



AIG SMART UNDERWRITING APPLICATION - BROKER GUIDANCE

AIG's new smart Cyber and E&O Insurance application provides you and your clients a more tailored experience, with questions applicable only to our underwriting of the risk. In addition, Cyber applicants will have greater transparency into how we underwrite their risk and will gain a better understanding of their cyber maturity through our accompanying reports. The following are tips and guidance for you when completing the application with your clients:

Our Cyber Underwriting Application infographic is a helpful resource for risk managers completing the application.

BEFORE SENDING THE APPLICATION TO THE RISK MANAGER



1. Explain the value in completing the full application

Tailored questions: Both Cyber and E&O applicants benefit from a tailored experience, with only questions pertaining to the client, its specific risks, and the coverages sought. For instance, a client applying for E&O coverage will not see cyber-related questions.

Transparency: Cyber applicants get a clearer view of how we underwrite their risk. They may even see direct impacts on policy terms if there's ongoing improvement year over year.

Better understanding of cyber risk: Cyber applicants can better understand how we view their cyber maturity, see their areas of strength and weakness, and receive recommendations for improvement.

While not all questions asked will be required, by answering all questions AIG can better evaluate the client's cyber risk and provide a more accurate quote.

Cyber applicants who complete the full application will receive (with opt-in) a Summarized Assessment Report (or SAR) based on their application responses, which includes their score summary, baseline risk trending, top risk scenarios, risk reducing controls, and more. Not only does this help the client better understand their cyber maturity, but they can also better understand how AIG views them as a cyber risk.

If the client binds coverage, they can receive our Executive Summary Report (or ESR), which contains greater detail than the SAR on their cyber maturity, as well as guidance on reducing their risk. The SAR and ESRs can be accessed from the AIG Cyber Portal once the underwriter has shared them. More information on this can be found in the "After Submitting the Application" section that follows.

Note: in order for a client to access their SAR and ESRs, they need to provide an email address where noted in the application for access to the AIG Cyber Portal. This can be the email address of the risk manager, CISO, or other party. Their email address will only be used for enrollment in the Portal. It will not be shared for marketing purposes.

Should the client not want to answer all questions, AIG may be able to make assumptions on some threat, impact and control questions. Despite the benefits of completing the full application, including receiving terms that match the risk more closely, clients can still receive a quote based upon answers to only the minimum required questions (those questions marked with a red asterisk).

Note: clients who do not complete at least the minimum required questions in the smart application are not eligible to receive the benefits associated with the application, including reporting, benchmarking, AIG Cyber Portal access, and CyberMatics.

AIG SMART UNDERWRITING APPLICATION - BROKER GUIDANCE

2. Explain the application features and logistics to the risk manager

Required sections and questions: Certain sections and questions will be required, such as the Exposure and Applicability sections.

Note: cyber applicants will see required questions are marked with a red asterisk. Questions marked with a gold star, while optional, will strongly impact their risk scores.

Prioritized questions and numbering: Responses to required questions will prompt additional questions, specific to their organization and risk, which will appear in order of priority. Therefore, the client may see some question numbers out of order, such as in the event that certain questions are higher priority or if certain questions do not apply to them. For instance, questions #12-15 in the E&O section only appear if the applicant is writing software as a professional service.

Parties involved: It's also important to let the risk manager know that other parties within their organization, such as their information security, general counsel, privacy, and finance teams, may need to respond to certain questions. The PDF can be saved and shared by each party as they complete their sections and returned to the risk manager upon completion.

eSignature: Once all questions have been completed, the risk manager should use the eSignature function to sign the application, then digitally send it back to you for submission to AIG. There's no need to print and sign, or submit a printed application, to AIG.

STEPS FOR THE RISK MANAGER TO COMPLETE THE APPLICATION

1. Once the risk manager is comfortable with the application format, provide them with the PDF or download link (www.aig.com/content/dam/aig/america-canada/us/documents/business/cyber/aig-usa-cyber-insurance-application.pdf) and remind him or her that the entire application should be completed digitally, within the PDF.

2. The risk manager should start the application by selecting the coverages sought and completing the Exposure and Applicability questions. Responses to these questions will populate additional risk-specific questions.

Note: the application will ask which coverages are being sought. Risk managers may not be aware of the specific coverages and may, by default, select all. This will affect the questions asked in following sections, so please discuss the coverage options with the risk manager before they begin.

3. At this point in time, other parties within their organization, such as their information security, privacy, general counsel, and finance teams, may need to complete sections of the application specific to their areas.

4. Once all sections have been completed, the risk manager should sign the application using the eSignature function. Again, there's no need to print it out and sign by hand. He or she should return that to you digitally for submitting to AIG.

AFTER SUBMITTING THE APPLICATION: CYBER APPLICANTS

Summarized Assessment Report: If a cyber applicant provides an email address where indicated for reporting, they will receive access to their SAR based on their application responses, which includes their score summary, baseline risk trending, top risk scenarios, risk reducing controls, and more. This provides them with a clear view of their cyber maturity and how we underwrote their risk.

The report will be available through the AIG Cyber Portal, to which they'll receive access following our underwriting of the account.

Executive Summary Report: Upon binding coverage, the client's ESR will be shared via the Portal. The ESR provides a more detailed analysis of the client's cyber maturity, including additional risk scores, prioritized practices for improvement, scenario likelihoods, control effectiveness details, and more.

Client Portal and Future Reports: The client can view their SAR and ESRs through the AIG Cyber Portal. An invitation email will be sent to the risk manager/designated recipient in the application.

If the client participates in CyberMaticsSM, they can then use the dynamic dashboard in the Portal to monitor how their cyber risk scores change over the policy period based on the data feed to AIG. This also aids in ease of policy renewal procedures, as AIG will already have verified answers to many of the application questions.

QUESTIONS? PLEASE CONTACT YOUR AIG UNDERWRITER.

