QATAR FINANCIAL CENTRE

TOKEN SERVICE PROVIDER GUIDELINES

VERSION 1 – August 2024

مركز قطر للمال
Qatar Financial Centre

Qatar Financial Centre Authority ● PO Box 23245 ● Doha, Qatar
T: +974 4496 7777 ● F: +974 4496 7676 ● info@qfc.qa ● qfc.qa

Table of Contents

I. PURPOSE

The primary goal of the Qatar Financial Centre (QFC) Token Service Provider Guidelines (hereinafter referred to as "the Guidelines") is to provide a set of illustrative principles and standards designed to result in security, integrity, and reliability of services. These guidelines outline the essential policy, procedure, system, and control concepts necessary to manage and mitigate the risks. The overarching theme focuses on promoting a robust framework for cybersecurity, data protection, regulatory compliance, etc., facilitating a secure and resilient ecosystem.

These Guidelines are not intended to be exhaustive or to supersede any legal and regulatory requirements. They are meant to be applied alongside the relevant laws, any subordinate legislation enacted under such laws and additional guidelines that the QFC might issue periodically in accordance with the pertinent laws and subordinate legislation.

Token Service Providers (TSP) must also consider and adhere to the applicable requirements and regulations set forth by all relevant State authorities, including but not limited to the Qatar Central Bank (QCB), the Ministry of Commerce and Industry (MOCI), Ministry of Communication and Information Technology (MCIT), Qatar Financial Centre Regulatory Authority (QFCRA), Qatar Financial Centre Authority (QFCA) and any other regulatory body with jurisdiction over TSP and related activities within the State of Qatar. The Guidelines recognise the necessity for TSP to ensure compliance with a broader regulatory landscape, to fully address the legal and operational complexities inherent in the management and provision of Token services.

TSP should be able to explain the rationale for the standards they have implemented for purposes of these guidelines and to explain any points of departure from compliance with these guidelines.

II. SCOPE AND APPLICABILITY

These Guidelines are applicable to all service providers that engage in token services business in or from the QFC and is applicable based on the functions and activities of the TSP. The document covers scenarios ranging from routine operational activities to critical incident response measures. It is intended for use by various stakeholders within the organisation, including IT professionals, senior management, and compliance officers. Additionally, these guidelines are relevant to third-party vendors and partners who engage with or provide services to the organization.

III. RELATIONSHIP TO OTHER STANDARDS

This document references guidelines, international standards, and best practices (for example ISO, NIST, etc.), ensuring its flexibility and global relevance and applicability. The Guidance describes general regulatory requirements applicable across various authorities and supports adherence to sector-specific standards.

The Guidelines are structured to supplement and strengthen existing requirements & standards, rather than replace them.

The Guidelines will be subject to periodic review and update. Future revisions will consider changes in the environment, advancements in technologies, and feedback from the

implementation of these Guidelines, and by engaging with stakeholders (like clients and regulatory bodies).

1. GOVERNANCE AND OVERSIGHT

This section sets out guidance on establishing effective governance structures and oversight mechanisms for TSP to manage organisational risks. It suggests best practices for developing robust systems and controls. It also highlights the roles and responsibilities of the board and senior management in promoting a culture of risk awareness and ensuring organisational compliance and resilience.

1.1 Overview of Systems and Controls

1) System Implementation: TSP are encouraged to implement adaptable systems and controls which reflect the business scale and complexity.
2) Governance Framework: Establishing a governance and risk assessment framework that reflects the business's nature and activities is advisable. This framework should include defining goals and competency requirements for staff (employees, third party and contractors).
3) Risk Management Framework: The framework should have specific systems and procedures to mitigate risks which align with the organisation's operational characteristics and are consistent with best practices.
4) Lifecycle Management: Policies should encompass the entire lifecycle of governance, from planning and implementation to maintenance and evaluation.
5) Framework Maintenance: TSP should have comprehensive governance frameworks that are consistent with global standards.
6) Policy Update: There should be regular updates to policies, standards, and procedures and the updates should be frequent enough to remain relevant and effective.
7) Risk Assessment: Risk assessments should be approved by senior management, should be conducted regularly, and reviewed periodically to ensure risks remain within acceptable limits.
8) Compliance and Non-compliance: Processes should aim to ensure adherence to established policies and procedures and should include measures to address instances of non-compliance.

1.2 Roles and Responsibilities of the Board and Senior Management

TSP should ensure that the roles and responsibilities, particularly those of the Chief Information Officer (CIO), Chief Technology Officer (CTO), Head of IT, Head of Compliance and Chief Information Security Officer (CISO) or Head of Information Security, are defined and approved by the Chief Executive Officer (CEO) in accordance with the organisational and regulatory demands. TSP should also have policies and procedures for internal oversight across various divisions to ensure consistent adherence to compliance and risk management. A periodic review of the roles and responsibilities is recommended to ensure effective management.

1) Chief Information Officer (CIO) / Chief Technology Officer (CTO) / Head of IT

    a) Strategic Planning: Develop and oversee the strategic plan for technology to support its services, ensuring alignment with the organisation's overall business goals.

b) Technology Oversight: Ensure the effective deployment, management, and security of technology systems that support operations.
c) Innovation and Development: Lead the exploration and implementation of new technologies to enhance offerings and improve operational efficiency.
d) Risk Management: Work closely with the Chief Information Security Officer (CISO) to identify, assess, and mitigate risks.
e) Compliance and Governance: Ensure technology practices comply with relevant regulations and standards, coordinating with legal and compliance departments.
f) Budget Management: Manage the IT budget and investments in technology solutions, ensuring cost-effective resource allocation.
g) Promptly updating the Board on significant technology risks, incidents etc.

2) Chief Information Security Officer (CISO) / Head of Information Security

a) Security Strategy: Develop and implement a comprehensive Information Security strategy, aligning with organisational risk tolerance and compliance requirements.
b) Risk Assessment and Management: Conduct regular risk assessments to identify vulnerabilities in the infrastructure and operations and develop strategies to mitigate these risks.
c) Incident Response: Lead the development and execution of an Incident Response Plan for security breaches or other security incidents, resulting in rapid recovery and minimal impact.
d) Compliance and Audits: Ensure adherence to security policies and regulatory requirements, facilitate audits and compliance checks.
e) Awareness and Training: Promote security awareness among employees and ensure that staff are trained on security best practices and policies.
f) Vendor and Third-Party Security: Oversee the security of third-party vendors and partners, conduct due diligence, and monitor for compliance with security standards.

3) The Board of Directors of a TSP should

a) Maintain a Risk Management framework that addresses the specific risks.
b) Oversee the Risk Management function so that it independently evaluates risks.
c) Provide senior executives with the necessary authority and resources to manage risks.
d) Approve a risk appetite statement reflecting the level of acceptable risk.
e) Regularly review the Risk Management Strategy to ensure it remains relevant.

4) CEO Approval: Both roles, whether as a CIO/CTO/Head of IT or as a CISO/Head of Information Security, require formal approval from the Chief Executive Officer (CEO) for their appointment, ensuring alignment with the organisation's leadership and strategic direction.

5) Collaboration and Reporting: Maintain close collaboration between the CIO/CTO/Head of IT and the CISO/Head of Information Security, with regular reporting to the CEO and Board on technology and security matters, highlighting achievements, challenges, and strategic direction.

2. RISK MANAGEMENT FRAMEWORK

TSP can effectively manage and mitigate risks by implanting a robust Risk Management framework. Below section is to provide guidance to TSP.

2.1 Risk Identification

1) Methods and Tools: Implement a range of methods and tools to identify risks including automated monitoring systems and feedback from operations teams to get a complete picture of potential vulnerabilities or threats that could impact the organisation's operations and technological infrastructure. For example, ISO/IEC 31000 provides guidelines on risk management principles and practices.

2.2 Risk Assessment

1) Processes: Develop processes to systematically evaluate the severity and probability of identified risks. This evaluation should consider the potential impact of each risk on the organisation's operations, reputation, and financial health. Techniques such as risk matrices or scoring systems can be used to quantify and prioritise risks, making it easier to address them effectively. For example, TSP can refer to NIST SP 800-30 guidelines.

2.3 Risk Mitigation Strategies

1) Outline of Strategies: Create a detailed plan outlining strategies to mitigate identified risks. These strategies should include both technological solutions, such as encryption and secure access controls, and policy implementations, such as staff training and incident response procedures. The aim is to reduce the likelihood of risk occurrence and minimise its impact should it materialize. Standards like ISO/IEC 27001 outlines the requirements for an information security management system, which can guide TSP in the implementation of these strategies.

The risk management framework should be dynamic, allowing for regular updates as new risks emerge and existing risks evolve. It is crucial for TSP to maintain an adaptive approach to risk management, ensuring continuous protection of assets and compliance with applicable regulatory standards. TSP should encourage a culture of risk awareness at all organizational levels.

3. CYBERSECURITY

Effective cybersecurity is crucial for TSP to safeguard their operations and maintain the trust of their clients. The cybersecurity framework outlined below includes several key components, each addressing various aspects of security:

3.1 Cybersecurity Policies

1) Comprehensive Coverage: TSP should develop, document, and enact a comprehensive cybersecurity policy that covers all necessary areas, including access controls, threat detection, and response strategies. This policy must also be provided to regulatory bodies like the QFC or other authorities as part of the licensing process and upon request.

2) Annual Review: The cybersecurity policy should undergo an annual review and revision to ensure it stays current and effective, aligning with evolving industry standards and regulatory requirements.

3.2 Security Measures and Controls

The security measures and controls should be robust, meeting the highest industry standards.

1) Access Control: Implement strict access control measures to ensure that access to networks, systems, and data is restricted to authorized users only. This could include multi-factor authentication, least privilege access, and periodic access reviews.

   The principles of 'never alone,' 'segregation of duties,' and 'least privilege' should be implemented when granting staff access to information assets. No single individual should have the capability to perform sensitive system functions alone. Access rights and system privileges should be assigned based on the specific roles and responsibilities of staff, contractors, and service providers. TSP should also consider implementation of the use of zero-trust architecture as an advanced approach to enhance security. TSP can refer to industry standards like NIST SP 800-207.
2) Cyber Threat Intelligence: Actively participate in Cyber Threat Intelligence sharing platforms to enhance threat detection, prevention, and response capabilities.
3) Data Loss Prevention (DLP): To monitor, identify, and prevent the unapproved transport of sensitive data, TSP should put DLP solutions into place.
4) Endpoint Security and Antivirus: TSP should implement complete endpoint security solutions, which include antivirus and anti-malware software to shield from attacks. To protect against vulnerabilities, TSP should make sure that all endpoints receive regular updates with the newest security fixes and definitions.
5) Digital Identity & Access Management: TSP should implement robust digital identity and access management solutions to guarantee secure and efficient user authentication and authorization. TSP should use technologies such as single sign-on (SSO) and identity federation to streamline user access.

3.3 Additional Security Practices

1) Risk Assessment and Management: Implement a structured and comprehensive risk assessment process to evaluate the potential impact of cybersecurity as well as other threats on IT assets. TSP can refer to standards for example, ISO/IEC 31000.
2) Secure Software Development: Adopt secure coding practices and conduct security testing throughout the software development lifecycle (SDLC).
3) Security Awareness Training: Implement a continuous security awareness training program for all employees to cultivate a culture of security across the organisation.
4) Regular Audits and Assessments: Perform periodic audits and assessments to evaluate the effectiveness of cybersecurity measures and identify areas for improvement.
5) Physical Security: Ensure that comprehensive physical security controls are in place to prevent unauthorized access to critical infrastructure.

3.4 Compliance and Monitoring

1) Legal and Regulatory Compliance: Stay informed of and ensure compliance with all applicable legal, regulatory, and industry requirements depending on the sector and activity. For example, the QFC Data Protection Regulations 2023, Qatar Personal Data Privacy Protection Law No. 13 of 2016, QCB Technology Risks, etc.
2) Monitoring and Logging: Implement comprehensive monitoring and logging mechanisms to continuously observe network and system activities for suspicious behaviour, aiding in the early detection of potential security incidents.

TSP should maintain a secure and resilient environment, to effectively manage cybersecurity risks, protect client, and company data against emerging threats.

4. DATA MANAGEMENT AND SECURITY

Effective data management and security are critical for TSP to ensure the protection of sensitive, confidential and personal data, maintain data integrity, and comply with applicable privacy regulations. This section outlines the key practices for managing data within a secure framework. TSP should also refer to QFC Data Protection Regulations 2023 for guidance.

4.1 Data Classification and Handling

Establish and implement procedures for classification, handling, and securing of data based on its sensitivity. This could include:

1) Identifying which data including personal data are considered sensitive or critical to the organisation's operations.
2) Assigning levels of security and access controls based on the classification to prevent unauthorized access or data breaches. Industry standards such as ISO/IEC 27001 can guide the implementation of appropriate security controls.
3) Regularly reviewing and updating data classification to reflect changes in business requirements or regulatory environments.
4) TSP should implement data anonymisation and pseudonymisation techniques to protect sensitive information while ensuring that the data remains useful for analytics and business purposes.

4.2 Data Protection Measures

Deploy advanced technologies and establish rigorous processes to protect data integrity, confidentiality, and availability. Key measures include:

1) Encryption of data in transit and at rest to safeguard against unauthorized access. TSP can refer to industry standards such as RSA, SHA, FIPS 140-2 to ensure protection of data at rest, in transit or in use.
2) Implementation of robust data backup and recovery systems to ensure data availability and integrity during a data loss incident. TSP can refer to best practices for example, ISO/IEC 27031.
3) Use of firewalls, antivirus software, and other defensive technologies to protect against external threats and vulnerabilities.

4.3 Data Privacy Compliance

Maintain an up-to-date overview of compliance with relevant privacy laws (for example, QFC Data Protection Regulations 2023) and regulations, including but not limited to:

1) Adhering to all applicable data privacy protection laws. Implementing policies that comply with sector-specific laws and regulations applicable to the handling of tokens and personal data. TSP can refer to frameworks like ISO/IEC 27701 can be referred for privacy information management.
2) Ensuring that all data management practices are transparent to clients and stakeholders, and that rights such as data access, correction, and deletion are easily exercisable by data subjects.

4.4 Data Retention and Archival

Establish clear policies and procedures for data retention, including:

1) Defining retention period and archival frequency for different types of data based on regulatory requirements and business needs.
2) Define appropriate access rights to prevent any unauthorized access to archived privileged information to avoid any compromise of confidentiality, integrity, and accessibility.
3) Ensuring secure disposal of data that is no longer needed, in accordance with relevant data protection regulations. TSP can refer to industry best practices such as NIST SP 800-88 for data destruction.
4) Regularly reviewing retention policies to ensure they remain aligned with current laws and organizational requirements. TSP can refer to standards like ISO/IEC 27040 for data storage security. TSP functioning in financial sector should refer to QCB's latest Cyber Security Circular for guidance.

TSP should ensure that their data management practices not only secure the data effectively but also align with legal and ethical standards, thereby enhancing trust and reliability in their services. This proactive approach to data management and security plays a crucial role in the organisation's overall data governance strategy and helps in mitigating risks associated with data breaches and compliance violations.

5. TECHNOLOGY MANAGEMENT

Effective technology management is essential for TSP to ensure the reliability, security, and efficiency of their systems and technology. This section provides guidelines and procedures for the development, maintenance, and ongoing management of technological resources:

5.1 System Development and Maintenance

1) Development: TSP should implement best practices for system development that include secure coding techniques, comprehensive testing phases, and integration of security measures from the ground up. Emphasize the importance of security by design to mitigate risks early in the development process. TSP can consider referring to standards like Open Web Application Security Project (OWASP), CERT secure code standards and MITRE CWE standards for Secure Coding Practices.
2) Maintenance: Establish routine maintenance schedules that include regular checks and balances to ensure systems operate effectively and securely. Maintenance

activities should also address the timely resolution of identified vulnerabilities or performance.

3) Secure Disposal: Develop procedures for the secure disposal of outdated or unnecessary systems and technology. This includes proper data deletion techniques to prevent data leakage and ensuring that all components are disposed of in accordance with environmental and security standards.
4) Open-Source Software: TSP should ensure that the use of open-source software addresses stability, security, and suitability for its intended purpose. The use of open-source software should be carefully managed with proper and continuous verification of any bugs or security issues. Swift action should be taken by the TSP in case of any issue.

5.2 Technology Updates and Patch Management

1) Regular Updates: Define procedures for the regular update of software and systems to safeguard against vulnerabilities. This includes the implementation of a structured update schedule that aligns with vendor release cycles and industry best practices, for example Information Technology Infrastructure Library (ITIL).
2) Patch Management: Establish a comprehensive patch management strategy that ensures all critical patches are applied promptly. The strategy should include assessment processes to prioritise patching based on risk exposure, testing patches before deployment to minimise system disruptions, and documentation of all patching activities for audit and compliance purposes. For example, NIST SP 800-40 for patch management.
3) Version Control: TSP should implement a version control system that accurately timestamps and identifies any system changes. For example, Git, SVN.

5.3 Backup, Recovery and Continuity

1) Backup Systems: Implement and maintain robust backup systems to recover all types of data and information including but not limited to on-chain, off-chain, wallets in the event of data loss, technical failure, or other disruptions. For example, Standards like ISO/IEC 27001 can be referred for guidance.
2) Disaster Recovery Planning: Develop and regularly update a disaster recovery plan that includes procedures for restoring digital asset wallets and transaction capabilities following a disaster. This plan should be tested periodically to ensure its effectiveness.
3) Business Continuity: Establish a comprehensive business continuity plan that ensures critical business functions can continue during and after a disruption. This plan should include strategies for maintaining operations and recovering from incidents with minimal disruption. TSP can refer to standards like ISO/IEC 22301 for best practices in business continuity management.

TSP should manage their technology landscape effectively, ensuring that all systems and software are up-to-date, secure, and aligned with the evolving technological and regulatory environment. This proactive approach to technology management is crucial for maintaining operational integrity and securing client data and assets.

6. TESTING AND AUDITS

Regular testing and audits are necessary for ensuring that TSP maintain secure systems, adhere and refer to industry standards, and comply with regulatory requirements. The

practices outlined here are intended to guide TSP in developing effective testing and audit procedures. These are not exhaustive and should be adapted to incorporate the latest testing and audit standards and requirements.

6.1 Schedule and Procedures:

1) Regular Testing: Establish a continuous testing schedule tailored to the organisation's operational demands and risk profile, including routine and event-triggered tests. TSP should also consider deploying automated testing tools and continuous integration/continuous deployment (CI/CD) pipelines which can improve efficiency and reliability.
2) Penetration Testing and Vulnerability Assessments (VA): TSP should deploy a combination of automated tools and techniques to perform a comprehensive VA. TSP should consider all relevant actors, third parties and critical components like assessments of smart contracts relevant to the TSP's operations. Standards like Penetration Testing Execution Standards, NIST SP 800-115 Technical Guide to Information Security Testing and Assessment can provide guidance to TSP.
3) Technical, Operational, and Security Vulnerabilities: Regularly identify and address technical, operational, and security vulnerabilities through systematic testing and assessments.
4) End-to end testing: TSP should be aware of all the actors on the network and its potential impact on TSP’s service performance. Testing should involve all the relevant actors and parties. TSP should consider throughput & non-functional testing when required.
5) Frequency: The frequency of these tests should be as per the regulatory, sector specific, client or stakeholder requirements and commitments. TSP should also ensure these tests precede the launch of new systems, applications, or products.
6) Documentation and Reporting: Maintain comprehensive documentation of all testing activities and outcomes including that of third parties.

6.2 Internal and External Audits:

1) Internal Audits: Implement robust internal surveillance procedures to regularly assess operational processes including conducting security testing on infrastructure and applications as per internal standards and external requests.
2) External Audits: Regular independent audits to review management practices, ensuring systems operate effectively and comply with policies, procedures, and regulatory frameworks. Report these findings to QFC or other authorities as required or on request.
3) Scope and Frequency: Define the scope and frequency of audits to cover all critical operational aspects, ensuring they reflect the organisation’s risk landscape and operational changes.

6.3 Comprehensive Audit and Assessment Strategies

1) IT Audits: Conduct IT audits for an independent assessment of the TSP’s technology-related risk management, governance, and internal controls. These audits should cover all IT operations, functions, and processes, identifying areas at risk.
2) Audit Expertise and Frequency: Ensure that auditors have relevant skills, and that the frequency of audits matches the importance and risk level of each IT asset,

function, or process. For example, ISACA's CISA for Certified Information Systems Auditor.

6.4 Enhanced Security Testing Practices

1) Cyber Exercises and Adversarial Simulations: Incorporate cyber exercises and scenario-based adversarial simulations into regular testing to enhance defensive capabilities. TSP should use current cyber threat intelligence to design test scenarios that cover potential attacks. For example, NIST Cybersecurity Framework can provide guidance to TSP.
2) Remediation Management: Develop processes for effective mitigation of identified vulnerabilities, continually updating these measures based on insights from audits and tests to strengthen security defences.

TSP must stay informed of the latest testing and audit standards to ensure their practices remain relevant and effective. This approach not only safeguards against potential threats but also reinforces the organisation's commitment to rigorous security standards and builds trust with clients and stakeholders.

7. THIRD-PARTY VENDOR MANAGEMENT

Effective management of third-party vendors is crucial for TSP to safeguard their operations and ensure compliance across all aspects of their business. This section provides guidelines on managing third-party vendors, from initial assessment to enforcing security requirements, in order to protect against potential risks introduced by external entities.

7.1 Vendor Assessment

1) Comprehensive Evaluation: TSP should develop and implement a comprehensive set of criteria for evaluating third-party vendors. These criteria should include the vendor's financial stability, reputation, compliance history, and security posture.
2) Formal Processes: TSP should establish formal processes for vendor assessment that include thorough due diligence checks, risk assessments, and trial periods before full engagement. This process should also involve regular reviews and reassessments to ensure that vendors continue to meet the required standards.
3) Multi-Tiered Evaluation Techniques: TSP should incorporate multi-tiered evaluation techniques, such as questionnaires, interviews, and on-site audits, to gather comprehensive information about potential vendors.
4) Risk Assessment Frameworks: TSP should leverage various third-party risk assessment frameworks. For example, Standardized Information Gathering, Vendor Risk Management Maturity Model.
5) Conflict of Interest: TSP should ensure that there is no conflict of interest with third parties.

7.2 Vendor Security Requirements

1) Clear Security Standards: TSP should define clear security requirements that all third-party vendors must meet to do business with the TSP. These requirements should align with the TSP's own security policies and the regulatory standards applicable to their operations.

2) Specific Security Measures: TSP should include requirements such as data encryption standards, access controls, incident reporting mechanisms, and compliance with relevant privacy laws and cybersecurity regulations.
3) Monitoring Compliance: TSP should implement a monitoring system to regularly assess the vendor's compliance with these security requirements. This system should include periodic audits, real-time monitoring of security logs, and regular updates from the vendor on any security developments.
4) Contractual Clauses: TSP should include clauses in contracts with third-party vendors that allow for termination or penalties if the security requirements are not met, ensuring that there is a legal obligation to maintain security standards.

8. OUTSOURCING MANAGEMENT

TSP should effectively manage its outsourcing partners in order to safeguard its operations and guarantee compliance across all aspects of its business.

8.1 Outsourcing Assessment

1) Evaluation: TSP should create and put to practice a comprehensive set of criteria for accessing outsourcing partners. These criteria should include the partner's financial health, reputation, compliance history, and security posture.
2) Formal Processes: TSP should establish and follow formal procedures for outsourcing evaluation which should include thorough due diligence checks, risk assessments, and trial periods before full engagement. TSP should conduct regular reviews and re-evaluation to ensure that outsourcing partners continue to meet the required standards.
3) Evaluation Methods: TSP should include evaluation methods, such as questionnaires, interviews, and on-site audits, to gather comprehensive information about potential partners.
4) Risk Assessment Frameworks: TSP when accessing outsourcing partners should leverage various risk assessment frameworks.
5) Conflict of Interest: TSP should make sure that there is no conflict of interest with outsourcing partners.

8.2 Outsourcing Security Requirements

1) Clear Security Standards: TSP should define clear security requirements that all outsourcing partners must meet to do business with the TSP. These requirements should align with the TSP's own security policies and any applicable law or regulatory standards applicable to their business.
2) Specific Security Measures: TSP should include clauses requiring data encryption standards, access limits, incident reporting procedures, and adherence to pertinent cybersecurity and privacy legislation.
3) Monitoring Compliance: To make sure the partner is adhering to these security criteria on a regular basis, TSP should put in place a regular monitoring procedure. Periodic audits, real-time security log monitoring, and frequent partner updates on security changes should all be a component of this system.
4) Contractual Clauses: TSP should include clauses in contracts with outsourcing partners that allow for termination or penalties if the security requirements are not met, ensuring that there is a legal obligation to maintain security standards.

TSP should efficiently manage its connections with third-party vendors and outsourced partners for technology and other services. The integrity and reliability of TSP's operations depend on all parties adhering to high security standards, which can only be achieved by TSP taking a proactive approach.

9. INCIDENT MANAGEMENT

TSP should have efficient incident management in place to promptly respond to and mitigate the effects of security incidents. This section outlines and offers advice about the key components of an incident management strategy, from detection through to analysis, in order to ensure a rapid and coordinated response.

9.1 Incident Detection

1) Detection Tools: TSP can promptly spot possible incidents by implementing robust detection tools and techniques. These could include intrusion detection systems (IDS), security information and event management (SIEM) systems, and continuous monitoring of network traffic. TSP can also leverage on standards for example, NIST SP 800-94 for IDS, ISO/IEC 27035 for incident management.
2) Staff Training: Training staff to recognise signs of security breaches, such as unusual system behaviour or unauthorized access attempts, and to report these signs immediately.
3) Ensure high sensitivity and minimal false positives by routinely updating and fine-tuning detection tools to meet evolving cybersecurity threats and vulnerabilities.

9.2 Incident Response Plan

1) Comprehensive Plan: Develop a detailed incident response plan that outlines the steps to be taken in the event of a security breach. The duties and responsibilities of all parties involved, including management, external stakeholders, and incident response teams, should be explicitly outlined in this plan.
2) Incident Procedures: The plan should include procedures for containing the incident, eliminating the threat, system recovery and communicating with internal and external stakeholders, including regulatory bodies.
3) Regular Testing: Regularly test and revise the incident response plan to ensure its effectiveness, incorporating lessons learned from drills and incidents.
4) Service Level Agreements (SLA): Create SLAs as a component of the support process to specify expected response times, responsibilities, and resolution times for different types of incidents. TSP should make sure SLAs address the underlying Distributed Ledger Technology (DLT) implementation concerning consensus and transaction finality to provide clarity on operational expectations and commitments. TSP should regularly monitor SLA compliance and take corrective actions for any breaches to maintain service quality and trust with stakeholders.
5) Kill Switch: TSP should include a "kill switch" mechanism into the incident response plan. This feature should allow for the immediate shutdown or isolate affected systems to prevent further damage and contain the breach quickly. The kill switch should be used in critical situations where immediate action is necessary such as to protect sensitive data and maintain system integrity.

9.3 Post-Incident Analysis

1) Root Cause Analysis: Conduct thorough post-incident analyses to determine the root causes of incidents and understand the effectiveness of the response strategies.
2) Forensic Analysis: Utilize methods such as forensic analysis to trace the steps of the attackers and identify any vulnerabilities exploited during the incident.
3) Feedback Loop: Develop a feedback loop from the analysis to enhance future response strategies and bolster overall security measures. This should include updating incident response plans and refining preventive measures based on the insights gained.
4) Training and Case Studies: Share findings with relevant teams and use them as case studies for training purposes to improve organisational learning and resilience.
5) Continuous Improvement: Develop a procedure for post-incident review for continuous improvement and necessary updates to policies and procedures.

9.4 Incident Reporting

1) Clear Procedures: Establish clear procedures for reporting security incidents to ensure timely communication and escalation. This includes internal reporting channels and external notifications to regulatory bodies and affected stakeholders including clients.
2) Reporting criteria: Define the criteria for reporting incidents based on their severity and impact, ensuring that all significant events are documented and communicated appropriately.
3) Centralized Log: Maintain a centralized incident log to record all incidents, actions taken, and lessons learned, providing a comprehensive record for future reference and analysis.
4) Transparency and Accountability: Ensure transparency and accountability in the reporting process by designating specific roles responsible for incident documentation and communication.

By integrating these components into their overall security strategy, TSP can ensure that they are prepared to effectively manage and mitigate the impacts of security incidents. This comprehensive approach not only limits damage in the short term but also strengthens the organisation's security posture against future threats.

10. REGULATORY COMPLIANCE

Regulatory compliance and effective reporting are foundational aspects of risk management for TSP. Adhering to legal standards and maintaining transparent communication with regulatory bodies and stakeholders are crucial for operational integrity and trust. This section outlines the necessary compliance requirements and the procedures for effective reporting.

10.1 Compliance Requirements

1) Understanding Regulations: Understand and adhere to all specific legal and regulatory requirements applicable to the organisation's operations. For example, the QFC Data Protection Regulations 2023, Qatar Personal Data Privacy Protection Law No. 13 of 2016, and relevant financial regulations issued by QCB, QFCRA etc.
2) Systems and Controls: Implement systems and controls that ensure continuous compliance with these legal frameworks. This may involve regular compliance

audits, continuous monitoring of compliance metrics, and engagement with legal experts to interpret complex regulatory requirements.

3) Stay Informed: Stay informed about changes and updates in regulatory requirements to ensure that the organisation remains compliant with all current laws and regulations.
4) Notification Requirements: TSP should comply with notification requirements as mandated by the regulations, rulebooks, or directives from the State of Qatar, QFC, and any applicable sectoral laws.
5) Access for Authorities: TSP should ensure that relevant authorities can access any information related to the TSP's adherence to rules, regulations, or standards, regardless of the information's storage location. This could include fulfilling any requirements for issuing notifications, including relevant contractual clauses, and securing all necessary consents. Additionally, TSP may be required to grant regulators/authorities the right to conduct audits, perform monitoring, and implement technology tools, as necessary.
6) Transactions: Ensure all transactions comply with local and international regulations. This could include, adhering to AML, Know Your Customer (KYC), and counter-terrorism financing (CTF) requirements. For example, QFCRA AML/CFTR Rules 2019.
7) Reporting and Record-Keeping: Maintain comprehensive records of all transactions and wallet activities. These records should be readily accessible for audit purposes and for reporting to regulatory bodies when required.
8) Reconciliation between Tokens and Actual Assets: TSP should ensure that reconciliation between tokens issued on the DLT, and the actual assets is performed regularly and accurately to maintain transparency and trust.
9) Compliance Tools: TSP should also explore the use of compliance management software or tools that could streamline tracking and reporting activities. For Example, Governance, Risk & Compliance Tool like Archers.

By maintaining rigorous compliance with regulatory requirements and implementing robust reporting procedures, TSP can avoid legal penalties and enhance their reputation in the marketplace. Effective compliance and transparent reporting are key to building long-term trust and reliability with both regulators and customers.

11. CRYPTOGRAPHY

Cryptography is essential for securing digital transactions and protecting data integrity within TSP. This section outlines the fundamental cryptographic measures that TSP should implement to ensure robust security for tokens and sensitive information. TSP should periodically conduct reviews to ensure future readiness to evolving threats (for example, adoption of quantum resistant algorithms).

11.1 Cryptographic Principles and Implementation

1) Adoption of Strong Cryptographic Standards: TSP should employ strong cryptographic standards such as, but not limited to, AES (Advanced Encryption Standard) for data encryption and RSA or ECC (Elliptic Curve Cryptography) for digital signatures. These standards help secure data transmissions and ensure the confidentiality and integrity of data at rest and in transit. For example, ISO/IEC 18033 for encryption algorithms.
2) Key Management: Implement comprehensive key management systems to handle the generation, storage, distribution, and destruction of cryptographic keys. This

system should include secure key storage mechanisms, the use of hardware security modules (HSMs) where appropriate, and policies for key rotation and revocation to mitigate the risk of key compromise. TSP should have policies and procedures detailing recovery of lost credentials for clients. For example, ISO/IEC 11770 for key management.

3) DLT Integration: TSP should ensure that cryptographic practices are integrated into DLT systems, securing blockchain transactions and maintaining the integrity of the ledger. For example, TSP can refer to standards like ISO/TC 307.

11.2 Secure Procedures

1) Use of Secure Communication Procedures: Enforce the use of secure communication procedures, such as TLS (Transport Layer Security), for all data exchanges. This ensures that data transmitted over networks is encrypted and protected from eavesdropping and "man-in-the-middle" attacks. For example, NIST SP 800-52 for TLS configurations.
2) Data Integrity Checks: Employ cryptographic hash functions, like SHA-256, to maintain data integrity. These functions allow verification of data authenticity and help detect any unauthorized changes to data. For example, ISO/IEC 10118 for hash functions.

11.3 Cryptographic Compliance and Updates

1) Regular Cryptographic Audits: Conduct regular audits of cryptographic practices to ensure they meet current security standards and compliance requirements. This could include reviewing the cryptographic algorithms in use and their configurations, as well as the effectiveness of the key management practices. For example, NIST SP 800-53 for security controls.
2) Stay Informed on Cryptographic Advances: Keep abreast of advancements in cryptographic techniques and potential vulnerabilities in existing cryptographic algorithms. Update cryptographic practices accordingly to protect against emerging threats and to incorporate technological improvements.
3) Training and Awareness: Provide ongoing education and training for staff on cryptographic policies and procedures. This ensures that all personnel understand how to properly use and manage cryptographic tools to protect organisational data.

Implementing these cryptographic measures will help TSP to protect against unauthorized access, ensure data privacy, and maintain the trust of their clients by securing digital transactions and sensitive information effectively.

12. WALLETS & TRANSACTIONS

Managing wallets and transactions securely is crucial for TSP to protect against fraud, ensure transaction integrity, and maintain client trust. This section provides guidelines for the secure management of wallets and the processing of transactions. TSP should also focus on regular security training for staff and being updated about the latest threats and best practices. TSP should ensure adherence to compliance and regulatory requirements.

12.1 Wallet Security Management

1) Secure Wallet Architecture: Implement robust wallet architectures that ensure the safety of the tokens. This could include the use of multi-signature wallets, which require multiple keys to authorize a transaction, thereby enhancing security.
2) Private Key Protection: Employ stringent measures to protect private keys, which are critical for accessing wallets. Techniques such as encryption, the use of cold storage solutions (offline storage), and physical security measures should be standard practice.
3) Regular Security Audits: Conduct regular security audits of wallet infrastructure to identify and mitigate potential vulnerabilities. These audits should include both hardware and software components of the wallet ecosystem.
4) Segregation of Wallets: Maintain separate wallets for different types of transactions and assets. This segregation helps to minimize risk by isolating various types of activities, thereby enhancing security, and reducing the potential impact of a breach.

12.2 Transaction Security

1) Transaction Monitoring: Implement systems to monitor transactions in real-time for signs of suspicious activity. This could include setting thresholds for transaction values that trigger manual review processes and monitoring interactions with whitelisted wallet addresses to ensure they remain within expected parameters.
2) Confirmation Procedures: Establish procedures for confirming transaction details with clients before processing significant or unusual transactions. This can help prevent unauthorized transactions due to phishing or other fraud attempts.
3) DLT Analysis Tools: Utilize blockchain analysis tools to track transaction patterns and identify potentially fraudulent activities. These tools can provide insights into complex chain interactions and help TSP maintain compliance with anti-money laundering (AML) and other regulations.
4) Transaction Finality: The finality of a transaction should be consistently aligned across regulations, policies, scheme rules, and the technical implementation design of the TSP service. This alignment must be clearly communicated to customers to ensure transparency and understanding of the service.

13. SMART CONTRACT

Smart contract management is essential to guarantee their security and optimal performance. This section outlines the key practices for managing smart contracts within a secure framework:

13.1 Smart Contract Security

1) Code Reviews and Audits: Conducting thorough reviews and audits of the smart contract code to identify and fix security vulnerabilities before deployment. TSP can refer to industry standards like OWASP Secure Coding Practices, ISO/IEC 27001 for information security management.
2) Access Controls: Implementing access controls to manage deployment and modification of the smart contracts, minimizing the risk of unauthorized activity. TSP can refer to industry standards like NIST SP 800-53 for access control, ISO/IEC 27002 for security techniques.
3) Monitoring and Auditing: Regularly monitoring and auditing smart contracts to ensure they operate as intended and avoid any tampering. TSP can refer to industry

standards and guidelines like ISO/IEC 27001 for information security management, Qatar Financial Centre Regulatory Authority (QFCRA) guidelines.

13.2 Smart Contract Management

1) Updating and Patching Procedures: TSP should establish clear procedures for updating or patching smart contracts if vulnerabilities or bugs are discovered post-deployment.
2) Comprehensive Documentation: Maintain comprehensive documentation of smart contracts, including their code, version history, and audit reports.
3) Contingency Plans: Develop contingency plans for reverting or disabling smart contracts in the event of critical issues.

13.3 Emergency Shutdown Mechanism

1) Develop Criteria for Activation: Define the conditions under which the emergency shutdown mechanism will be activated, such as detecting unauthorized access, critical bugs, or double-spending attempts.
2) Risk and Probability Assessments: Incorporate risk and probability assessments within the shutdown mechanism to evaluate threats in real-time and trigger the shutdown if necessary.
3) Develop Response Protocols: Outline detailed response protocols for when the shutdown mechanism is activated, including steps for system audits, data restoration, and stakeholder communication.
4) Regular Audits and Updates: Conduct regular audits to ensure the shutdown mechanism remains effective and up to date with the latest practices.

TSP should ensure that their smart contract management practices not only secure the contracts effectively but also align with legal and ethical standards, thereby enhancing trust and reliability in their services. A proactive approach to smart contract management plays a crucial role in the organization's overall governance strategy and helps mitigate risks associated with data breaches, compliance violations, and contract vulnerabilities. TSP should also ensure to keep all these details documented.

APPENDIX 1

Best practice, legislation, standards, and guidelines

TSP should have regard to best practice, legislation, standards, and guidelines, as set out in the tables in this Appendix. The best practices set out in the tables below are aimed at promoting the adoption of sound and robust practices for the TSP.

It is anticipated that the tables will be regularly updated to take account of the continually evolving best-practice developments in digital assets. TSP should ensure that they always access the latest version of best practise developments.

State of Qatar

#	Entity	Link and website sections	Purpose & Digital and Information Technology focus	Topic
1	Qatar Central Bank (QCB)	Qatar Central Bank (qcb.gov.qa) -Policies and Legislation -FinTech and Innovation -Instructions for Financial Technology Companies -Information Security - Distributed Ledger Technology Guideline	The QCB serves as the primary financial regulator for the State of Qatar. It oversees monetary policy, regulates banks, and ensures the stability of the financial system within the country. QCB plays a key role in promoting a safe and stable financial environment by supervising various financial institutions and markets. In addition to its regulatory functions, QCB drives the national Fintech strategy, aiming to foster innovation and support the growth of financial technology in Qatar. This strategy includes enhancing market developments, encouraging the adoption of innovative technologies, and creating a conducive environment for Fintech startups. Moreover, QCB emphasizes stringent information security mandates to protect the integrity of financial data and systems, ensuring a robust framework for digital transformation and cybersecurity.	Central Bank, Regulator, Information technology
2	Ministry of Communication and Information Technology (MCIT)	Ministry of Communications and Information Technology (mcit.gov.qa) -Legislation and Policies	The MCIT in the State of Qatar is the government entity responsible for regulating and developing the telecommunications and information technology sector in Qatar. The ministry works to implement the policies of the Qatari government in the field of communications and information technology, while promoting technology and innovation in line with Qatar National Vision 2030, in addition to providing high-quality services to the citizens and businesses in Qatar.	Regulator, Data Management
3	National Cyber Security Agency (NCSA)	National Cyber Governance and Assurance Affairs (ncsa.gov.qa) -Regulatory Tools	The NCSA is focused on developing and proposing cybersecurity policies, legislation, standards, and controls, while ensuring compliance through coordination with national authorities. It implements a national Cyber Risk Framework, identifies critical sectors, and formulates a National Cyber Security Strategy. The NCSA also conducts National Cyber Security Drills to verify business continuity and risk management preparedness, pinpointing areas for improvement. Additionally, it issues certificates of compliance with national information security standards and conducts periodic reviews and audits. The agency is responsible for accrediting cybersecurity service providers and issuing cyber security assurance	Regulator, Cybersecurity Policy and Legislation Development, Personal Data Privacy Protection, Audit, Certification

			certificates for devices, systems, and applications based on national and international standards. As the regulator for the Personal Data Privacy Protection Law (PDPPL), the NCSA ensures adherence to the law, develops, and publishes guidelines, and engages with stakeholders.	
4	Qatar Financial Centre Regulatory Authority (QFCRA)	Qatar Financial Centre Legislation Qatar Financial Centre Legislation | Rulebook (thomsonreuters.com)	The QFCRA oversees the regulation and supervision of financial institutions within the Qatar Financial Centre. It ensures compliance with international standards in areas such as banking, insurance, and asset management, while fostering a secure and competitive environment. Additionally, the QFCRA is expanding its regulatory framework to include digital assets regulations, positioning Qatar as a forward-thinking hub for financial technology and digital finance.	Regulator
5	Qatar Financial Centre Authority (QFCA)	Qatar Financial Centre Legislation Qatar Financial Centre Legislation | Rulebook (thomsonreuters.com)	The QFCA is a regulatory and business development body in Doha, Qatar, established to foster economic expansion and diversification in Qatar. Operating with its own legal, regulatory, and tax framework, QFCA offers competitive tax advantages and 100% foreign ownership to attract international firms. It supports a range of financial services including banking, asset management, and insurance, with a strategic focus on developing sectors like digital assets to adapt to evolving market needs	Financial Centre, Data Protection Rules, Companies Rules
6	Communications Regulatory Authority (CRA)	https://www.cra.gov.qa/	The CRA of Qatar is responsible for overseeing the telecommunications and information technology sectors. It regulates access to digital services and maintains competition, ensuring fair practices and consumer protection within these industries.	Regulator, Blockchain, Consumer protection, information technology

International

#	Entity	Link	Purpose & Blockchain Focus	Topic	Geography of Origin
1	British Standards Institution (BSI)	https://britishblockchainassociation.org/	The BSI is the national standards body of the United Kingdom. It aims to disseminate knowledge, foster innovation, and develop methodologies to help individuals and organizations embed excellence into their practices. BSI supports clients with blockchain project requirements, assisting them in harnessing the benefits of this technology. As part of the ISO technical committee TC307 initiative, BSI contributes to global efforts focusing on blockchain and distributed ledger technologies.	DLT Requirements	United Kingdom
2	European Telecommunications Standards Institute (ETSI)	https://www.etsi.org/	ETSI offers opportunities, resources, and platforms for understanding, shaping, and collaborating on globally applicable standards that promote interoperability, security, and competitive advantage. In 2018, ETSI formed an industry specification group on blockchain, Permissioned Digital Ledger, which has published reports on several topics, including smart contract specifications, data management, and interoperability.	Permissioned distributed ledgers; smart contracts; data; interoperability; healthcare; I0T	France
3	International Organisation for Standardization (ISO)	https://www.iso.org/committee/6266604/x/catalogue/	ISO is an independent, non-governmental, international organisation that develops standards to ensure the quality, safety and efficiency of products, services, and systems. The Open Systems Interconnection model (OSI) has covered the topics of digital currencies, interoperability (between blockchain and DLT systems and overall), foundations, security/privacy/identity, smart contracts and applications, governance, use cases, within ISO/TC 307. ISO-14064 also covers blockchain topics.	Security; privacy; identity; governance; smart contracts; digital currencies; interoperability; foundations; applications	Switzerland

4	International Token Standardization Association (ITSA)	https://my.itsa.global/	ITSA developed the International Token Identification Number (ITIN) to create an open market standard for identifying cryptographic tokens. Its framework, the International Token Classification (ITC), categorizes tokens based on their characteristics and assigns unique identifiers. Additionally, ITSA developed the International Token Database (TOKENBASE), setting a standard for qualitative and quantitative analysis of these tokens.	Tokens	Germany
5	Joint Technical Committee (JTC 1)	https://jtc1info.org/	The ISO and IEC Joint Technical Committee (JTC 1) for information technology is a consensus-based, voluntary international standards body. JTC 1 focuses on standardization for emerging technologies and innovations by promoting active cooperation among standards development organizations (such as ISO, IEC, ITU-T, fora, consortia, etc.) to prevent overlapping work. As part of a JTC 1 initiative, ISO and IEC formed the Joint Advisory Group (JAG) on Emerging Technology and Innovation (JETI) to facilitate standards development for future emerging technologies. Any entity seeking to authenticate and verify standards work requires sponsorship from a JTC 1 committee.	Blockchain requirements; applications	Switzerland
6	National Institute of Standards and Technology (NIST)	https://www.nist.gov/	NIST is a physical sciences laboratory and non-regulatory agency within the US Department of Commerce, dedicated to promoting American innovation and industrial competitiveness. NIST's research initiatives have explored various blockchain topics, including use cases, applications, existing services, protocols, security guarantees, and cryptographic mechanisms such as quantum-resistant public-key cryptographic algorithms. These efforts have resulted in scientific papers, experimental software, and resources supporting other NIST projects related to blockchain, recognizing its potential across multiple systems, including manufacturing supply chains, data registries, digital identification, and records management.	Blockchain applications and existing services; protocols; security; cryptography	United States

APPENDIX 2

Checklist

This checklist is designed as a reference tool for TSP to ensure compliance with industry standards and regulations in digital asset management. It provides actionable items across key areas such as cybersecurity, data security, and regulatory compliance, helping TSP to identify and address potential gaps in their operations and maintain a secure and compliant environment.

#	Section	Criteria	Status
1.1	Governance and Oversight	Implement robust systems and controls to manage organisational risks.	
1.2		Establish a comprehensive governance framework for oversight.	
1.3		Update policies regularly to reflect changes in regulatory and operational environments.	
2.1	Risk Management Framework	Utilize various tools to identify potential risks.	
2.2		Evaluate the severity and probability of identified risks systematically.	
2.3		Develop and implement strategies to mitigate identified risks.	
3.1	Cybersecurity	Develop and maintain comprehensive cybersecurity policies.	
3.2		Conduct regular security audits to ensure systems are secure.	
3.3		Formulate and evaluate an incident response plan to manage potential security breaches.	
4.1	Data Management & Security	Classify data according to sensitivity and secure it accordingly.	
4.2		Implement strong data protection measures to safeguard data integrity and confidentiality.	
4.3		Ensure compliance with relevant privacy laws and regulations.	
5.1	Technology Management	Adhere to best practices during system development and maintenance.	
5.2		Maintain and update technology systems regularly to mitigate vulnerabilities.	
5.3		Ensure secure disposal of outdated or unnecessary technology.	
6.1	Testing and Audits	Schedule and perform regular testing of systems to detect vulnerabilities.	
6.2		Conduct both internal and external audits to evaluate compliance and system integrity.	
6.3		Maintain accurate documentation of all testing and audit activities.	
7.1	Third-Party Management	Thoroughly evaluate third-party vendors to ensure compliance with security requirements.	
7.2		Monitor third-party compliance with established security requirements regularly.	
8.1	Outsourcing Management	Thoroughly evaluate outsourcing partners to ensure compliance with security requirements.	
8.2		Monitor outsourcing partner compliance with established security requirements regularly.	
9.1	Incident Management	Implement tools to detect incidents and respond promptly.	
9.2		Develop a detailed incident response plan outlining roles and communication strategies.	
9.3		Perform post-incident analysis to determine causes and improve future responses.	
10.1	Regulatory Compliance and Reporting	Comply with all applicable legal and regulatory requirements.	
10.2		Maintain clear and accurate reporting procedures for communication with regulatory bodies.	
11.1	Cryptography	Employ strong cryptographic standards to protect data transactions.	
11.2		Manage cryptographic keys securely including generation, storage, and destruction.	
11.3		Regularly audit cryptographic practices to ensure they meet security standards.	
12.1	Digital Asset Wallets & Transactions	Secure digital asset wallets to prevent unauthorized access and fraud.	
12.2		Monitor transactions continuously for suspicious activities.	
12.3		Ensure all transactions comply with applicable regulatory and legal requirements.	

13.1	Smart Contract Management	Conduct thorough reviews and audits of smart contract code to identify and fix security vulnerabilities before deployment.	
13.2		Implement access controls to manage the deployment and modification of smart contracts.	
13.3		Regularly monitor and audit smart contracts to ensure they operate as intended and avoid any tampering.	