of this product review, please direct these to your relevant underwriting contact at QBE.

<b>CARRIER NAME</b>	QBE UK Ltd, QBE Europe SA/NV, QBE Underwriting Ltd (Syndicates 386 & 1886), Lloyd's Insurance Company (LIC)
<b>PRODUCT NAME</b>	Cyber: Pen Cyber Insurance Policy
<b>NAME OF ANY CO-MANUFACTURERS</b>	None
<b>DETAILS OF PRODUCT DEVELOPMENT AND REVIEW PROCESS</b>	<p>Our Product Governance Framework is set out in the QBE EO Insurance Product Development and Review Policy which is approved by the QBE EO Board.</p> <p>The Insurance Product Development Guidelines detail the standards for the development and ongoing management of EO products, including how we consider and approve new products and any significant adaptation or change to the distribution strategy of an existing product. Our process requires the completion of various forms by the proposer of the product development, with oversight of the Product Leader, covering the business case and opportunity assessment through to pre and post launch responsibilities.</p> <p>The Product Oversight Group (POG), co-chaired by the Head of Product Leaders and the Head of Governance, Sustainability and Standards is responsible for providing oversight of and adherence to the Product Governance Framework. The POG oversees, manages and either approves or recommends for approval (to the Divisional CUO and MD) all Product Development and the current and ongoing annual product reviews (where applicable). Either of the POG Co-Chairs will make the final decision whether the proposed product development falls within the scope of the Policy and Guidelines.</p> <p>There is additional oversight from our Compliance team for products which trigger one or both of the following:</p> <ul style="list-style-type: none"> <li>- Products assessed as High Product Risk (HPR) – i.e. rated as high risk for conduct risk; and/or</li> <li>- Products intended to be transacted on a direct basis with no intermediary involvement, or via an aggregator site.</li> </ul>

	<p>For these cases, an additional HPR Questionnaire (HPRQ) is completed which is presented to the QBE EO Conduct Risk Group for customer challenge. The HPRQ includes additional consideration of target market, distribution strategy, product testing and post-sales barriers.</p> <p>The proposer of the development must conduct appropriate testing before a product is brought to the market. The Business Case and Opportunity Assessment contains questions which help demonstrate our product testing considerations when developing the product. The purpose of product testing is to assess whether the product will meet the needs, objectives and characteristics of the identified target market. It is important for identifying any potential drawbacks, understanding the future use of the product, testing the communication with and distribution to consumers and putting the customer at the heart of the product design.</p>
<b>PRODUCT INFORMATION</b>	<p>Cyber Response - first party incident response costs (legal, IT forensics &amp; PR costs),</p> <p>Business interruption losses</p> <p>Third party liability arising from a cyber incident</p> <p>Financial support, technical and strategic advice and guidance through the consequences of a cyber security breach</p> <p>As part of the QCyberProtect wording launch, cover was expanded over the course of 2024 to provide up to £250,000 of social engineering losses.</p> <p>Cyber physical damage cover will be offered in 2026.</p> <p>There have not been any material changes to assumptions that underpin the pricing, however we have adjusted our approach for sub-£250m UK business to now provide cover on an any on claim basis rather than a single aggregate limit.</p>
<b>TARGET MARKET</b>	<p>We consider companies in all market segments, including SME, and all industry sectors, with the exception of government owned entities (public administration), government education, government healthcare and crypto risks. Target industries include professional services and construction firms. Our target customers are those clients who can demonstrate minimum cyber security controls regardless of industry.</p> <p>No changes to our target market within last 12 months.</p> <p>Additional covers or extensions to coverage and any amendments may be negotiated on a case by case basis with the Insured's broker in the normal course of underwriting. Products can be reviewed and tailored to individual clients needs as determined and negotiated by the Client via their Broker.</p>
<b>TYPE OF CUSTOMER FOR WHOM THE PRODUCT WOULD BE UNSUITABLE</b>	<p>QBE's cyber product is not designed for individuals/personal cyber security.</p> <p>The business is placed by specialist cyber brokers, although this is not always the case with SME business. Where risks are not written on a QBE based form, the Brokers will provide a specific wording which are subject to independent review by clients and their insurance brokers and then proposed by and on behalf of a client.</p>

<b>ANY NOTABLE EXCLUSIONS OR CIRCUMSTANCES WHERE THE PRODUCT WILL NOT RESPOND</b>	<p>QBE's cyber product is not designed for individuals/personal cyber security.</p> <p>No notable changes to the exclusions over last 12 months. Standard market exclusions for the products apply.</p> <p>QBE policy wording is written in line with UK law. Notice of change documents are provided with each version of our base wording, where requested.</p>
<b>OTHER INFORMATION WHICH MAY BE RELEVANT TO DISTRIBUTORS</b>	We regularly meet with brokers to explain our appetite and target market.
<b>DATE FAIR VALUE ASSESSMENT COMPLETED</b>	January 2026
<b>EXPECTED DATE OF NEXT REVIEW</b>	January 2027

## Fair Value Assessment

<b>RAG</b>	<b>Requirement</b>	<b>Rationale</b>
	<b>Target Market</b> - the product is fit for purpose and remains consistent with the needs, characteristics and objectives of the identified target market	To ensure the product is fit for purpose we take into consideration the demands and needs of clients as well as account specific requests arising out of day-to-day negotiations. All products are reviewed as a Business-as-Usual approach underwriting process against available market coverage and assessed relative to alignment with customer needs in conjunction with the customers' brokers.
	<b>Fair Value</b> - the product provides fair value for customers, when considering the relationship between the overall price and the quality of the product(s) and/or services provided	This is an evolving product and as a result we consider and review losses experienced against the price charged to provide consistency and fair value to the client. Wordings are reviewed, driven by changes within the market, to ensure they provide appropriate cover for the risks the insureds face. Fair value is evidenced by low complaints in the last 12 months, strong renewal retention and high claims settlement statistics.
	<b>Distribution strategy</b> - the distribution strategy remains appropriate and distribution arrangements do not have any detrimental impact on value for customers	<p>All distribution is through brokers, remuneration is through brokerage which is detailed on the slip and/or quote documentation and which is reviewed at each renewal.</p> <p>There is regular review of the broker panel and all brokers have a TOBA in place with QBE to satisfy their appropriateness.</p>

<p><b>Customer Understanding</b> - the information provided to the customer enables them to make informed decisions</p>	<p>Distribution is on an intermediated basis and therefore the Broker or cover holder is responsible for advising and explaining the terms provided and the appropriateness of these for the insureds individual circumstances. Most brokers will provide a comparison of the terms offered in order to help insureds understand the differences. From time to time the Broker may specifically request QBE provide input on our terms / coverage.</p>
<p><b>Customer Support</b> - support provided to the customer allows them to fully utilise the product they purchase, e.g. make a claim, complain, cancel or amend cover</p>	<p>Customers can contact QBE in many different ways, via the broker or directly via dedicated Cyber Underwriters and Claims Adjusters who can provide expertise and assistance when needed. The intermediary will assist the customer in respect of making complaint, cancelling or amending cover. In Cyber, claims are normally made directly through our 24/7 breach response hotline, provided by law firms who adhere to SLAs in terms of answering the calls. Brokers may assist also with making a claim. Documentation to clearly explain what to expect from the claims process and how it can be accessed is available.</p>