Risk & Control Scope								
Column reference	**Shall/ Should / May**	**Description**	**Guidance to fill**	**Source document to refer**	**EU AI Act Reference**			
AI, algorithmic or autonomous system reference/ name	Should	Name or reference of the AAA system like Name, associated organization (organisation/ third party)						
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					
Process	Should	Process associated with the AI, algorithmic or autonomous system	Process includes Problem and objective framing, Necessity and proportionality assessment, design, Data collection, data labelling, data processing, model development, testing, validation, deployment, monitoring (including post market monitoring) and decommissioning					
Sub Process	May	Identified sub activity within the process	For instance, in data processing, there could be activities involving sampling, deduplication, filling missing data, outlier notmalization etc					
Process owner/ Sub process owner	Should	Individual (designation) who is responsible for the process/ sub process	Designation and role of the individual is relevant. Name may not be required in all cases					
Risk reference	Should	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 Taxonomy				
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]	Risk Taxonomy				
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 management Process				
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	Risk management Process				
Impact	Shall	Detailing the anticipated impact contributed by the	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.	Risk Taxonomy				
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	Risk Taxonomy				
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	Risk Taxonomy				

Impact quantification (may not be feasible in all cases)	Should	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	Risk management Process				
Severity	Shall	A classification of the severity of the risk	The severity or consequences can be illustrated as insignificant, minor, moderate, major and catastrophic	Risk management Process				
Overall Risk Level	Shall	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 management Process				
Foreseeable risk/ Emergent Risk/ Systemic Societal	Should	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)	NIST risk submission				
Root cause	Shall	A description of the key rootcauses	This is to express about the compromisor - essentially inside or outside threat actor/s, or harmful when operating as expected					
Risk Category	Shall	Categorizing risks into broader segments	This helps in consolidating the risks and examining them at an organizational level. These categories will align with the broader risk management approach of the organization and will integrate with ERM. There may be risks that fall under more than one risk category. Hence, this column is a tagging column than an independent risk category column	Risk Taxonomy				
AI Risk Principle	Should	Providing reference to relevant AI principle of the organization	Aligning the risks to the AI principles of the organization. There may be more than one AI principle that will get aligned to the risks	Risk Taxonomy				
Control reference	Should	A reference number or code to every control	This could be alpha or numeric or both					
Control description	Shall	A description of the control for the risk	One control may be common for more than one risk. They could be direct or compensating controls. Providing a description of them for better understanding of the controls	Risk management Process				
Responsibility	Shall	Individual (designation) who is responsible for the control.	Designation and role of the individual is relevant. Name may not be required in all cases. This person may or may not be the process or sub process owner. This in some cases could be a committee responsibility					
Reassessment trigger	May	Identifier for reassessment	A trigger based on other actions to determine whether the risk requires reassessment					
Control effectiveness	Shall	Control effectiveness assessment	Assessing the effectiveness of the control designed for the identified risk					
Recommendation	Shall	Recommendation for failed control or partial effect	Recommendation to address the failed control including alternative control or additional controls					
Responsibility for implmenting recommendation	Shall	Individual (designation) who is responsible for implementing the control	Designation and the role of the individual. Name is not required. Process is to ensure accountability to implement recommendations					