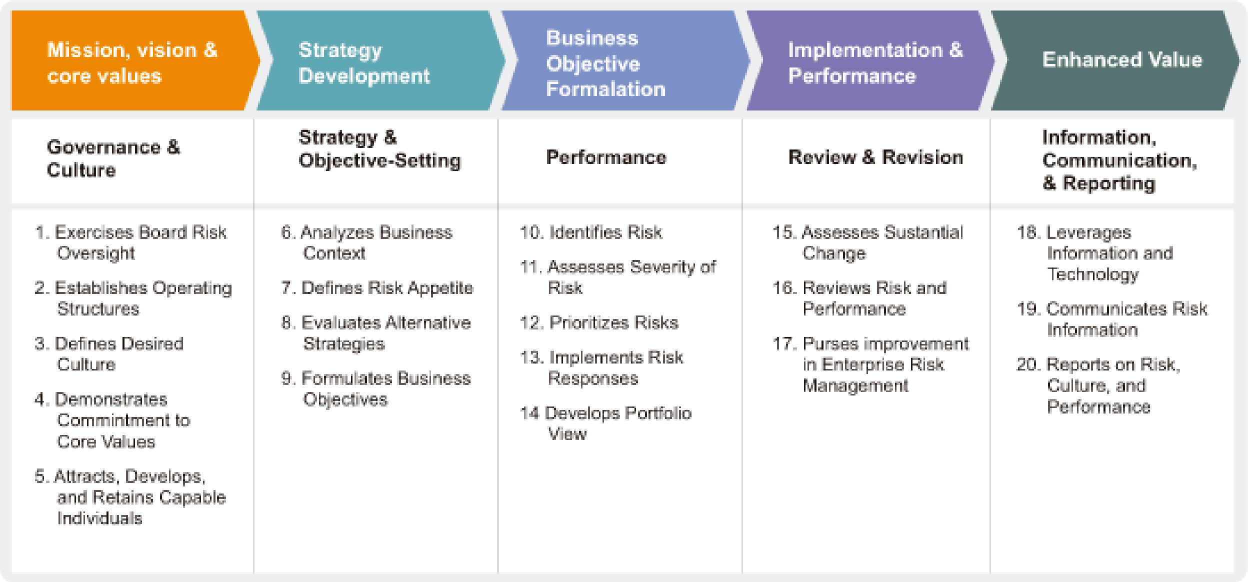
Guidelines on managing AI risks with COSO ERM framework

The Committee of Sponsoring Organization (COSO) has published a framework for Enterprise Risk Management. The Framework defines essential enterprise risk management components, discusses key ERM principles and concepts, suggests a common ERM language, and provides clear direction and guidance for enterprise risk management (here).

In this document, we have considered the COSO ERM framework and detailed how FH Risk Management work integrates with the components of the framework. We detail specific actions for each of the 20 components of the framework providing guidance on measures for integrating FH Risk Management efforts to the broader Enterprise Risk Management.

COSO ERM framework



Mission, vision & core values	Strategy Development	Business Objective Formalation	Implementation & Performance	Enhanced Value
Governance & Culture	Strategy & Objective-Setting	Performance	Review & Revision	Information, Communication, & Reporting
1. Exercises Board Risk Oversight 2. Establishes Operating Structures 3. Defines Desired Culture 4. Demonstrates Commintment to Core Values 5. Attracts, Develops, and Retains Capable Individuals	6. Analyzes Business Context 7. Defines Risk Appetite 8. Evaluates Alternative Strategies 9. Formulates Business Objectives	10. Identifies Risk 11. Assesses Severity of Risk 12. Prioritizes Risks 13. Implements Risk Responses 14 Develops Portfolio View	15. Assesses Sustantial Change 16. Reviews Risk and Performance 17. Purses improvement in Enterprise Risk Management	18. Leverages Information and Technology 19. Communicates Risk Information 20. Reports on Risk, Culture, and Performance

A. Governance & Culture

A1. Exercises board risk oversight

- **Board adoption of principles:** The Board shall approve adoption of AI Governance Principles and the associated program to implement the principles into practice. This includes approving the establishment of an

Algorithmic Risk Committee, Ethics Risk Committee, Children's Data Oversight Committee and Testing and Evaluation Committee or a designated officer thereof as appropriate for the purpose of implementing the principles.

- **Board adoption of AI Risk Management Program:** The Board shall approve the adoption of AI Risk Management (including ethical risk) Program that establishes the organizational level Risk Management Framework, Risk Taxonomy, Risk Tolerance and Risk-Benefit decision criteria in addition to roles and responsibilities of committees and/ or designated personnel.
- **Audit Committee Oversight:** The Board may consider designating an Audit committee or a sub committee to oversee effectiveness of AI Risk Management implementation and ongoing risk dialogue on AI Risk Management including regular sessions with ARC, EC and CDOC as appropriate.
- **Board composition and skillset:** The Board may have at least one member with specialized expertise in one or more areas of AI Risk Management or an overall knowledge of AI Risk Management.
- **Committee appointment:** The Board shall provide input and approve appointment, dismissal or restructuring of organizational level Algorithmic Risk Committee, Ethics Risk Committee, Children's Data Oversight Committee and Testing and Evaluation Committee or a designated officer thereof (including an Chief Ethics Officer, Chief Data Ethics Officer or a designated officer for implementing the principles).
- **Report on program implementation:** The Board shall require reports and updates from the committees or designated officers for implementing the AI Governance principles on the progress and document the proceeding in the minutes of the Board.
- **Report on material issues:** The Board shall examine measures adopted to remediate material gaps (in implementing AI Governance Principles in practice) or material harms reported or responding to regulatory enquiries associated with AI, algorithmic or autonomous systems.
- **Resource adequacy:** The board shall mandate the chief executive officer to assess adequacy of resources for implementation of AI Risk Management Program.

A2. Establishes operational structures

- **Independence for designated officer:** The Board shall ensure that the AI Risk Management Program shall require independence of the designated officer responsible for implementing or driving AI Risk Management.
- **Designated officer reporting:** The Chief Executive Officer shall ensure that the designated officer directly reports to and regularly communicates with The Board on AI Risk Management.
- **Designated officer level:** The Chief Executive Officer shall also ensure that the designated officer and AI Risk Management Program shall have stature relative to other functional leaders or organizational policies.
- **Designated officer authority:** The Chief Executive Officer shall confer sufficient authority to the designated personnel to manage implementation of AI Risk Management Program effectively.
- **Resource allocation for the program:** The Chief Executive Officer shall ensure sufficient resources for the AI Risk Management Program to be effective.
- **Adoption of policies and procedures:** The Chief Executive Officer shall enable adoption of policies and procedures for operationalizing the AI Risk Management program.
- **Protocols for reporting or escalation:** The Chief Executive Officer shall establish protocol and/ or procedures for escalation (including the hierarchy thereof) of significant or material AI Risk Events (including Failures, Defects and Adverse Events).

A3. Defines desired culture

- **Policy approval:** The Board shall approve policies associated with the pillars of Ethics, Bias, Privacy, Cybersecurity and Trust (eg. Data Ethics Policy, Privacy Policy etc) for adoption with specific reference to AI Risk Management Program.
- **Adequacy of policy:** The designated officer shall ensure that the expectations associated with Ethics, Bias, Privacy, Cybersecurity and Trust are clearly articulated in the policies.
- **Training and communication on policies:**The designated officer shall determine the requirement for training (including the extent thereof) on policies for employees, contractors, third parties and board members. The

designated officer shall deploy measures that provide training based on the requirement for training on the policies for employees, contractors, third parties and board members.

- **Awareness assessment on policies:** The designated officer may in consultation with the Chief Executive Officer or anyone so appointed by the Chief Executive Officer deploy a mechanism to assess awareness of policies and to monitor their adoption on an ongoing basis across organization.
- **Culture influence:** The Chief Executive officer in consultation with the designated officer deploy measures to exhibit the culture of standing by AI principles and AI risk management program with his/ her tone at the top.
- **Identifying Key risk indicators:** The designated officer shall develop objectively measurable AI Key Risk Indicators (KRIs) tied to risk identifications, evaluations, tradeoffs and mitigations, where appropriate.
- **Adoption of AI risk policies:** The Chief Executive Officer shall establish meaningful incentives for adoption and consistent implementation of AI Risk Policies.
- **Leadership alignment:** The Chief Executive Officer shall deploy measures to ensure that leaders (as may be defined by the CEO) across the organization are actively including AI Governance Principles and AI Risk considerations as part of the ongoing business operations.

A4. Demonstrates commitment to core values

- **Tone at the top:** The designated officer shall actively promote a culture of AI risk awareness, including setting an ethical and responsible tone by leadership
- **Review material decision using risk-benefit criteria:** The designated officer shall review material decisions adopted using Risk-Benefit criteria to assess potential risk implications and mitigation efforts in that regard.
- **Accountability integrated to performance measure:** The Chief Executive Officer shall deploy a mechanism that incorporates accountability for the management of (1) AI risks and (2) AI risk management program implementation into employee performance measurement, promotions, and incentive programs, particularly at senior levels.
- **Anti-relationation policy:** The designated officer shall in consultation with the ethics officer ensure retaliation policy includes references to retaliation in the context of adoption of AI risk management or AI Governance Principles.
- **Root cause analysis for adverse incidents:** The designated officer shall deploy a mechanism for reviewing the root causes (intentional and

unintentional) and remediations adopted for adverse events reported through Adverse Incident Reporting System and measures to prevent their recurrence.

- **Establish multi-stakeholder channels:** The designated officer shall establish access with external stakeholder groups (civil society, NGO or specialist organizations) for teams across the value chain to gather multi-stakeholder feedback. In addition, the designated officer shall create criteria for selection and empanelment of external stakeholder groups across the value chain.
- **Consistent principle adoption for tradeoff decisions:** The designated officer shall ensure that the decisions adopted for trade offs or Risk-Benefit scenarios are consistently applied in line with the AI Governance Principles.
- **Awareness based on lessons learned:** The designated officer shall establish a communication mechanism to ensure that lessons learned from failures across the organization in appropriate detail, to avoid their recurrence.

A5. Attracts, Develops and retains capable individuals

- **Hire and Retain Designated Personnel:** The Chief Executive Officer shall hire and retain a designated officer with appropriate experience/expertise to lead the AI risk management
- **Risk Management Staffing:** The Chief Executive Officer shall staff the AI risk management with individuals that possess relevant expertise
- **Due Diligence:** The designated officer shall deploy adequate procedures for conducting risk-based due diligence on third parties who support in AI design, development and deployment.
- **Performance Management:** The designated officer shall in consultation with the Chief Executive Officer adopt a mechanism to include AI risk management and adoption of AI governance principles as part of the performance metrics of employees.

B. Strategy & Objective-setting

B1. Analyzes business context

- **Strategy alignment with principles:** The designated officer shall consider organizational strategy and AI governance principles adopted in performing AI risk assessments and managing AI risk.
- **Organizational change and risk impact:** The ARC shall consider and review significant changes to the organizational structure, technology, people and processes and its impact on AI risk management.

- **External environment change and risk impact:** The ARC shall examine and consider the potential implications of external environment (e.g., competitive, economic, enforcement trends, environmental, political, social forces) on AI risks (for eg. demands for banning facial recognition can have an impact on risk perceived for AI)
- **Risk interdependencies:** The ARC shall identify and consider AI risk interdependencies in the development of strategy.
- **Risk considerations for cultural and regional context:** The ARC and EC shall examine the risks and ethical considerations in the context of cultural/ regional factors and relevant legal frameworks based on locations where the organization or the AI operates/ applied.

B2. Defines risk appetite

- **Include AI risk in org risk profile:** The designated officer shall consider AI risk as part of the organization's risk profile in determining risk appetite
- **Classify risks:** The designated officer shall consider AI risk by (1) type of risk (e.g., discrimination), (2) business unit or organizational function (e.g., human resources), and (3) location or region
- **AI risks and business impact:** The designated officer shall determine and evaluate the relationships between AI risks risks and their impact on achievement of business objectives
- **Define risk appetite and review periodically:** The designated officer shall discuss with the Chief Executive Officer on risk appetite on a regular basis and update as necessary based on changes in AI risk

B3. Evaluates alternative strategies

- **Risk aligned to business context:** The designated officer shall ensure that the AI risk management and adoption of AI Governance principles shall be tailored to key stakeholder, domain and industry needs
- **Seat at the table:** The Chief Executive Officer shall ensure that the designated officer has a seat at the table in discussions of strategies (to provide inputs from the risk management lens)
- **Risk inputs on strategic topics:** The Chief Executive Officer shall seek inputs and insights from the designated officer regarding how strategy affects AI risk or vice versa.
- **Risk based due diligence on M&A transactions:** The Chief Executive Officer shall mandate the designated officer to perform risk-based due diligence on merger and acquisition targets prior to execution of the transaction. The review shall provide for Go or No go decisions and also

provide with an action plan for risk mitigation if the decision is to progress with the transaction.

- **Risk consideration for strategic decisions:** The chief executive officer shall consider implications of strategic decisions (including subsequent changes in strategy) in the design of the AI principles and AI risk management program.

B4. Formulates business objectives

- **Risk management as integral to business objective:** The chief executive officer shall consider establishing AI risk management as a essential component of business objective
- **Business and risk interactions on business objectives:** The chief executive officer shall ensure that a definitive structure and process is established for interactions between business and AI risk management based on changes in business objectives
- **Risk metrics within business objectives:** The chief executive officer shall consider including objectively measured AI risk metrics within business objectives, reflecting the management of AI risk and the effectiveness of AI risk management program implementation, and carrying appropriate weight in incentive and other compensation decisions

C. Performance

C1. Identifies risk

- **Define risk identification and assessment process:** The ARC, EC and TEC shall describe the AI risk identification and assessment process as part of the documented policies and procedures including limitations, assumptions and exclusions.
- **Identify key risks associated with AI:** The ARC, EC and TEC shall identify AI risks associated in the context of AI, algorithm or autonomous system in the context of planned strategy and business objectives
- **Internal and external factors consideration:** The designated officer along with the ARC, EC and TEC assess and agree on internal (business, domain, industry etc) and external environment factors to consider in identifying risks on a periodic basis.
- **Identify emergent risks:** The ARC, EC and TEC shall have a process of identifying new and emerging risks

- **Deploy Key risk indicators:** The Algorithmic Risk Committee shall define and deploy Key risk indicators for monitoring the triggers for change in AI risk - internal and external, emergent risk and/ or a realized risk.
- **Risks arising from use of third parties:** The ARC, EC, TEC shall consider risks associated with use of third parties in the process of design, development, deployment and decommissioning of the AI, algorithmic or autonomous systems.
- **Insights from incident management:** The ARC, EC, TEC and the designated officer shall consider information gathered through Adverse Incident Reporting System (AIRS), incident management mechanisms, other reporting channels, and results of investigations/ root cause analysis therein in identifying risks.

C2. Assesses severity of risk

- **Criteria for risk assessment:** The designated officer shall define the criteria for risk assessment including risk likelihood, risk weights and risk levels. The designated officer shall also develop and share with ARC, EC and TEC an appropriate risk taxonomy for the organization.
- **Risk scoring:** The ARC, TEC and EC shall adopt a uniform scale/scoring system for measuring severity of AI risks considering both qualitative and quantitative measures.
- **Risk impact, severity and likelihood:** The ARC, EC and TEC shall also establish criteria to assess impact, severity and likelihood of compliance risk event occurrence and to assess severity of risk at different levels (organizational, regional, affiliate, etc.)
- **Control design and adequacy:** The designated officer along with ARC, EC and TEC shall consider design and operation of internal controls and multi-stakeholder feedback mechanism that is intended to prevent or detect AI risk events
- **Bias in risk assessment:** The designated officer shall implement measures to minimize bias and inadequate knowledge in assessing severity (e.g., minimize self-assessments, use multidisciplinary teams)

C3. Prioritizes risk

- **Risk priority criteria:** The ARC and EC shall define the priority for AI risks based on the assessed level of risk relative to factors including business objectives and people impact among others.

- **Risk response priority:** The ARC, EC and TEC shall develop risk-based action plans for mitigation (risk responses, implemented in next step) and their priority.

C4. Implements Risk response

- **Policy and process changes to mitigate risks:** The ARC and EC shall consider the need for modifications, amendments or enhancements to policies, the AI risk management program and/ or the AI governance principles to mitigate risks. Any modifications shall undergo governance and oversight by the Board or designated authority as may be prescribed by the board and approved by the board prior to implementation.
- **Risk response assignment:** The ARC and EC shall assign responsibility for each AI risk response to identified stakeholders along with the timeline and monitor the same on an ongoing basis.
- **Risk response process:** The ARC, EC and TEC shall examine the adequacy of processes to implement integrated risk responses and effectiveness of such processes thereof.
- **Internal audit of risk responses:** The ARC, EC and internal audit shall consider AI risk responses when developing monitoring and auditing plans

C5. Develops portfolio view

- **Risk interactions or inter-relationships:** The ARC, EC and TEC shall deploy measures to monitor potential implications of risk interactions (specifically with reference to interactions between risks, interactions between mitigation of one risk and other risk, and interaction between mitigations).
- **Integrated with ERM:** The designated officer shall integrate AI risk management efforts with ERM to the extent it is critical at enterprise level.
- **Risk portfolio view:** The designated officer, ARC, EC and TEC shall have regular meetings/ communications between functions for gaining and sharing holistic view of the risks.

D. Review & revision

D1. Assesses Substantial Change

- The Algorithmic Risk Committee and the Ethics Committee shall consider evaluating the strategic initiatives of the organization to identify critical and material AI risks and deploy adequate mitigation measures against them in a timely manner.

- **Consistency in applying Risk Tolerance:** The Algorithmic Risk Committee and ethics committee shall ensure that the risk tolerance is measured in a consistent manner irrespective of change in key management personnel.
- **Risk contributed by change:** The Algorithmic risk committee, the Ethics Committee, the Children's Data Oversight Committee and Testing and Evaluation Committee shall identify potential new/ change in regulations, regulatory guidances (including local and regional regulations) and enforcement trends that impact or has relevance the organization in the context of AI risk and deploy measures to comply with such regulations (including reporting or auditing obligations if any).

D2. Review Risk and Performance

- **Annual risk assessment:** The designated personnel shall develop an annual risk assessment exercise consisting of risk surveys, risk research, adverse events review to ensure all critical risks are considered as part of the assessment and evaluation exercise.
- **Monitor risks:** The ARC and EC shall monitor risk metrics on a periodic basis and report at the management and board levels. The ARC and EC shall deploy mechanisms to update the risk metrics on a periodic basis or based on specific need to change (triggered by risk impact or risk event).
- **Monitor mitigation plans:** The ARC, EC and TEC shall deploy mechanisms to monitor mitigation plans for high-priority risks, assign assurance responsibilities clearly across the three lines of defense, and set clear performance expectations.
- **Internal audit of AI risk management:** The Chief executive officer shall mandate internal audit or other designated function or personnel to conduct AI risk awareness culture audit and control effectiveness audit on a periodic basis and submit the outcomes and the gaps therein with the ARC, EC, TEC and the designated personnel for remediation or action
- **Examine gaps via audit:** The ARC, EC, TEC and the designated personnel shall monitor the gaps identified in internal or external audit (including control effectiveness review and AI risk awareness culture audit) and deploy adequate measures to mitigate them.
- **Root cause analysis:** The ARC, EC and TEC shall ensure specific root causes analysis is performed on risk events or adverse events experienced by the organization and appropriate mitigation measures are undertaken.

- **Audit clauses in contract:**The Chief executive officer shall ensure that appropriate right to audit clauses are included as part of the third parties and contractors contracts who are involved in designing, developing, deploying and maintaining AI, algorithmic and autonomous systems.
- **Feedback on AI risk management:** The designated officer shall obtain ongoing feedback with reference to AI risk management from training conducted, adverse event reports, employee surveys, and exit interviews.

D3. Pursues improvement in enterprise risk management

- **Industry or domain risk trend awareness**: The designated personnel shall maintain adequate awareness on emerging AI risk management practices and emergent risks reported in the relevant domain and/ or industry.
- **Effectiveness self assessment for program:** The AI risk management team shall conduct a self assessment of the effectiveness of the AI Risk Management Program, identify areas that require material progress and report to the Chief executive officer with a progress plan for the area where the effectiveness needs to be improved.
- **Feedback on risk information and reports shared:** The ARC and EC shall engage with the Board to understand the feedback, adequacy and usefulness of the AI risk information shared.
- **Benchmarking of AI risk management:** The Chief Executive officer shall consider conducting independent evaluation or conducting a benchmarking of the AI risk management program. The chief executive officer shall review efficacy of the AI risk assessment process on a periodic basis based on reports, adverse reports and other information.
- **Internal audit of AI risk management program:** The chief executive officer shall ensure that internal audit plays an active role in periodically evaluating the effectiveness of the AI risk management program

Information, communication & reporting

E1. Leverages information and technology

- **Resource allocation:** The chief executive officer shall ensure that the designated officer driving AI risk management program shall have adequate access to all information relevant to effectively manage AI risk.
- **Team skills:** The chief executive officer shall provide the AI Risk management team with relevant resources including information technology, data science, sociology, philosophy etc to assess risks.

- **Automated testing and monitoring:** The designated officer shall deploy appropriate automated testing and metric monitoring measures for identifying and assessing risks and monitoring performance of internal controls on an ongoing basis.

E2. Communicates risk information

- **Communication process:** The designated officer or the committee thereof shall deploy a process to ensure that the employees receive clear and regular communications on their roles regarding AI risk management and AI governance principles.
- The Chief Executive officer shall enable and ensure there is periodic reporting to the board by the designated officer on AI risk management.
- **Communication and escalation protocols:** The designated officer deploys methodology and protocols to ensure that employees and third parties (hired for AI design, development and deployment) have a clear understanding of points in time when escalation needs to be done.
- **Communication training for third parties:** The designated officer shall provide AI risk communications that support, help and relate to training and job responsibilities for the employees and third party contractors hired for designing, developing, deploying and maintaining AI, algorithmic and autonomous systems.
- **Risk communication and response:** The designated officer shall deploy a communication protocol for effective two-way communication between functional teams and AI Risk management teams.

E3. Reports on risk, culture and performance

- **Report on effectiveness of program:** The designated officer shall develop and report on meaningful operational and substantive metrics associated with the effectiveness of the AI Risk Management program
- **Report on training adherence:** The designated officer shall provide a report to the Learning and Development team on the status of adherence to training schedules for staff across organizational functions.
- **Reporting on material issues:** The designated officer shall provide periodic (preferably quarterly) reports to management and Chief Executive Officer on AI risk including summary of and material findings from ARA, ERA and TEC At-risk report.
- **Reporting of corrective action plan:** The ARC and EC shall ensure that the corrective action plans are tracked, monitored and reported to the management and the board

- **Report on emerging risk trends from incident management:** The designated officer shall use a incident management or reporting system for compiling a report on emerging risk trends and documenting the adverse events and their resolutions under Adverse Event Tracking System (AETS)
- **Report on remediation status of critical enterprise risks:** The designated officer shall share remediation efforts of enterprise critical risks and their status (including timeline for sufficiency in remediation) for material risks faced by the organization.
- **Report on material unmitigated risks and their potential impacts**: The designated officer shall report on assessed instances of unmitigated impacts (prior to remediation) and assessed metrics of systemic societal impact to the management for sensitizing on risk and enabling more involved risk management culture.