الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

هيئة قطر للأسواق المالية
Qatar Financial Markets Authority
State of Qatar • دولة قطر

Compliance Controls of the National Information Assurance (NIA) for Financial Market Participants

[IAS-FIN-NFMP]

Standard

Complementary to National Information Assurance Standard V2.1 – Normative Controls specific for Financial Market Participants

Qatar Financial Markets Authority

National Cyber Security Agency (NCSA)

March 2026

V 1.0

DISCLAIMER / LEGAL RIGHTS

Qatar Financial Markets Authority (QFMA) and National Cyber Security Agency (NCSA) has designed and created this publication, titled "Compliance Controls of the National Information Assurance (NIA) for Financial Market Participants" - V 1.0 - Public, in order to help Financial Market Participants, understand cyber security risks in the digital realm, and mitigate these risks by applying the security requirements identified in this document along with the National Data Classification Policy (NDCP) and the National Information Assurance Standard (NIAS).

QFMA and NCSA are responsible for the review and maintenance of this document.

Any reproduction of the present document either in part or full and irrespective of the means of reproduction; shall acknowledge QFMA and NCSA as the source and owner of the "National Information Assurance (NIA) for Financial Market Participants".

Any reproduction concerning this document with intent of commercialization shall seek a written authorization from the QFMA & NCSA. QFMA and NCSA shall reserve the right to assess the functionality and applicability of all such reproductions developed for commercial intent.

The authorization from QFMA & NCSA shall not be construed as an endorsement of the developed reproduction and the developer shall in no way publicize or misinterpret this in any form of media or personal / social discussions.

Document Control

Document Details	
Document ID	**IAS-FIN-NFMP**
Version	**V 1.0**
Classification & Type	**Public**
Abstract	**Security Controls for Financial Market Participants, An annexure to National Information Assurance Standard V2.1.**

Review/Approval

Name / Role	Department	Reviewed/Approved	Version	Date
The Official	Policies Affairs, NCSA		1.0	
	Qatar Financial Markets Authority		1.0	

Revision History

Version	Author (s)	Revision description	Date
1.0	QFMA & NCSA	Published V1.0 document	1.0

LEGAL MANDATE(S)

National Cyber Security Agency (NCSA)

Based on Amiri Decree No.1 for 2021 about the establishment of National Cyber Security Agency (NCSA), which aims to maintain and regulate national cyber security and to enhance and protect the vital interests of the state in the face of cyber threats, and according to Article No. (3) of the decree it is concerned with developing and updating policies, governance mechanisms, standards, controls and guidelines necessary to enhance cyber security in coordination with the concerned authorities, and circulating them with the relevant authorities and follow-up commitment to them.

The National Cyber Security Strategy 2.0, Pillar 2 – Legislation, Regulations & Law Enforcement for a Secure Cyberspace, SO 1 – Develop appropriate legal & regulatory frameworks, Initiative 4 – Develop cyber security regulatory frameworks for the latest emerging technology trends, further strengthens the mandate of NCSA as the competent authority to publish relevant cyber security policies, standards, frameworks, and guidelines.

And within this context, this National Information Assurance for Financial Market Participants has been developed which aims to regulate and govern the cyber security requirements for the Qatar Financial Market participants regulated by QFMA.

This is a complementary standard that must be used along with the National Data Classification Policy and the National Information Assurance Standard.

This standard has been developed based on the responsibilities assigned to NCSA as per Amiri Decree No.1 for 2021. In the event, a conflict arises between this document (specific provision or clauses) and the laws of Qatar, the latter (law), shall take precedence. Any such term (specific provision or clauses), to that extent shall be deemed omitted from this document, without affecting the remaining provisions of this document. Amendments in that case shall then be required to ensure compliance with the relevant applicable laws of the State of Qatar.

Qatar Financial Markets Authority

Qatar Financial Markets Authority (QFMA) was established by virtue of Law No. 33 of 2005, amended by the Amiri Decree of Law No. 14 of 2007 and Law No. 10 of 2009 as an independent supervisory and regulatory authority of financial markets in the State of Qatar. The QFMA has the powers necessary to regulate, control and supervise the financial markets.

Law No. 8 of 2012 regarding Qatar Financial Markets Authority, as amended by Decree-Law No. 22 of 2018, confirms the QFMA's independence and having all the powers required for conducting its regulatory, supervisory and control functions more effectively in compliance with the provisions of Law No. 33 of 2005, as amended.

Specifically, Article 29 within Law No. 8 of 2012, states that a person shall be eligible to conduct financial markets activities only after obtaining a license by the Authority stating the permitted activity or activities. The requirements, controls and procedures for granting licenses and the standards of practicing the activity shall be decided by the Board pursuant to the provisions of this law. Further Article 31, states that the Authority may, by written notice, issue instructions to financial markets and other persons subject to the Authority's jurisdiction. Financial markets and persons shall incorporate such instructions in their applicable rules and shall commit to observe them. The Authority may request such markets and persons to prepare or amend specific rules on their scope of work in a specified time. If they do not comply with the request or the timelines specified in the request, the Authority may, on their behalf, prepare or amend these rules and compel them to bear the cost.

The adoption and implementation of this standard is the full responsibility of the concerned organizations. NCSA and QFMA do not take any responsibility for any damages related to un-informed decision of adopting and implementing this standard.

Requirements Levels:

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as follows:

- SHALL: This word, or the terms "REQUIRED" or "MUST", mean that the definition is an absolute mandatory and baseline requirement of the specification.
- SHALL NOT: This phrase, or the phrase "MUST NOT", mean that the definition is an absolute prohibition of the specification.
- SHOULD: This word or the term "RECOMMENDED", mean that the definition is not a mandatory or baseline requirement. However, agencies shall consider them as additional controls for assets that have been classified as Medium or High in the Information Asset Classification exercise.
- MAY: This word, or the adjective "OPTIONAL", mean that an item is truly optional.

Tabel of Contents

1. Introduction 7
1.1. Context 7
2. Purpose, Scope, Usage and Authority 8
2.1. Purpose 8
2.2. Scope 8
2.3. Usage 8
3. Key Definitions 9
4. Risks, and Challenges 10
4.1. Risks 10
4.2. Challenges 10
5. Control Statements 11
Information Security Governance [IG] 11
Risk Management [RM]] 11
Third Party Security Management [TM]] 12
Security Awareness [SA] 12
Incident Management [IM]] 12
Business Continuity Management [BC]] 13
Logging & Security Monitoring [SM]] 13
Audit & Certification [AC]] 14
Software Security [SS] 14
Access Control Security [AM] 15
6. Compliance and Enforcement 15
6.1. Compliance and Enforcement 15
6.1.1. Compliance Process 15
6.1.2. Roles and Responsibilities 15
6.2. Transitioning and effective date 16
6.2.1. Effective date 16
6.2.2. Transition period 16
6.3. Exceptions and deviations 16
6.3.1. Exceptions to Standard Requirements 16
6.3.2. Deviation process from Standard Requirements 16
7. Appendix 17
7.1. Acronyms 17
7.2. RTS 6/7 algorithmic trading principles, translated into clear, auditable control objectives mapped directly to NIA v2.1 17
7.3. References 18
7.4. List of Figures 18
7.5. Table of Tables 18

1. Introduction

1.1 Context

Today we live in a connected world, where most of the services that we use are available online. Whilst this has provided numerous benefits and ease of living, it has also opened up a whole new surface area of attacks. The biggest threat is to the online financial services that we use.

Cyber Risk is now acknowledged as amongst the top 5 threats by leading global bodies such as the World Bank and the World Economic Forum amongst others.

Financial systems are amongst the systems at highest risk predominantly because of the financial gains it provides to the criminals and in general the impact it has on the public. It is therefore imperative that we acknowledge the risks and take actions to mitigate these risks.

To this end, Qatar Financial Markets Authority, proposes to adopt the National Data Classification Policy and the National Information Assurance Standard, along with this complementary standard to bolster the cybersecurity maturity of participants operating within the Qatari Financial Markets.

2. Purpose, Scope, Usage and Authority

2.1. Purpose

The purpose of this standard is to provide an overview of key cyber risks involved in financial market trading and identify adequate safeguards and controls. This standard complements the NIAS v2.1 and aligns with the international standard IOSCO. The standard is intended to be used to certify organizations in financial markets.

2.2. Scope

The scope of this standard cover's participants in the Qatari financial market regulated by QFMA. Further, this standard applies to individuals, processes, and systems related to market trading, monitoring, and client applications.

2.3. Usage

The organizations in the Qatari financial market regulated by QFMA, shall implement and certify against this standard to demonstrate their cyber security compliance to QFMA and provide assurances to their customers.

Participants shall note that this document must not be considered in isolation. Compliance shall be achieved through integrated adherence to this document, the National Data Classification Policy, and the National Information Assurance Standard.

The requirements mentioned in this standard (Section 5), along with those mentioned in Appendix 7.2 are mandatory. Further, wherever this standard state that a control in NIA v2.1, 'shall be extended', such extension applies only within the scope of Financial Market Participants and does not modify the baseline NIA v2.1 text.

Lastly, this compliance does not constitute assurance of any artificial intelligence (AI) models or AI enabled systems in use. Where assurance of AI models or systems is required, certification against ISO/IEC 42001 may be used to demonstrate assurance up until such time that QFMA or the NCSA does not produce its own relevant standard.

3. Key Definitions

Organization	Refers to any business/non-business entity operating in the State of Qatar and regulated by QFMA.

4. Risks and Challenges

4.1. Risks

The following section takes a holistic look at the risk landscape from a financial market perspective.

a. Unavailability of the Exchange and Market Infrastructure:

The exchange and market infrastructure are very sensitive to computing delays, which can lead to trades being not executed or fulfilled. Unavailability of the platform can affect index prices, ETFs, derivatives, and all instruments pegged to those markets, triggering knock on risks in margining and risk models, leading to huge monetary losses. Cyber-attacks can make trading systems slow or unavailable—e.g., DDoS on exchange gateways, market data feeds, or order routing infrastructure.

b. Loss of Integrity

The market and trading platforms are very sensitive since it deals with money and financial information of the participants, namely the brokers and customers who trade on the platform, it also has an impact on the companies which are traded in the market. As such it is very important to maintain the integrity of the system. Any attack that compromises the integrity of the systems by way of tampering with price/volume data, order books, or trade confirmations without necessarily taking systems down may undermine market integrity and open the door to undetected market abuse.

Such attacks may also occur due to compromise of trading algorithms and smart order routers or manipulation of high frequency trading (HFT) algorithms, execution algos, or risk-check engines.

c. Supply Chain Risk (Vendors, Cloud, and Third Parties)

Our dependence on digital services providers means that if a vendor is compromised, the problem becomes acute if there is concentration in a few market data or technology providers leading to sector wide outages

d. Risks due to Emerging technology such as AI

The unbridled and unregulated use of emerging technology such as AI, can pose the risk of loss of confidence, leading to financial impacts. Such risks may manifest by way of ability of technology such as AI, to manipulate the market by way of harder to detect spoofing, layering, and pump and dump behavior, Algorithmic “herding” in response to manipulated signals, magnifying price swings.

4.2. Challenges

Some of the key challenges facing financial markets is the need to maintain integrity of its system, trust of its customers, whilst defending its complex, multi stakeholder IT systems, against diverse cyber threat vectors.

5. Control Statements

Information Security Governance [IG]

To meet the requirements of this domain, Organizations MUST:

CCMP-IG 01:

Establish a Cybersecurity Steering Committee (CSC) responsible for overseeing the organization's cybersecurity strategy, governance, and risk management.

a. Ensure that the CSC is chaired by a senior executive and includes representatives from IT, risk management, legal, compliance, and business units to ensure cross-functional oversight.

b. Define and document the CSC's mandate, including roles, responsibilities, authority, and decision-making processes to ensure clear accountability and effective governance

c. Conduct periodic cybersecurity risk assessments and strategy reviews, with findings reported to senior management and the Board of Directors (where applicable).

d. Meet at least once every quarter with the senior management and the board to review cybersecurity incidents, compliance status, threat intelligence, and overall cybersecurity posture.

CCMP-IG 02:

Define and Measure relevant metrics across various control domains to assess the information security maturity of the organization and track their growth on a YoY basis.

CCMP-IG 03:

Report the progress on information security maturity to the leadership, through the Cyber Security Steering committee. Organizations may use tools such as cyber resilience score cards to report the progress.

Risk Management [RM]

To meet the requirements of this domain, Organizations MUST:

CCMP-RM 01:

The control RM 5 in Chapter 4 Section 2 Risk Management [RM], shall be extended to include a Risk Assessment on a minimum annual basis for all systems related to market trading, monitoring, and customer facing APIs.

CCMP-RM 02:

Ensure that any technology adopted within the business (esp. market trading, monitoring, and customer facing APIs.) is evaluated for potential security risks. Any new technology is implemented using a "Security by Design" philosophy and necessary controls are integrated to mitigate any potential risks to the system.

Third Party Security Management [TM]

To meet the requirements of this domain, Organizations MUST:

CCMP-TM 01:

The control TM 5 in Chapter 4 Section 3 Third Party Security Management [TM], shall be extended to include a Third-Party Security audit on a minimum annual basis for all systems related to market trading, monitoring, and customer facing APIs.

CCMP-TM 02:

Monitor third-party performance and data flows for anomalies.

CCMP-TM 03:

Ensure that the third-party vendor, complies with the contractual and regulatory requirements including but not restricted to data transfers, and that such compliance is monitored using tools such as automated dashboards.

Security Awareness [SA]

To meet the requirements of this domain Organizations MUST:

CCMP-SA 01:

Provide skills-based trainings as necessary to equip the IT and Information Security team with the skills necessary to align with job roles and responsibilities. The trainings shall be updated to address the change in technology and the threat landscape amongst other things.

Incident Management [IM]

To meet the requirements of this domain, Organizations MUST:

CCMP-IM 01:

Develop detailed playbooks for handling critical threats such as but not limited to algorithm manipulation, participant outages, and data breaches in systems related to market trading environments.

CCMP-IM 02:

The control IM 8 in Chapter 4 Section 8 Incident Management [IM], shall be extended to state "Report all Critical incidents to QFMA and NCSA within two (2) hour of incident identification".

CCMP-IM 03:

Incorporate lessons learned from previous incidents to enhance the overall security framework including people, processes, and technology.

Business Continuity Management [BC]

To meet the requirements of this domain, Organizations MUST:

CCMP-BC 01:

The control BC 2 in Chapter 4 Section 9 Business Continuity Management [BC], shall be extended to state "An active-active configuration with failover capabilities shall be implemented for all systems related to market trading, monitoring, and customer facing APIs.".

CCMP-BC-02:

The control BC 8 in Chapter 4 Section 9 Business Continuity Management [BC], shall be extended to state "Conduct at least two unplanned (only a restricted set of individuals will be notified of the drill) BCM drills, on an annual basis, such that at least one of them will be a full simulation test, where all activities will be relocated from the original site to the failover site, with full participation of all stakeholders involved (employees, outsourced staff, vendors, auditors etc.). The other drill could be a table top drill or a subset of the full drill, where certain components of the BCP are tested based on criticality or results of the full simulation.

Logging & Security Monitoring [SM]

To meet the requirements of this domain, Organizations MUST:

CCMP-SM 01:

Monitor and secure market trading environments, by pro-actively conducting vulnerability scans.

a. Such vulnerability scans should be conducted on a minimum monthly basis.

b. Identified vulnerabilities shall be evaluated and a mitigation plan shall be defined and executed based on the risk assessment.

c. Any patches / updates shall be applied as per the change management plan.

d. Critical vulnerabilities shall be addressed within a risk-defined timeframe, with 72 hours as the target for internet-facing or actively exploited vulnerabilities.

CCMP-SM 02:

Develop processes, tools, or mechanisms as appropriate to detect rogue algorithms or programs that may manipulate the market. Responsibility for detection and termination of rogue algorithms shall be proportionate to the participant's role. Exchanges shall ensure market-level safeguards, while brokers shall ensure controls within systems under their operational control.

CCMP-SM-03:

Develop and integrate automated kill-switch functionality to terminate such rogue applications for immediate response.

CCMP-SM 04:

Participate in industry/sector bodies such as FS-ISAC (Global) and integrate external cyber threat feeds into the enterprise threat monitoring systems.

CCMP-SM-05:

Utilize the information available to enhance the situational awareness, and defensive measures for proactive defenses.

CCMP-SM 06:

Collaborate with peers within the sector and the sector regulator to share threat intelligence, insights and best practices related to information security to enhance and develop the cyber maturity of the sector.

Audit & Certification [AC]

To meet the requirements of this domain, Organizations MUST:

CCMP-AC-01:

Develop a unified compliance framework that includes applicable regulations such as the National Data Classification Policy, National Information Assurance Standard, Personal Data Privacy Protection Law, sectorial regulations, and any other applicable global regulations to ensure consistent monitoring and reporting across jurisdictions.

Software Security [SS]

To meet the requirements of this domain, Organizations MUST:

CCMP-SS 01:

The control SS 5 in Chapter 5 Section 6 Software Security [SS], shall be extended to state that algorithms used in systems related to market trading, monitoring, and customer facing APIs are designed, implemented, and operated in a manner that ensures market integrity and resilience against cyber-attacks. Further, such algorithms shall implement documented pre-trade controls, post-trade monitoring, and emergency controls (including kill-switch functionality) to prevent disorderly trading, market manipulation, or unintended behavior.

CCMP-SS 02:

The control SS 5 in Chapter 5 Section 6 Software Security [SS], shall be extended to state that systems related to market trading, monitoring, and customer facing APIs shall be adequately stress tested. Accordingly, significant entities (e.g. exchanges, CCP=connected brokers) shall stress test critical market infrastructure up to 8 - 10x of their peak trading volumes, while other brokers may apply stress testing to at least 2-3x of their documented peak load.

Access Control Security [AM]

To meet the requirements of this domain, Organizations MUST:

CCMP-AM-01:

Monitor user behavior, focusing on unusual access patterns, and data exfiltration attempts, amongst other things whilst using systems related to market trading, monitoring, and customer facing APIs.

6. Compliance and Enforcement

6.1. Compliance and Enforcement

This complementary standard provides additional security requirements and controls necessary for implementing an Information Security Management System for participants in the financial markets regulated by QFMA. These controls are in addition to controls in National Information Assurance Standard v2.1.

6.1.1. Compliance Process

Entities regulated by QFMA shall note that this document shall not be considered in isolation. This complementary standard shall be complied with along with the National Data Classification Policy (NDCP) and the National Information Assurance Standard (NIAS). The compliance shall be demonstrated by way of certification to NIAS along with this standard.

6.1.2. Roles and Responsibilities

NCSA and QFMA are responsible for enforcing and monitoring compliance to this standard. Any changes/updates to this standard will be jointly developed by NCSA and QFMA. QFMA will be responsible for enforcing this standard to its regulated entities. Organizations regulated by QFMA will demonstrate their compliance to the standard by obtaining and maintaining the certification. The certification scheme will be developed and implemented by NCSA.

QFMA is the competent authority to resolve any queries that you may have about this complementary standard.

6.2. Transitioning and effective date

6.2.1. Effective date

The standard is effective from the date of official publication of this standard.

6.2.2. Transition period

Qatari financial markets regulated Organizations shall be provided with a transition period of twelve (12) months from the effective date of publication to demonstrate their roadmap to comply with this standard.

6.3. Exceptions and deviations

6.3.1. Exceptions to Standard Requirements

All the requirements stated in this standard (Section 5), along with Appendix 7.2 are mandatory. However, it is possible that the organizations may be forced to deviate from certain security requirements specified in this standard on the following grounds:

Safety and Operability considerations – any situation created if, by following a particular security requirement, may lead to endangering the human lives or significantly and negatively impacting the operations of the organization and its systems.

Business Constraints considerations – the current technology (legacy) or the business process requirements does not allow for the specific security requirements or configuration to be applied or may require significant financial costs or resources that may not be proportional or acceptable or the system is in the process of being upgraded/replaced.

6.3.2. Deviation process from Standard Requirements

In the above cases, the deviation shall be documented, a Risk Assessment shall be conducted to ascertain the risks due to non-application of the specific requirement. The organization shall identify and implement alternative or compensating controls to be put in place. If alternative or compensating controls are also not possible, the organization shall record this deviation as un-mitigated residual risk.

The deviation and the associated risk shall be reported to (communicated) and signed off (acknowledged and accepted) by the organization's senior management. The sign off shall be done by either the Head of the organization or the person authorized and delegated by the Head of organization, or the Head of the Risk Management, or the Head of Internal Audit. Lastly, this deviation along with the mitigation plan shall be communicated to QFMA through official correspondence channels. Based on this information, the QFMA will review the exception request and provide its approval or rejection.

If the exceptions are related to NDCP or NIAS, the organization will follow a similar process except that, QFMA shall provide its decision in coordination with National Cyber Security Agency (NCSA).

7. Appendix

7.1. Acronyms

IOSCO	International Organization of Securities Commissions

7.2. RTS 6/7 algorithmic trading principles, translated into clear, auditable control objectives mapped directly to NIA v2.1

Purpose

This Annex defines specific, auditable control objectives applicable to algorithmic trading systems, market monitoring platforms, and customer-facing trading APIs.

The objective is to ensure market integrity, operational resilience, and cybersecurity assurance in alignment with NIA v2.1, while maintaining proportionality based on the organization's role and systemic impact.

Scope of Applicability

These controls objectives apply to:

- Trading algorithms used for order generation, routing, execution, or optimization
- Automated trading components embedded within OMS, EMS, or API platforms
- Surveillance systems monitoring algorithmic or high-frequency trading activity

Applicable entities include:

- Exchanges and market operators
- Licensed brokers and trading members
- Third-party vendors providing algorithmic trading platforms or components (where applicable)

Control	Objectives	Requirements	Mapping to NIAS v2.1
Governance & Accountability	Algorithmic trading systems shall operate under clear governance, ownership, and accountability structures.	• Formal assignment of ownership for each trading algorithm • Defined approval authority for algorithm deployment and modification • Board or senior management oversight of algorithmic trading risk	• IG – Information Security Governance • RM – Risk Management
Secure Design & Change Management	Trading algorithms shall be securely designed, tested, and deployed using controlled and auditable processes.	• Secure development lifecycle for algorithmic logic • Pre-deployment testing in controlled environments • Formal change management for logic, parameters, and configurations • Segregation of development, testing, and production environments	• SS - Software Security • Application & Software Security • Operations Security and CM - Change Management • System Hardening Controls
Pre-Trade Risk Controls	Trading algorithms shall include preventive controls to avoid disorderly trading and excessive market impact.	• Order size, price, and volume thresholds • Rate-limiting and throttling mechanisms • Prevention of self-trading and runaway execution	• SS – Software Security • AM – Access Control
Monitoring & Anomaly Detection	Algorithmic activity shall be continuously monitored to detect abnormal, unintended, or potentially manipulative behavior.	• Real-time monitoring of algorithm performance and trading patterns • Detection of deviations from expected behavior • Comprehensive logging for forensic and supervisory review	• SM – Logging & Monitoring
Emergency Controls (Kill-(Switch Capability	Organizations shall be able to immediately limit or stop algorithmic trading activity in the event of malfunction, compromise, or market disorder.	• Manual and/or automated suspension mechanisms • Defined escalation and authorization procedures • Tested response procedures integrated with incident management	• IM – Incident Management • BC – Business Continuity
Stress Testing & Capacity Resilience	Algorithmic trading systems shall demonstrate resilience under peak and stressed operating conditions.	• Stress testing aligned with risk profile and trading volumes • Testing of failure scenarios, latency sensitivity, and system saturation • Documented results and remediation actions	• BC – Business Continuity • RM – Risk Management
Third-Party & Vendor Dependencies	Where algorithmic trading systems are sourced from or supported by third parties, equivalent security and resilience controls shall be enforced.	• Security assessment of vendors providing trading algorithms or platforms • Contractual enforcement of control objectives • Ongoing monitoring of vendor performance and risk	• SM – Logging & Monitoring

Table 1 Mapping RTS 6/7 algorithmic principles to NIAS

7.3. References

Guidance on cyber resilience for financial market infrastructures, IOSCO, June 2016.

7.4. List of Figures

No entries found.

7.5. Table of Tables

Table 1 Mapping RTS 6/7 algorithmic principles to NIAS.

End of Document