

# cAIRE report

## Consolidated AI Risk Evaluation Report (cAIRE)

- **cAIRE** report consolidates **Risk Outcomes**, **Risk Mitigations** and **Residual Risk** associated with an AI, algorithm or autonomous systems for completeness and integration into Operational Risk Management (ORM) and Enterprise Risk Management (ERM) as dictated by company policy.
- The ORM team shall consolidate and update the **cAIRE** report updated “as-needed” (“as-needed” does not include any real-time or post market monitoring). They shall also report the material Risk and **Adverse Impacts** (according to corporate policy) to the management and board as appropriate.
- The **cAIRE** report is prepared based on the inputs from six key reports. They are (1) **Algorithm Risk Assessment**, (2) **Ethics Risk Assessment**, (3) **TEC At-Risk Report**, (4) **AI Governance Assessment Report**, (5) **Children’s Data Oversight Assessment Report** (6) **Data Management Committee Report**. These reports contain **Risk Logs**, overall risk assessment, gaps from control assessment and **Residual Risk Logs**.
- **Algorithm Risk Assessment** is an analysis of all risks associated with the comprehensive lifecycle of an AI, algorithmic or autonomous system, not covered by the **TEC AT-Risk report**, the **Ethical Risk Analysis**, the **AI Governance Assessment** and the **Systemic Societal Impact Analysis**.
- **Ethics Risk Assessment** is a study of instances of ethical choice, softlaw, application of *Code of Ethics* and *Code of Data Ethics* principles and shared moral frameworks across the lifecycle of the AI, algorithm or autonomous systems
- **TEC At-risk report** is a periodic report (at least quarterly) prepared or compiled by TEC containing risk mitigations for identified risks and residual (unmitigated) risks with accuracy, validity, reliability, robustness and resilience of AI, algorithmic or autonomous systems. The report shall also contain the **Risk Log** (list of risks considered or identified), **Risk Evaluation** and control assessment performed during the process.
- **AI Governance Assessment Report** is an analysis and designation of accountability, oversight and responsibility for committees (**Ethics Committee**, **Algorithm Risk Committee**, **Children’s Data Oversight Committee** and **Testing and Evaluation Committee**), designated individuals (per a **Duty Designation Letter**). The organization shall charge an individual or committee responsible for the interconnectivity of all committees and the organization as a whole, including the Chief Executive Officer and the Board of Directors for any/all risk associated with an AI, algorithmic or autonomous system including duties associated with compliance with audit criteria. The individual or committee

designated accountable for AI Governance shall be an expert in risk management to prepare and oversee the **AI Governance Assessment**.

- **Children’s Data Oversight Assessment Report**
- **cAIRE** report is a consolidation of three key reports (a) Threat & Risk Log, (b) cAIRE Residual Risk schedule and (c) Risk and Control schedule.
- Threat & Risk Log is a list of emergent risks identified based on horizon scanning (including industry, domain, technology etc) that may become applicable for the AI, algorithm or autonomous system of the organization over a period of time. This is a risk intelligence to gather insights on risks that may become relevant for the organization in the context of AI, algorithm or autonomous system.
- **cAIRE Residual Risk** schedule is consolidation of the **Residual Risks** from all the reports along with the treatment plan and specific impact assessments. This report provides management with the unmitigated risks and their implications on business strategy and operations.
- Risk and Control schedule is a consolidation of risks and mapped mitigating controls for risks where appropriate mitigations exist. These are provided as inputs to internal audit for validating operational effectiveness and efficiency of controls mapped to mitigate such risk.
- cAIRE report provides inputs to ERM wherein material risks that are relevant from an enterprise level are compiled for oversight and monitoring.