| Column reference | Shall/ Should / M | Description | Guidance to fill |
|---|---|---|---|
| AI, algorithmic or autonomous system reference | Should | | |
| AI, algorithmic or autonomous system description | Shall | A reference of the scope, nature, context and purpose. | This need not be eloborated in this column. This is just to reflect that risk assessment need to be undertaken for each of the AI, algorithmic or autonomous systems |
| Risk reference | May | A reference number or code to every risk identified | This could be alpha or numeric or both |
| Risk | Shall | Brief reference of the exposure, danger, harm or loss | Its a brief reference. For example, Privacy exposure is a risk |
| Risk description | Shall | Details of risk including its known root causes and impacts | [Adverse Outcome/s that has an effect on people / society / the environment] caused by [missing controls, insufficient control/s] compromised by [inside or outside threat actor/s, or harmful when operating as expected], that may result in [impacts/s] |
| Example of risk | Should | An example explaining the detailed risk | For example, Privacy exposure for children caused by lack of age-appropriate privacy policy. that may result in potential non compliance |
| Input/ Indicator | Shall | A classification as to whether the identified risk is a risk input or a risk indicator | Risk indicators becomes a risk input when their root cases are identified |
| Risk source | Should | A guidance as to the source of risk | There are 4 illustrative sources. They are known risks, secondary research, enquiry/ survey, expanded perception to emergent/ foreseeable risks |
| Is this risk already considered by the org? | | A reference to indicate this risk is already considered by the or | Provide reference to the risk where it is already considered by the org |
| Impact | Shall | Detailing the anticipated impact contributed by the risk | The impact could be explaining whether the said risk will lead to non compliance or financial loss or reputational loss as the case may be. |
| Impact Type | Shall | Classifying perceived impact of the risk | There are 3 broad classification of the impact. They are Impact to individuals/ groups, societal impact and environmental impact |
| Sub impact | May | Providing detailed classification of the impact | The detailed sub impacts include Life impact Physical, Mental and Psychological impact Damage to reputation and/ or identity Privacy exposure and associated harassment etc |
| Impact quantification (may not be feasible in all cases) | May | Quantifying financial impact (if applicable) for the identified risk | Best estimate based on facts and considerations associated with the risk. |

| | | | |
|---|---|---|---|
| Likelihood | Shall | A classification of the likelihood of the risk | The likelihood can be illustrated as Very high, high, moderate, low and very low |
| Severity | Shall | A classification of the severity of the risk | The severity or consequences can be illustrated as insignificant, minor, moderate, major and catastrophic |
| Overall Risk Level | Should | Classification of the level of risk | This is determined based on the risk evaluation. The outcome of risk evaluation (typically classified as high, medium and low) |
| Risk specific to a region/ geo/ location/ group/ communi | Should | Classification as to whether the risk is tied to a region or other factors | Identifer to see if the risk related to any specific population based on location, age or other factors |
| Risk is systemic | Should | Classification as to whether the risk is systemic | Identifier to see if the risk is systemic or otherwise |
| Propotional voting scale | Should | Proportion of DIMSF representatives who provided inputs in this regard | Provide a proportion of representatives who voted for this risk |
| Foreseeable risk/ Emergent Risk/ Systemic Societal | May | Classifying the risk identified | This helps in understanding broader treatment plan at an enterprise level and also determine the considerations for disclosure to users (if any) |