## Annex XXIV – Instructions for cyber risk proposed template

EIOPA-BoS-19-353
25-26 June 2019

**General comments:**

When a special justification is needed, the explanation is not to be submitted within the reporting template but shall be part of the dialogue between undertakings and national competent authorities.

| | ITEM | INSTRUCTIONS |
|---|---|---|
| C0010 | Internal Risk Identification Code | This code can be assigned by the undertaking to the risk being captured by the template. It shall be numerical and is only meant for internal purposes for risk identification.<br><br>The code shall be unique and be kept consistent over time. Moreover, it shall be consistent with HRG and shall distinguish between B2B policies and policies addressed to private individuals. |
| C0020 | Identification of the Party to which the risk relates | The choice is based on a closed list which allows to choose from:<br>1. First Party Loss – Direct Loss incurred by the insured<br>2. Third Party Loss – Liability coverage/losses to others<br>3. Costs and related services<br><br>Where 1. Relates to risks which have impact on the insured only (see "Risk Description" section to see the detailed list), 2. Relates to risks insisting on possible third parties which are linked to the insured and 3. Relates to coverage of costs and related services only (e.g. legal costs) |
| C0030 | Risk Description | This item has a direct dependence from the previous item ("Identification of the Party to which the risk relates"). If the previous item (mandatory) is not selected, an error message will appear. It is also possible to choose item "Other" if no one of the descriptions fits in the list provided (further details will be asked in the field dedicated to "Risk Detailed Description")<br><br><u>First Party Loss – Direct Loss Incurred by the insured</u><br>- Network Interruption<br>(refers to a network security failure leading to business interruption.<br>Examples may include a Distributed Denial of Service or "DDoS" attack (i.e website being overloaded with requests organized by a malicious party) or a hacker accessing the network and deleting critical files, or adding malicious code that causes the system to fail)<br>- Network Interruption OSP<br>(where OSP stands for Open Settlement Protocol (OSP), i.e. a client-server protocol that manages access control, accounting, usage data and inter-domain routing to make it easier for Internet service providers (ISPs) to support IP telephony)<br>- Network Interruption: system failure<br>(which may include an "unintentional or unplanned outage" on the network.<br>The failure could be due to human error, system error or both. (e.g. a company upgrading its accounting system may unexpectedly cause the entire network to freeze in the process)<br>- Cyber Extortion<br>(a form of online crime in which a website, e-mail server, or computer system is subjected to repeated denial of service (DDoS) or other attacks by malicious hackers, who demand money in return for promising to stop the attacks) |

| | | |
|---|---|---|
| | | - Electronic Data Incident<br>(incident in which sensitive, confidential or otherwise protected data is accessed and/or disclosed in an unauthorized fashion. Data breaches may involve personal health information ( PHI ), personally identifiable information ( PII ), trade secrets or intellectual property)<br>- Cyber Theft<br>(may include online fraud or other similar illicit activities)<br>- Data Restoration<br>(refers to the process of copying backup data from secondary storage and restoring it to its original location or a new location. A restore is performed to return data that has been lost, stolen or damaged to its original condition or to move data to a new location)<br>- Extra expense<br>- System clean-up costs<br>- Administrative investigation and penalties<br><br><u>Third Party Loss – Liability Coverage/Losses to others</u><br>- Physical injury<br>- Data Protection and Cyber Liability<br>(includes also GDPR implications regarding third party data protection)<br>- Media Liability<br>(i.e. reputational risk)<br>- Wrongful collection of information<br>- Media Content infringement/defamatory content<br>- Violation of notification obligations<br>(notification of data breaches is provided in defined time lags by law and or GDPR provisions)<br><br><u>Costs and related services</u><br>- First Response<br>(costs incurred in responding quickly to attacks to restore service)<br>- Event management<br>(all activities needed to restore normal activities)<br>- Communication Costs<br>(big data breaches may require mass communication of the outcomes of the breach)<br>- Credit/Identity monitoring<br>(ensure the restoration/block of credit or identity data collected from customers/employees, etc.)<br>- Criminal Reward Fund<br>(contribution to government funds established to cover cyber liabilities towards third parties)<br><br>Please note that the third description is meant to apply to the costs and related services that relate to the insured only (even if as benefit to others). |
| C0040 | Risk Detailed Description | This item has a direct dependence from the previous item (“Risk Description”). If the previous item (mandatory) is not selected, an error message will appear. Furthermore, if item “Other” has been chosen in “Risk Description”, it will be possible to edit the field without incurring in warning/errors.<br><br><u>Network Interruption</u> |

| | | |
|---|---|---|
| | | - Loss of business income due to cyber incident<br>- Business interruption<br>- Damage to intangible assets<br>- Damage to tangible assets (Products liability)<br><br><u>Network Interruption OSP</u><br>- Loss due to outside provider security or system failure<br><br><u>Network Interruption: system failure</u><br>- Loss due to system failure or human error<br><br><u>Cyber Extortion</u><br>- Cost of ransom payment<br>- Cyber specialist<br><br><u>Electronic Data Incident</u><br>- Loss due to accidental damage of computer systems<br><br><u>Cyber Theft</u><br>- First Party Loss – Financial Loss (includes losses with regard, for example, to company and/or personal data theft, that is a loss that relates to a first party that also has an economic impact on it) |
| C0050 | Line of Business | The field allows to choose between the whole set of Non-Life Lines of Business<br>Name of the line of business, as defined in Annex I to Delegated Regulation (EU) 2015/35. The following close list shall be used:<br>1 - Medical Expense Insurance<br>2 - Income Protection Insurance<br>3 - Workers' Compensation Insurance<br>4 - Motor Vehicle Liability Insurance<br>5 - Other Motor Insurance<br>6 - Marine, Aviation and Transport Insurance<br>7 - Fire and other Damage to Property Insurance<br>8 - General Liability Insurance<br>9 - Credit and Suretyship insurance<br>10 - Legal Expenses Insurance<br>11 - Assistance<br>12 - Miscellaneous Financial Loss<br>13 - Proportional reinsurance - Medical Expense Insurance<br>14 - Proportional reinsurance - Income Protection Insurance<br>15 - Proportional reinsurance - Workers' Compensation Insurance<br>16 - Proportional reinsurance - Motor Vehicle Liability Insurance<br>17 - Proportional reinsurance - Other Motor Insurance<br>18 - Proportional reinsurance - Marine, Aviation and Transport Insurance<br>19 - Proportional reinsurance - Fire and other Damage to Property Insurance<br>20 - Proportional reinsurance - General Liability Insurance<br>21 - Proportional reinsurance - Credit and Suretyship insurance<br>22 - Proportional reinsurance - Legal Expenses Insurance<br>23 - Proportional reinsurance - Assistance<br>24 - Proportional reinsurance - Miscellaneous Financial Loss<br>25 - Non-Proportional reinsurance - Health<br>26 - Non-Proportional reinsurance - Casualty |

| | | |
|---|---|---|
| | | 27 - Non-Proportional reinsurance - Marine, Aviation and Transport<br>28 - Non-Proportional reinsurance - Property |
| C0060 | Risk Unbundling | The field provides for a closed alternative answer:<br>- Yes (in case Cyber coverages have been 100% unbundled from other related risks covered in the policy)<br>- Main risk being covered (in case Cyber is not 100% unbundled from all the risks covered by the contracts) |
| C0070 | Validity period (start date) | Displays the starting date of the contract (identify the ISO 8601 (yyyy–mm–dd) code of the date when the reporting to the supervisory authority is made). |
| C0080 | Validity Period (end date) | Displays the ending date of the contract (identify the ISO 8601 (yyyy–mm–dd) code of the date when the reporting to the supervisory authority is made). |
| C0090 | Currency | Identify the currency of the contract |
| C0100 | Sum insured | Displays total sums insured |
| C0110 | Deductible | Amount of relative or absolute deductible applied to the contract (if applicable) |
| C0120 | Premium written | Premiums written during the reporting period. |
| C0130 | Sum reinsured on a facultative basis | Sum reinsured on a facultative basis for active contracts during the reporting period. |
| C0140 | Sum reinsured other than facultative basis, with all reinsurers | Sum reinsured other than facultative basis, with all reinsurers for active contracts during the reporting period. |
| C0150 | Net retention of insurer | Net retention of insurer |
| C0160 | Number of Claims settled with Payment | Number of claims settled during the year with payment |
| C0170 | Claims paid | Amount of claims paid during the reporting period. |
| C0180 | Numbers of Claims settled without payment | Number of claims settled without payment during the reporting period |
| C190 | Technical provisions | Amount of Technical Provisions |