مصرف قطر المركزي
Qatar Central Bank
State of Qatar • دولـــة قطـــر

Artificial Intelligence Guideline

(Regulating the use of Artificial Intelligence by QCB Licensed Entities)

Table of Contents

PART A (GENERAL PROVISIONS) 4

1. Short Title & Commencement 4
2. Definitions 4
3. Introduction 6
4. Purpose 7
5. Scope 7

PART B (GOVERNANCE) 7

6. Strategy 7
7. Corporate Governance 8
8. AI Governance Policy 9
9. Risk Management 9
10. Register 10
11. AI Approval 11
12. Outsourcing 12

PART C (HUMAN OVERSIGHT OF AI IN USE) 13

13. Human Oversight of AI 13

PART D (AI LIFE CYCLE MANAGEMENT) 15

14. Approvals of AI System training and testing 15
15. AI Data Governance 15
16. Framework for High-Risk AI Management 17
17. AI Security 18
18. Documentation 19

19. Monitoring.....19

PART E (INTERACTIONS WITH CUSTOMERS).....20

20. Customer Information and Consent.....20

21. Customer Rights and Recourse.....21

22. Option to Opt-out.....21

23. Exemptions.....22

PART F (COMPLIANCE WITH SECONDARY REGULATIONS).....22

24. Compliance with Secondary Regulations.....22

PART A (GENERAL PROVISIONS)

1. Short Title & Commencement

The instructions set forth herein are titled the "Artificial Intelligence Guideline" for 2024 and shall enter into force as of 04/09/2024.

2. Definitions

For the purpose of this guideline, the following terms are defined as follows, unless the context otherwise suggests.

S. No.	Term	Explanation
1	AI Model	A software program or Algorithm trained using specific data to recognize certain patterns and uses to perform specific tasks.
2	AI Trust, Risk & Security Management (TRiSM)	A mechanism that supports an AI Model's governance, trustworthiness, fairness, reliability, robustness, transparency and data protection.
3	Algorithm	A set of commands that must be followed for a computer to perform calculations or other problem-solving operations.
4	Artificial Intelligence (AI)	A set of technologies that seek to simulate human traits such as knowledge, reasoning, problem solving, perception, learning and planning, and depending on the AI Model, produce an output or decision (such as a prediction, recommendation, or classification).
5	AI System	A System(s) derived from AI Algorithms, which in turn were developed based on an underlying AI Model.
6	Bias	AI results that are not representative of the actual real world or desired model world as a result of Data Sets containing biased data.
7	Customer	A natural or legal person receiving goods or services produced by or utilizing AI Systems.
8	Data Sets	The raw data on which AI Algorithms are derived from.
9	Entity	An Entity regulated by the Qatar Central Bank.

10	High-Risk AI	AI Systems that are risk assessed as having the potential to cause significant negative impact to an Entity's operations or the financial system; Where high risk indicates a risk that is significant as a result of its severity, intensity, probability of occurrence, and duration of its effects, and its ability to affect an individual, a plurality of persons or to affect a particular group of persons or limit their access to financial resources or essential services.
11	Human Oversight	Use of trained human Supervisor(s) to provide a level of direct Human Oversight of AI Systems usually following one of three protocols; 1. AI assisted decision-making or AI with Human Oversight: Humans are actively involved, and no decision can be made without human approval for designated outputs. 2. Human exception oversight: Humans are involved in a monitoring or supervisory capacity and empowered to intervene when the AI Model performs outside expected parameters or fails. The human has the power to close the system down. 3. Fully autonomous AI: AI System where the normal operations are fully under control of the AI Algorithm.
12	Input Data	The data provided to or directly acquired by an AI System to generate a specific result or output.
13	Life Cycle	The duration of an AI System, from design through retirement. Substantially modified AI Systems must be considered as a new AI System, thereby ending the lifecycle of the previous AI System.
14	Material AI Portfolio	An Entity's portfolio of AI Systems, either individual system or group systems, where a disruption in service or breach of security or confidentiality of systems or data may have the potential to materially impact an Entity's compliance with its obligations under the applicable legislation, financial performance, reputation and potentially the soundness or the continuity of an Entity's main services and activities.
15	Operator	A natural person who operates or has oversight over an AI System in use.
16	Monitoring System	All activities carried out by Providers of AI Systems to collect and review experience gained from the use of AI Systems they place on the market or put into service for the purpose of identifying any need to immediately apply any necessary corrective or preventive actions.

17	Providers	A natural or legal person, public authority, agency, or other body that develops an AI System or that has an AI System developed and places that system on the market or puts it into service under its own name or trademark, whether for payment or free of charge.
18	Qatar	The State of Qatar.
19	QCB	The Qatar Central Bank.
20	QCB Law	Law of the Qatar Central Bank and the Regulation of Financial Institutions No. (13) of 2012.
21	Register	Inventory of an Entity's AI arrangements.
22	Sector-Specific Security Regulation	QCB Information Security regulations that are applicable to Entities from a specific subsector within the financial sector in Qatar.
23	Sensitive Personal Information (SPI)	Personal data, related to ethnic origin, children, health, physical or psychological condition, religious creeds, marital relations, and criminal offenses.
24	Supervisor	A natural person who performs the Human Oversight function.
25	Testing Data	Data used for providing an independent evaluation of the trained and validated AI System in order to confirm the expected performance of that system before it is placed on the market or put into service.
26	Training Data	Data used for training an AI Model and helping it develop Algorithms.
27	User	A natural or legal person, including a public authority, agency, or other body, under whose authority the system is operated.
28	Validation Data	Provides an unbiased evaluation of a model fit on the Training Data Set while tuning the model's hyperparameters.

3. Introduction

The term "AI" encompasses a wide range of applications, reflecting its broad and diverse scope. It implies that a system is designed to operate with elements of autonomy. Based on machine and human-provided data and inputs, an AI System infers how to achieve a given set of objectives using logic and knowledge-based approaches. AI Systems may also produce self-generated outputs such as content (generative AI Systems), predictions, recommendations, or decisions.

AI provides opportunities for the financial sector, enabling advancements in various applications. However, AI also introduces risks and concerns, including biases, discrimination, privacy and security issues, lack of transparency, accountability, and ethical dilemmas. These challenges need to be addressed by financial institutions prior to and during the use of AI.

4. Purpose

This guideline sets requirements and provides general guidance for the use of AI Systems, or systems provision by all Entities regulated by the QCB to ensure their usage is safe, secure, and efficient. The guideline defines the principles for using AI, assessment of risks related to AI and the ability to categorize AI Systems.

5. Scope

This guideline covers the use of AI by a QCB regulated Entity. It shall be applicable when an Entity develops and implements AI on its own, purchases AI Systems, or outsources processes or functions that rely directly on AI.

PART B (GOVERNANCE)

6. Strategy

6.1. An Entity must create a defined AI strategy based on the Entity's needs and risk appetite. It must also be consistent with the Entity's relevant strategies and internal policies and processes.

6.2. An Entity must conduct a periodic review of its AI strategy at a time consistent with other strategic reviews.

6.3. An Entity should ensure that its strategy provides a business case, addresses information and communication technology requirements, information security, and operational risk management including business continuity, disaster recovery, and resiliency framework.

6.4. An Entity's AI strategy should define an implementation plan and architectural roadmap which covers the target IT environment, the transition from the current environment to the target environment and the operating model, including any organizational change or additional skillsets that may be necessary.

6.5. An Entity must allocate sufficient resources to handle any AI projects and ongoing business needs.

7. Corporate Governance

7.1. The Board of Directors (BOD) and senior management of an Entity remain accountable for the outcomes and decisions of the Entity's AI Systems including those systems that make decisions on behalf of the Entity.

7.2. The key responsibilities of the BOD include but are not limited to:

7.2.1. Approving the level of AI exposures to be tolerated in the overall risk framework.

7.2.2. Deciding whether an Entity's existing governance structures are fit for purpose.

7.2.3. Assigning clear lines of accountability and responsibility.

7.2.4. Ensuring adequate human resourcing of all AI functions.

7.3. The key responsibilities of the senior management include but are not limited to:

7.3.1. Must have one or more members with the knowledge to understand and manage technology risks, ideally including AI.

7.3.2. Must be responsible for the assessment, understanding and monitoring of the Entity's reliance on AI.

7.3.3. Must ensure responsibility for, and oversight of the various stages and activities involved in AI portfolio deployment is allocated to the appropriate personnel and/ or departments.

7.3.4. Must provide information to the BOD that is clear, consistent, robust, timely, well-targeted and contain an appropriate level of technical detail to allow the BOD to provide effective oversight and challenge management.

7.4. An Entity should establish either a function overseeing AI or delegating its responsibility to an existing function within an Entity.

7.5. The function responsible for overseeing AI must utilize or create appropriate committees to assess AI use cases prior to implementation.

7.6. An Entity must manage risks associated with the use of AI within the enterprise risk management structure.

7.7. An Entity must ensure that their AI Systems promote fair treatment, produce objective, consistent, ethical, fair outcomes, and are aligned with an Entity's ethical standards, value, and codes of conduct.

7.8. An Entity may appoint an ethics oversight body or ethics focused resources in its corporate structure.

7.9. An Entity may develop monitoring controls to measure the fairness of an Entity's AI Model and policies when and how to initiate remedial actions.

7.10. An Entity may define what it means for an AI Model to be fair by area of system or use case.

7.11. An Entity may consider and assess the impact the Entity's AI Models may have on individuals or groups of individuals to ensure that such individuals or groups are not systematically disadvantaged unless the decisions suggested by the models have a clearly documented justification.

7.12. An Entity must take precautions to minimize unintentional or undeclared Bias.

8. AI Governance Policy

8.1. An Entity must ensure that the functions associated with AI governance are fully aware of their roles and responsibilities, properly trained, and provided with the resources and guidance needed for them to discharge their duties.

8.2. An Entity must allocate key roles and responsibilities associated with managing the Entity's AI portfolio to ensure:

8.2.1. Management of AI-related risks through regular audits covering regulatory compliance, governance, customer interactions, risk management process, systems, and control evaluation, and applying required mitigation controls.

8.2.2. The maintaining, monitoring, documenting, and review of the AI Models that have been deployed.

8.2.3. Clear allocation of roles & responsibilities between model owners, developers and approvers.

8.2.4. Ensuring relevant staff involved with AI Systems are properly trained to interpret AI Model output and decisions and to detect and manage Bias in data when working and interacting directly with AI Models.

8.2.5. Ensure that all staff who deal with the AI System are aware of and sensitive to the benefits, risks and limitations of using AI.

9. Risk Management

9.1. An Entity must evaluate risks associated with deployment of AI within the organization.

9.2. An Entity must evaluate the use of the AI System in critical organizational processes.

9.3. An Entity must determine AI risk levels by conducting risk and criticality assessments of the process and functions that the AI System implementation is a part of or connected to.

9.4. An Entity must manage the process so that the AI risk assessment stays in line with overall process and function risk assessment.

9.5. An Entity must inform its AI risk score by using additional factors.

9.5.1. An AI System that allows no direct Human Oversight will probably be judged a higher-than-normal risk, while an AI System that works at delivering "AI-assisted" outcomes, where the final determination is always made by a human with relevant expertise, will likely be judged a lower risk category.

9.5.2. An Entity assessing the use of an AI System developed by a third-party vendor must consider the access to information allowed and the reputation of the vendor as important risk assessment variables.

9.6. The Entity will determine whether a specific AI System is "High Risk" using the definition in Section (2), and the risk evaluation and rating per clauses (9.1) to (9.5).

9.7. Notwithstanding the determination made in clause (9.6), an Entity must classify an AI System as high-risk if or when there is a level of potential harm to natural persons from the system, namely with respect to:

9.7.1. Interactions determining consumer access to financial services offerings.

9.7.2. Internal organizational decisions that affect employees in a material manner.

9.7.3. Processing sensitive personal information.

9.8. An Entity, if it is the Provider, must have or develop the risk management system that specifically is designed to handle AI related risk with capacity to handle the profile of each AI System.

10. Register

10.1. An Entity must develop and maintain an updated Register of information on all its AI Systems arrangements.

10.2. An Entity must disclose to QCB the criteria it is using to determine if the contract for a specific AI System that is high-risk or not.

10.3. An Entity must disclose to QCB a high-level risk and impact assessment.

10.4. High-risk systems must be highlighted.

10.5. AI Systems must highlight the Provider.

10.6. An Entity is required to disclose the full Register to QCB on an annual basis, and upon request by QCB.

10.7. The Register of the Entity must include for each system:

10.7.1. The classification of high-risk or not high-risk.

10.7.2. The role of an Entity, that is, whether it a User of the system or a Provider of the system.

10.7.3. A category assigned by an Entity that reflects the nature or functional use of the AI System.

10.7.4. The Human Oversight protocol used.

10.7.5. In addition, if the AI System is purchased or licensed or outsourced:

10.7.5.1. The name of the Provider and any outsourcer.

10.7.5.2. Third party supplier assessment.

10.7.5.3. The country of registration, local corporate registration number and LEI (where applicable).

10.7.5.4. Registered address and relevant contact details.

10.7.5.5. Name of the parent company (where applicable).

10.7.5.6. Governing law of the AI licensing or purchase arrangement.

10.7.5.7. The creation date of the system and all subsequent upgrades.

10.7.5.8. The contract start date, as applicable.

10.7.5.9. The next contract renewal date.

10.7.5.10. For any high-risk system:

i. Assess the AI's substitutability as easy, difficult, or impossible.

ii. Identify an alternate service Provider, (where applicable).

10.8. An Entity must maintain a detailed description of all High-Risk AI Systems including Life Cycle (development history, data used, testing, tracking).

10.9. The date of the most recent risk assessment or audit of all High-Risk AI Systems together with a summary of the main results, and the date of the next planned risk assessment/ audit.

11. AI Approval

11.1. An Entity must receive official QCB approval prior to launching a new AI System as a Provider and to any material modification of an existing one.

11.2. An Entity must receive official QCB approval prior to signing any High-Risk AI purchase, licensing, or outsourcing agreement in line with the outsourcing guidelines and recommendations from QCB.

11.3. Prior to granting approval, QCB may direct a particular AI System for further evaluation in a sandbox environment.

11.4. An Entity must ensure that it adheres to any requirement within this guideline.

12. Outsourcing

12.1. An Entity that outsources any activity to support its operations when developing, providing, using, or implementing an AI System should ensure regular due diligence on the outsourcing service provider is carried out (identity, legal status, activities, financial position, etc.) and obtain prior consent from QCB.

12.2. An Entity must conduct a due diligence review on the capabilities and expertise of the outsourcing service provider prior to its selection.

12.3. An Entity should conduct a risk assessment of the outsourcing service provider, including the location of the data when it is processed, stored, and transmitted, and any relevant vendor contracted by the third party.

12.4. An Entity must periodically review the suitability and performance of the outsourcing service providers.

12.5. An Entity must obtain approval from its Board of Directors to outsource any function in relation to the use of AI and must document it.

12.6. An Entity must put in place proper mechanisms to ensure the confidentiality and security of information that the outsourcing service provider may have access to.

12.7. An Entity must put in place proper reporting and monitoring mechanisms to ensure that the integrity and quality of work conducted by the outsourcing service provider is maintained.

12.8. The external and internal auditors of the Entity must be able to review the accounting records and internal controls of the outsourcing service provider.

12.9. An Entity must also have a contingency plan in the event that the arrangement with the outsourcing service provider is suddenly terminated.

12.10. An Entity must have a service agreement with the outsourcing service provider. The service agreement should be comprehensive and contain minimum the following clause:

12.10.1. The right to monitor and be informed about the outsourcing service provider's compliance with applicable laws, regulations, international standards (wherever applicable) and to require timely remediation if issues arise.

12.10.2. A clause on professional ethics and conduct in performing their duties.

12.10.3. Clearly defined roles and responsibilities of the outsourcing service provider.

12.10.4. Robust confidentiality and security procedures and controls.

12.10.5. Sound business continuity management procedures.

12.10.6. The Entity has the right to terminate the services of the outsourcing service provider if it fails to comply with the conditions imposed or is directed by QCB to do so.

12.10.7. Inclusion of exit clauses that ensure any data will be wiped out upon termination of the outsourcing.

12.10.8. QCB right to audit the outsourcing service provider's accounts.

12.11. An Entity shall be responsible as the principal for all the acts of omission or commission of their outsourcing service providers.

PART C (HUMAN OVERSIGHT OF AI IN USE)

13. Human Oversight of AI

13.1. Any AI Systems must have a Human Oversight protocol.

13.2. High risk AI Systems must be designed and developed in such a way, including with appropriate human-machine interface tools, that they can be effectively overseen by natural persons during the period in which the AI System is in use.

13.3. The User must assign Human Oversight to a Supervisor who has the necessary competence, training, and authority to operate or oversee the relevant AI System.

13.4. An Entity must ensure that the Supervisor is given tools and authority as appropriate and proportionate to the circumstances to:

13.4.1. Understand the capacities and limitations of the High-Risk AI System and are able to duly monitor its operation.

13.4.2. Correctly interpret the High-Risk AI System's output, considering for example the interpretation tools and methods available.

13.4.3. To decide, in any situation, not to use the High-Risk AI System or otherwise disregard, override or reverse the output of the High-Risk AI System.

13.4.4. Have the authority and means to intervene in the operation of the High-Risk AI System or interrupt the system through a "stop" button or a similar procedure.

13.5. **Fully Autonomous AI (Non-High Risk):**

13.5.1. Where an Entity uses an AI System that has no Human Oversight of the execution of decisions, and the AI has full control of activity with no option for human override then, even if the system is viewed as low or no risk, the Entity must provide very detailed information to support the use of such a system for QCB approval.

13.6. **Fully Autonomous AI (High Risk):**

13.6.1. An entity that plans to provide or use a High-Risk AI System that has no Human Oversight of the execution of decisions must obtain prior QCB approval before launching and will be expected to notify QCB as soon as such a system is being actively considered or developed.

13.6.2. The AI System must have built in guard rails or specific limits that the AI cannot override.

13.6.3. Entities must review the guard rails and specific limits on a frequent set schedule or in response to external volatility spikes.

13.6.4. Entities must set in-built limits and link to warning levels or auto-close routines.

13.6.5. The Supervisor(s) must have the capacity to close the system down in the event outputs from or data around the system seems aberrant.

13.7. **Human Exception Monitoring:**

13.7.1. An entity that plans to provide or use an AI System that requires Human Oversight in a monitoring role, with the ability to take over control must ensure there will be appropriate human-machine interface tools the ability to allow a Supervisor to take over control.

13.7.2. Human monitoring must provide information that a Supervisor can respond to in a manageable time frame to adjust parameters during the operation of the Algorithm.

13.7.3. An Entity may ensure the design and development of AI Systems in such a way that it allows a Supervisor to oversee the AI Algorithm's functioning and allow decision making in a timely manner.

13.7.4. An Entity must ensure that appropriate Human Oversight measures should be in place before use.

13.7.5. An Entity must ensure an AI System is subject to built-in operational constraints that cannot be overridden by the system itself.

13.7.6. An Entity must ensure the AI System is responsive to the Supervisor.

13.8. **AI Assisted Human-Decision Making:**

13.8.1. An Entity must have Operators who are trained to be able to interpret AI generated output where that output is of a nature that can be used by Operators to make decisions.

PART D (AI LIFE CYCLE MANAGEMENT)

14. Approvals of AI System training and testing

14.1. For any new High-Risk AI Systems, an Entity must submit the full results of the training, validation, and testing of the system to QCB for approval.

14.2. An Entity that is a User of AI Systems must submit the instructions received from the Provider for use of the AI System and the Providers technical and training results to QCB.

14.2.1. The User must establish internal procedures to ensure such information is used by the User itself.

14.2.2. The User must provide the results of its own use testing and its specific data sources or other inputs and Human Oversight plan.

14.3. If a User Entity makes any material change to an AI Model with a view to placing it on the market or putting it into service under its own name or trademark it will be considered a Provider and the requirements with respect to Providers in this Guideline will apply to that Entity.

15. AI Data Governance

15.1. An Entity must ensure it can manage an AI System over its Life Cycle, either directly or via contractual provision by a Provider. The management of the AI System over the product Life Cycle is the responsibility of the Provider. An Entity may be a Provider of an AI System directly. A Provider is expected by contract to provide all the data from development, testing, pre and post-market introduction and regular performance testing, and system development.

15.2. The Entity must make available to QCB the full range of data an AI Provider is contractually obligated to provide to the Entity.

15.3. An Entity should ensure it has different Data Sets for training, validation, and testing.

15.4. The Entity must use the Training Data and Validation Data to train the AI System. Such data should be subject to internal data quality control procedures.

15.5. An Entity may ensure the model is reviewed to identify any unintuitive or false causal relationships. The validation may be carried out by an independent function within an Entity or by an external organization.

15.6. The Entity must use the test data to determine the accuracy of the AI System.

15.7. The Entity must ensure the model is checked for systematic Bias by testing it on different demographic groups to observe whether any groups are being systematically advantaged or disadvantaged.

15.8. An Entity should adopt an effective data governance framework specifically designed for AI to ensure that data used by the AI Model is accurate, complete, consistent, secure, and provided in a timely manner for the AI System to function as designed. The framework should document the extent to which the data meets an Entity's requirements for data quality, gaps in data quality that may exist and steps an Entity will take, where possible, to resolve these gaps over time.

15.9. An Entity that develops high risk systems should use techniques involving the training of models with data developed on the basis of training, validation and Testing Data Sets when:

15.9.1. An Entity's training, validation, and Testing Data Sets must be subject to appropriate design choices, data governance and management practices. Those practices must concern, the following:

15.9.1.1. Data collection processes.

15.9.1.2. Relevant data preparation processing operations, such as annotation, labelling, cleaning, enrichment, and aggregation.

15.9.1.3. The formulation of relevant assumptions related to the Entity's ability to acquire suitable data sets to allow the development of systems, notably with respect to the information that the data are supposed to measure and represent.

15.9.1.4. A prior assessment of the availability, quantity and suitability of the Data Sets that are needed.

15.9.1.5. Examination in view of possible Biases that are likely to affect health and safety of natural persons or lead to discrimination.

15.9.1.6. The identification of any possible data gaps or shortcomings, and how those gaps and shortcomings can be addressed.

15.10. An Entity should ensure Testing Data Sets are sufficiently relevant, representative and have the appropriate statistical properties, including as regards the Customers of whom the AI System is intended to be used (i.e., how relevant the data and inferences drawn from the data are to the AI System.

15.11. An Entity should ensure the Data Sets are as free of errors and complete as possible in view of the intended purpose of the AI System and sourced from reputable vendors.

15.12. An Entity should, where relevant, conduct rigorous, independent validation and testing of material trained AI Models to ensure the accuracy, appropriateness, and reliability of the models prior to deployment.

15.13. An Entity should ensure the model is reviewed to identify any unintuitive or false causal relationships. The validation may be carried out by an independent function within an Entity or by an external organization.

15.14. An Entity must ensure that the data used to develop AI Systems is of high quality especially when techniques involving the training of models are used, with a view to ensure that the AI System performs as intended and safely and it does not become the source of discrimination.

15.15. To the extent that it is strictly necessary for the purposes of ensuring Bias monitoring, detection, and correction in relation to the High-Risk AI Systems, the Providers of such systems may process personal data, subject to compliance with the Qatar Law No. (13) of 2016 on Personal Data Privacy Protection. To the extent feasible, using of security and privacy-preserving measures, such as pseudonymization, or encryption where anonymization is used.

16. Framework for High-Risk AI Management

16.1. Where an Entity is the User or Provider of a High-Risk AI System it must put a framework in place that ensures compliance with this guideline. It must be documented in a systematic and orderly manner in the form of written policies, procedures, and instructions, and must include at least the following aspects:

16.1.1. A framework for regulatory compliance, including compliance with QCB procedures for how to manage or modify High-Risk AI Systems.

16.1.2. Techniques, procedures, and systematic actions to be used for the design, design control and design verification of a High-Risk AI System.

16.1.3. Techniques, procedures, and systematic actions to be used for the development, quality control and quality assurance of the High-Risk AI System.

16.1.4. Examination, testing and validation procedures to be carried out before, during and after the development of the High-Risk AI System, and the frequency of post-launch reviews.

16.1.5. Systems and procedures for data management, including data collection, data analysis, data labelling, data storage, data filtration, data mining, data aggregation, data retention and any other operation regarding the data that is performed before and for the purposes of the placing on the market or putting into service of High-Risk AI Systems.

16.1.6. The setting-up, implementation and maintenance of a Monitoring System.

16.1.7. Systems and procedures for record keeping of all relevant documentation and information.

16.1.8. Resource management, including security of supply-related measures.

16.1.9. An accountability framework setting out the responsibilities of the management and other staff.

16.2. The implementation of aspects referred to in clause (16.1) must be proportionate to the size of the Provider's organization and use of High-Risk AI.

17. AI Security

17.1. An Entity must comply with the Sector-Specific Security Regulation in all its deployment of AI solutions.

17.2. An Entity must develop a program for AI Trust, Risk and Security Management (AI TRiSM). The program must include:

17.2.1. Toolsets for content anomaly detection.

17.2.2. Toolsets for data protection from Providers and other third-parties.

17.2.3. Toolsets for third-party system security.

17.2.4. Policy for the acceptable use of AI.

17.2.5. Processes for assessment of privacy, fairness and bias.

17.3. An Entity's TRiSM program must ensure that AI Providers adhere to their program which includes:

17.3.1. Utilizing defined AI Model management processes.

17.3.2. Building AI Models with defined controls against security breaches.

17.4. An Entity must examine any AI Model's attack surface prior to deployment, and address any security findings.

17.5. An Entity must ensure that its AI model is protected from integrity related attacks to prevent model manipulation.

17.6. An Entity must ensure that the AI model is protected against query attacks that may lead to model manipulation or theft.

17.7. An Entity must ensure that the AI model is protected against prompt injections that may lead to data poisoning or data drift.

17.8. An Entity that utilizes AI must deploy a Data Loss Prevention (DLP) tool to protect against sensitive data loss.

17.9. An Entity that utilizes AI must deploy tools for content anomaly detection.

18. Documentation

18.1. An Entity should maintain documentation outlining the design of the AI Model, whether in the role of Provider or User, including but not limited to, where applicable:

18.1.1. The Input Data source and data description (types and use of data) as per the AI data governance above.

18.1.2. The data quality checks and data transformations conducted.

18.1.3. Reasons and justifications for specific model design and development choices.

18.1.4. Methodology or numerical analyses and calculations conducted.

18.1.5. Results and expected outcomes.

18.1.6. Quantitative evaluation and testing metrics used to determine soundness of the model and its results.

18.1.7. Model usage and implementation.

18.1.8. Form and frequency of model validation, monitoring and review.

18.1.9. Assumptions or limitations of the model with justifications.

19. Monitoring

19.1. An Entity must support the Monitoring Systems and plans for High-Risk AI Systems. This means for its own AI Systems but also accessing the information provided of all activities carried out by Providers of AI Systems to collect and review experience gained from the use of AI Systems.

19.2. The Entity must ensure the compliance of the Provider to its obligations to evaluate the conformance to the predicted model outcomes of AI Systems throughout their Life Cycle, the Monitoring System must collect, document, and analyze relevant data, which may be provided by Users, or which may be collected through other sources on the performance of High-Risk AI Systems.

19.3. The Entity should maintain records of its experience with AI Systems which are auditable and where relevant and considering the type of system used, should maintain on-going and up-to-date information through:

19.3.1. Establishing audit logs and maintaining traceability of decisions and outcomes of the AI System.

19.3.2. Developing and maintaining design documentation.

19.3.3. Maintaining records of the various versions of the model including its code should establish a robust system for versioning and then maintaining a record of each version of the AI Model.

19.3.4. Archiving original Data Sets used to develop, re-train or calibrate models.

19.4. When an Entity has a high-risk or Material AI Portfolio technical or model related error or failure, an Entity should establish a process to review the error and rectify it, withdraw it or recall it in a timely manner, which may include notifying another function.

19.5. In the event of a serious incident, the Entity should report the matter to QCB immediately after the Provider has established a causal link between the AI System and the serious incident or the reasonable likelihood of such a link.

PART E (INTERACTIONS WITH CUSTOMERS)

20. Customer Information and Consent

20.1. An Entity must notify Customers when they are interacting with an AI System.

20.2. An Entity must be transparent with Customers about their use of AI through their conduct and through accurate, understandable, and accessible plain language disclosure.

20.3. An Entity should ensure that Customers are informed of products and/ or services that utilize AI, the associated risks, and limitations of the technology:

20.3.1. Prior to providing the service initially (for non-high-risk systems like chatbots).

20.3.2. Each update of an AI System will be treated as a new version requiring Customer notification.

20.3.3. Use of AI can be disclosed in the general product description or terms of use in line with clause (17.2).

20.3.4. Each time Customers (or employees) interact with the service for High-Risk AI like credit, insurance, or employee issues.

20.4. An Entity must provide information to Customers how to use the AI System and ensure Customers always have access to the instructions.

20.5. An Entity must provide clear explanations of the types of data, types of variables and factors that influence the decision-making process used by AI Systems upon Customers' request.

20.6. An Entity must disclose the manner in which an AI decision may affect an individual Customer, and whether the decision is reversible.

20.7. An Entity, when offering High-Risk AI Systems, will prompt the Customer to check their personal information including financial data is up to date.

20.8. An Entity will provide a visible and accessible feedback channel for questions or comments.

20.9. An Entity should collect Customer consent to acceptance of the risks associated with the use of AI prior to providing the service. For non-high-risk AI Systems this could be a one-time event as above or in general terms of use.

20.10. An Entity does not need to disclose intellectual property, publishing of proprietary source code or details on Entity's and the Provider's internal processes.

20.11. The use of AI and model details used to detect security issues such as fraud and identity theft are excluded from disclosure requirements.

21. Customer Rights and Recourse

21.1. An Entity must put in place a mechanism for Customers to raise inquiries about AI decisions and request reviews of decisions made by AI Systems with no human intervention.

21.2. An Entity must offer the Customer a two-choice process where the Customer may supply data to alter the system and resubmit to the AI System, or they may request a review of a negative AI decision by a qualified human-decision-maker.

21.3. Any subsequent complaint by an aggrieved Customer must be handled through standard customer complaint processes.

22. Option to Opt-out

22.1. An Entity should consider whether to provide Customer with the option to opt out from the use of the AI product or service, and whether this option should be offered by default or only upon request. Relevant considerations include:

22.1.1. Degree of risk or harm to the Customer.

22.1.2. Reversibility of the decision made.

22.1.3. Availability of alternative decision-making mechanisms.

22.1.4. Cost or trade-offs of alternative mechanisms.

22.1.5. Complexity and inefficiency of maintaining parallel systems.

22.1.6. Technical feasibility.

22.2. Where an organization has weighed the factors above and decided not to provide an option to opt out, it must provide other modes of recourse to the Customer such as providing a channel for reviewing the decision.

23. Exemptions

23.1. An Entity seeking an exemption from any requirement within this guideline must request it from QCB. All exemptions are subject to QCB approval.

23.2. An Entity must link its exemption request to a specific requirement in this guideline from which it is seeking a waiver.

23.3. An Entity must support its exemption request with a clear and documented business case or rationale.

23.4. An Entity must ensure that the appropriate individuals or levels of authority within the Entity consistently approve the exemption.

23.5. An Entity must duly record in the Entity's exemptions Register any approved exemptions and assign an expiration date – the date by which the exemption will be mitigated or resolved by the Entity seeking the exemption.

23.6. An Entity must remain accountable for any risks stemming from approved exemptions.

PART F (COMPLIANCE WITH SECONDARY REGULATIONS)

24. Compliance with Secondary Regulations

24.1. Along with the QCB Law and this guideline, an Entity must also comply with the below mentioned secondary regulations, and subsequent amendments, while operating in Qatar:

24.1.1. Sector-Specific Security Regulation.

24.1.2. Law No. (13) of 2016 on Personal Data Privacy Protection.

24.1.3. Technology Risks Circular, January 2018 issued by QCB.

24.1.4. Cloud Computing Regulation 2024 issued by QCB if entity is leveraging cloud-based AI solutions.

24.1.5. Regulations or guidelines issued by QCB, including those related to emerging technologies.