FailSafe × LDU

The Guide To

BLOCKCHAIN SECURITY AND COMPLIANCE

Digital Asset Regulation
in Singapore

Table of Contents

Foreword

Blockchain service providers globally face stringent compliance obligations, particularly in the areas of technology risk management (TRM), anti-money laundering (AML), counter-terrorism financing (CTF), and consumer protection. As companies look to expand into crypto-friendly jurisdictions and participate in regulatory sandbox programs, the focus on compliance becomes even more essential.

Ensuring compliance with these strict regulations is key to building trust and stability in the blockchain ecosystem. This is where FailSafe's comprehensive solutions - Guard, Interceptor, Radar and AuditAI - help providers meet regulatory requirements while proactively addressing risks. These solutions not only help providers meet regulatory requirements but also empower them to proactively address potential risks, maintain robust security protocols, and ensure long-term operational resilience. Additionally, LDU's legal, compliance, and regulatory expertise can guide you toward clarity, so you no longer need to second-guess your rights and obligations, ensuring you remain fully compliant with evolving standards.

Smart contract security and network monitoring are critical for resilient IT systems, safeguarding against internal and external threats. FailSafe's comprehensive security modules serve as essential building blocks in this process. These modules work in tandem to ensure that blockchain systems adhere to current regulations while providing the agility needed to adapt to future changes.

This guidebook acts as a comprehensive roadmap for blockchain service and digital asset providers in Singapore, showing how to integrate FailSafe's core modules into their compliance strategies. It also provides insight into navigating The Monetary Authority of Singapore (MAS) licensing regime with LDU's compliance expertise.

Our goal is to assist organizations in effectively addressing the critical concerns that form the basis of their compliance obligations, thereby safeguarding their operations and enhancing consumer trust. The aim is to provide digital asset companies with a comprehensive guide to understanding and meeting the Technology Risk Management (TRM) related requirements under the MAS for obtaining a Standard Payment Institution License (SPIL) or Major Payment Institution License (MPIL), such licenses are considered to be gold standard in today's digital assets marketplace.

Compliance in Singapore: Becoming MAS License-Ready

Unified Security Ecosystem

In today's rapidly evolving digital landscape, web3 companies aiming to operate in Singapore's digital assets industry must navigate complex regulatory requirements, particularly when seeking to obtain a Standard Payment Institution License (SPIL) or a Major Payment Institution License (MPIL). The Monetary Authority of Singapore (MAS) has established stringent guidelines to ensure the security, resilience, and operational integrity of digital payment systems, and compliance with these regulations is critical for long-term success.

This guidebook has been designed to provide web3 companies with a clear, actionable roadmap to help them become MAS license-ready. Even if you do not intend to be regulated, these suggestions are considered to be industry gold standard. By focusing on three key sections, it outlines the essential regulatory requirements, practical steps for compliance, and the tools and services available from FailSafe and LDU to support your journey.

1. **Key MAS Requirements for SPIL/MPIL Licensees**

The MAS's Technology Risk Management (TRM) framework, outlined in MAS Notice FSM-N13 (FSM-N13), MAS Notice FSM-N14 (FSM-N14), and the MAS Technology Risk Management Guidelines, forms the cornerstone of compliance for digital asset service providers.

This section covers the core regulatory requirements essential for SPIL/MPIL licenses:

a. Technology Risk Management;
b. Critical System Identification;
c. Cyber Hygiene;
d. Data Protection; and
e. Incident Response.

2. **Practical Steps and Best Practices**

Once the regulatory requirements are understood, the next step is implementation. This section outlines practical steps and best industry practices your company can adopt to ensure compliance.

This guide outlines how to build a TRM framework and adopt cybersecurity protocols. Proactive planning and thorough documentation will help meet MAS expectations and differentiate your company in the web3 ecosystem.

3. Summary of Key Services from FailSafe and LDU

To support your compliance efforts, FailSafe and LDU offer a suite of specialized services that not only simplify the compliance process but also ensure seamless integration with MAS requirements.

FailSafe provides specialized cybersecurity tools tailored for web3 companies. Guard enhances smart contract security through access control, ensuring that only authorized personnel can execute privileged operations. Interceptor ensures real-time blockchain defense, swiftly moving vulnerable funds to secure wallets in case of potential threats. Meanwhile, Radar offers AI-powered transaction monitoring to secure digital assets and maintain MAS's TRM compliance. Additionally, LDU provides expert legal, regulatory, and data protection consultancy to ensure your business aligns with MAS guidelines. LDU helps companies implement compliant policies for incident reporting, cyber hygiene, and data protection, ensuring seamless adherence to FSM-N13 and FSM-N14.

By addressing MAS's key requirements early, your company can enhance operational resilience, ensure regulatory compliance, and stay ahead of the competition. This guidebook is your essential companion to navigating the complex regulatory landscape and securing the licenses needed to operate in Singapore's thriving digital assets market.

Key MAS Requirements for SPIL/MPIL Licensees

1. Technology Risk Management

Under FSM-N13 and the MAS Guidelines on Risk Management Practices (TRM Guidelines), digital asset companies must implement a comprehensive TRM framework to manage technology risks effectively. This framework ensures the confidentiality, integrity, and availability of systems and data, a key condition for obtaining a license. The framework must cover four essential processes: risk identification, risk assessment, risk treatment, and ongoing risk monitoring. Therefore, illustrating these processes is key. For companies providing online financial services, a major TRM requirement is a penetration test, which is also mandatory. An independent validation of remediation efforts must be completed prior to the granting of a license.

Furthermore, each applicant is required to complete a technology risk questionnaire, which covers:

- Cyber Hygiene
- Sensitive Data Loss Prevention
- Penetration Testing
- TRM Guidelines and Audit

How our Tools and Documentation Can Help Achieve

Essential Tools for Compliance

AuditAI: This tool performs near-instant smart contract audits using machine learning algorithms to detect major vulnerabilities. This aligns with MAS's requirements for identifying and mitigating technology risks. The secondary audit feature further strengthens compliance by ensuring remediation actions meet regulatory standards, which can be done on a more regular basis and with higher accuracy. To provide an additional layer of security and assurance, FailSafe complements AuditAI's automated analysis with manual audits conducted by their team of certified auditors. This combined approach not only bolsters compliance but also provides enterprises with the confidence that their smart contracts are thoroughly scrutinized and secured against emerging threats.

Radar: A comprehensive solution for real-time anomaly detection, Radar supports address-labeling for AML/KYC compliance, transaction screening, and predictive analytics for risk-scoring. This tool addresses the ongoing risk monitoring requirement stipulated in TRM Guidelines by providing instant alerts, ensuring continuous protection against potential system risks and fraud.

© 2024, FailSafe and LDU. All Rights Reserved.

Required Documentation for Compliance

TRM Policy: This policy outlines the governance structure, roles, and responsibilities within the risk management framework, showing MAS that you have the internal processes to manage and mitigate risks effectively.

Risk Assessment Reports: Regularly updated reports that identify potential risks and vulnerabilities, with corresponding controls. These reports, aligned with MAS's requirements, help demonstrate your firm's proactive stance on identifying and managing technology risks.

Risk Treatment Plans: Documented measures to mitigate identified risks, ensuring your enterprise-wide risk assessments are adequately addressed. These plans support your submission for an SPIL/MPIL license by detailing how risks are controlled and managed.

Ongoing Monitoring Logs: Logs that show continuous monitoring of systems and technology risks, updated periodically in line with MAS's guidelines. This documentation helps maintain compliance with the requirement for ongoing risk monitoring.

Board Meeting Minutes: Minutes demonstrating senior management and board oversight, with detailed discussions on TRM-related matters. This proves governance and leadership commitment to MAS's risk management framework.

2. Critical System Identification and Data Protection

According to FSM-N13, companies must identify their critical systems and ensure these systems maintain high availability. The total unscheduled downtime for critical systems must not exceed 4 hours within any 12-month period. Additionally, companies must establish clear system recovery objectives to ensure quick recovery in the event of disruption. This includes having a data privacy policy and appointing a data protection officer, in line with the Personal Data Protection Act (PDPA).

How our Tools and Documentation Can Help Achieve Compliance

Essential Tools for Compliance

Interceptor: This automated threat response tool allows for rapid detection and recovery. By maintaining complete incident logs and offering a dedicated Recovery Vault for at-risk digital assets, Interceptor ensures visibility across both on-chain and off-chain activities. This tool helps maintain compliance by adhering to MAS's requirement of high availability and swift recovery. Moreover, its self-custodial security architecture helps secure sensitive data, aligning with MAS's data protection standards.

Guard: Guard provides configurable transaction management policies and dynamic transaction limits. With its smart contract access control management and accurate geo-fencing, it ensures enhanced data security and minimizes system disruptions. The tool's compatibility with multi-signature infrastructure ensures that critical systems are protected from unauthorized changes, meeting the recovery and availability requirements.

Required Documentation for Compliance

Data Loss Prevention Policy: This policy outlines strategies to prevent unauthorized access to sensitive data and demonstrates adherence to the TRM Guidelines. It aligns with the PDPA requirements, ensuring companies safeguard personal data while preventing leaks through intentional or inadvertent actions.

Data Protection Policy: A comprehensive document detailing how personal data is collected, stored, and protected in compliance with the PDPA. This ensures that companies have processes in place to handle personal data securely, mitigating the risk of data breaches.

Critical System Inventory: A detailed list of all critical systems, their roles, and the measures in place to ensure their availability. This inventory is vital for ensuring compliance with the 4-hour maximum downtime requirement and is essential for auditing purposes under the TRM Guidelines.

System Recovery Plans: These plans document the Recovery Time Objectives (RTO) and outline recovery procedures for each critical system. Regular testing of these recovery procedures ensures compliance with MAS's mandate of recovering critical systems within 4 hours of disruption.

System Downtime Logs: Companies must maintain logs that record the availability and unscheduled downtime of critical systems. These logs must also include corrective actions taken and any ongoing risks, providing transparency in case of an audit by MAS.

Validation Reports: System recovery testing must be regularly validated, and reports detailing the results of these tests are required to demonstrate that recovery time objectives are consistently met. These reports help maintain operational resilience, a core requirement of the TRM Guidelines.

3. Cyber Hygiene and IT Security

Companies are required to protect systems and customer information from unauthorized access, companies must implement robust cybersecurity measures in line with FSM-N14. This includes establishing clear policies and procedures for managing the security of information systems, ensuring that cyber hygiene practices are rigorously followed, and maintaining oversight of system integrity through ongoing assessments and updates.

How our Tools and Documentation Can Help Achieve Compliance

Essential Tools for Compliance

Guard: This tool offers configurable transaction management policies, including dynamic transaction limits, smart contract access control, geo-fencing, and device intelligence. With compatibility for multi-signature infrastructure, Guard ensures that systems and customer information are protected from unauthorized access in real-time. This aligns with FSM-N14, which mandates stringent cybersecurity measures.

© 2024, FailSafe and LDU. All Rights Reserved.

Interceptor: A core component of our cybersecurity suite, Interceptor offers real-time defense against blockchain attacks by monitoring memory pools and pending transactions. When a potential hack is detected, Interceptor swiftly relocates funds to a secure, self- custody smart contract wallet, ensuring protection with a 99.8% success rate. This tool directly addresses the MAS's requirement for cyber resilience and incident management, safeguarding digital assets from unauthorized transactions or hacks.

Radar: Radar uses AI and machine learning to continuously monitor transactions for suspicious activity. It detects potential fraud, theft, and sybil attacks in real-time, enabling compliance with MAS's guidelines on cybersecurity and AML regulations. By proactively identifying anomalies, Radar strengthens your organization's overall security posture, making it easier to demonstrate compliance with FSM-N14 on IT security.

Required Documentation for Compliance

Cybersecurity Policy: A comprehensive policy detailing measures like multi-factor authentication (MFA), malware protection, and network security protocols. This document demonstrates adherence to FSM-N14 by showing how your systems prevent unauthorized access.

Security Patch Logs: A record of all system patches applied, including timelines for critical updates, is essential to meet MAS's cybersecurity standards on system integrity and protection against vulnerabilities.

Access Control Logs: Documenting system access measures, including logs of MFA usage and administrative account protections, will help demonstrate compliance with MAS's guidelines.

Security Incident Logs: Comprehensive documentation of any security incidents, including response actions, remedial measures, and outcomes, is critical to show proactive measures in line with MAS's requirements for incident response and cybersecurity resilience.

4. Incident Response and Reporting

According to FSM-N13 and TRM Guidelines, companies must report any IT security incidents, system malfunctions, or breaches to MAS within 1 hour of discovery. Within 14 days, a root cause analysis and impact report must be submitted to MAS, detailing the cause, impact, and mitigation steps taken.

How our Tools and Documentation Can Help Achieve Compliance

Essential Tools for Compliance

Interceptor: Interceptor provides real-time detection and intervention during blockchain attacks. Upon detecting a potential breach, it executes a protective transaction to move vulnerable funds to secure wallets, mitigating further damage. This tool is instrumental in preventing financial loss during IT security incidents and supports quick recovery, which is critical for meeting MAS's 1-hour reporting requirement. By preemptively neutralizing threats,

© 2024, FailSafe and LDU. All Rights Reserved.

Interceptor reduces the impact of incidents, thereby facilitating more focused root cause analysis and impact reporting within the MAS-mandated 14-day window.

Guard: Guard enforces multi-signature mechanisms and strict security checks, ensuring only authorized personnel can perform privileged operations on smart contracts. This minimizes the risk of breaches and supports MAS's FSM-N13 and TRM Guidelines by providing real-time activity logs for swift incident detection and reporting. If an incident occurs, Guard's logs enable rapid root cause analysis and detailed impact reports within the MAS-mandated 14-day window, ensuring compliance and streamlined incident management.

Radar: Radar continuously monitors blockchain transactions for fraud, theft, and anomalous activities. By providing real-time detection of suspicious patterns, Radar ensures early identification of security breaches, helping to meet MAS's 1-hour notification requirement. Its detailed anomaly reports streamline the root cause analysis process, ensuring compliance with the requirement to submit a detailed report within 14 days. Radar's ability to track compliance with AML and transaction integrity also ensures ongoing monitoring and operational integrity as required by the TRM Guidelines.

Required Documentation for Compliance

Incident Response Plan:

This document outlines the procedures to be followed in the event of an IT security incident, including roles, responsibilities, and escalation protocols. A solid incident response plan ensures that your company can quickly respond and report incidents within the 1-hour requirement.

Incident Logs: Logs that detail all IT incidents, including the time of occurrence, discovery, and notification to MAS. These logs provide evidence of prompt incident detection and response, key elements of compliance with MAS regulations.

Root Cause Analysis (RCA) Reports: These detailed reports explain the cause of the incident, its impact on operations, and the steps taken to remediate the issue. Submission of these reports to MAS within 14 days ensures compliance with FSM-N13's reporting requirements.

Impact Analysis Reports: These reports assess the operational, customer, and regulatory effects of the incident. Preparing and maintaining impact analysis documentation helps fulfill the TRM Guidelines by ensuring a structured and thorough evaluation of incidents.

The next section will go over some practical steps to take, best practices to adopt, and necessary preparation to take in order to prepare you to be license ready with the MAS.

Practical Steps and Best Practices

1. Developing a Technology Risk Management Strategy

Overview: A robust TRM strategy is essential for compliance with MAS regulations. This section will walk companies through developing a comprehensive TRM framework that is proportionate to the complexity and risks of their digital payment services.

Key Components:

1. Board Oversight and Governance:

   MAS requires active board and senior management oversight of technology risk. This involves establishing a TRM framework and ensuring the board has the knowledge to manage these risks effectively.

   Steps to Take:

   - Assign a Chief Technology Officer (CTO) or equivalent to oversee the TRM strategy.
   - Conduct regular board-level discussions on technology risks.
   - Implement a clear risk appetite and tolerance framework.

2. Risk Identification and Assessment:

   The TRM strategy must outline a process for identifying and assessing IT risks, including risks from third-party vendors and internal IT operations.

   Steps to Take:

   - Regularly assess critical systems and data assets.
   - Identify potential technology risks such as system failures, cyberattacks, and data breaches.

3. Risk Treatment and Control Measures:

   Establish and conduct an enterprise wide risk assessment (EWRA) that outlines controls and processes for mitigating identified risks.

Steps to Take:

- Develop policies for IT security, data protection, and disaster recovery, along with a robust EWRA.
- Implement controls such as multi-factor authentication, encryption, and regular system patching.

4. Ongoing Monitoring and Reporting:

   Companies must continuously monitor their systems and report any technology risks to MAS as part of their TRM strategy.

   Steps to Take:

   - Conduct regular system audits and technology risk reviews.
   - Maintain an incident reporting system to meet MAS's 1-hour reporting requirement for IT incidents.

2. Cybersecurity Best Practices for Digital Asset Companies

Overview: Cybersecurity is a critical aspect of MAS's Technology Risk Management requirements, particularly under the FSM-N14 notice on cyber hygiene. This section provides a step-by-step guide to implementing cybersecurity best practices that align with MAS regulations.

Key Practices:

1. Multi-Factor Authentication (MFA):

   Requirement: MAS mandates that administrative and critical system accounts use MFA to safeguard against unauthorized access.

   Steps to Take:

   - Implement MFA for all systems handling sensitive customer information.
   - Ensure MFA solutions are deployed for administrative accounts.

2. Malware Protection:

   Requirement: Companies must implement robust malware protection measures to mitigate the risk of cyberattacks.

   - Steps to Take:
   - Deploy anti-virus software and firewalls across all systems.
   - Regularly update malware protection tools to address emerging threats.

© 2024, FailSafe and LDU. All Rights Reserved.

3. Security Patch Management:

   Requirement: MAS requires companies to ensure timely application of security patches to address system vulnerabilities.

   Steps to Take:

   - Implement a patch management schedule that prioritizes critical systems.
   - Regularly review and update system configurations to ensure compliance.

4. Incident Response Plan:

   Requirement: Companies must have an incident response plan to handle cybersecurity incidents and report them to MAS.

   Steps to Take:

   - Establish a formal incident response plan detailing roles and actions in case of a breach.
   - Train staff on recognizing and reporting security incidents.

3. Preparing for MAS Audits and Inspections

Overview: MAS audits and inspections are a critical part of maintaining compliance under the Payment Services Act. This section will guide companies in preparing for such audits, focusing on the documentation, system controls, and reporting required.

Key Preparation Steps:

1. Documenting Compliance:

   Requirement: Companies must maintain detailed records of their TRM policies, cybersecurity measures, and incident reports.

   Steps to Take:

   - Keep an updated register of critical systems and their recovery plans.
   - Maintain a log of all security patches, system updates, and incident responses.

2. Conducting Internal Audits:

   Requirement: Regular internal audits must be conducted to ensure the effectiveness of TRM and cybersecurity measures.

   Steps to Take:

   - Schedule periodic internal audits of systems, policies, and processes.
   - Report findings to senior management and rectify any compliance gaps.

© 2024, FailSafe and LDU. All Rights Reserved.

3. MAS Inspection Checklist:

   Requirement: Ensure readiness for MAS inspections by preparing a detailed checklist that covers all areas of compliance.

   Steps to Take:

   - Compile a checklist of key compliance areas, including system security, incident reporting, and cybersecurity controls.
   - Conduct mock inspections to ensure all regulatory requirements are met.

© 2024, FailSafe and LDU. All Rights Reserved.

Summary of Services

FailSafe

FailSafe provides a comprehensive suite of technical solutions to help digital asset companies meet MAS's Technology Risk Management (TRM) requirements.

Guard: Enhancing Smart Contract Security through Access Control

FailSafe's Guard is a robust access control tool that fortifies the operational security of smart contracts. By integrating multi-signature mechanisms and rigorous security checks, Guard ensures that privileged operations are carried out exclusively by authorized personnel. Any transaction failing to meet these stringent criteria is blocked, ensuring that only legitimate and verified actions proceed. This tool adds an essential layer of protection, minimizing the risk of unauthorized transactions and insider threats.

Interceptor: Real-Time Defense Against Blockchain Attacks

A critical feature of FailSafe's suite is Interceptor, a revolutionary tool designed to actively counter blockchain-based attacks. When a potential hack or unauthorized transaction is detected, Interceptor executes a protective transaction that swiftly moves vulnerable funds to a secure, self-custody smart contract wallet. With a remarkable 99.8% success rate, Interceptor monitors pending transactions in the memory pool, identifying potential threats in real-time. By preemptively deploying protective measures, Interceptor effectively defends enterprise treasuries and funds from malicious actors, offering unparalleled peace of mind.

Radar: AI-Powered Risk Intelligence and Monitoring for Regulatory Compliance

In an era where compliance with AML regulations is increasingly scrutinized, FailSafe's Radar provides enterprises with a powerful tool for monitoring blockchain transactions. Utilizing artificial intelligence (AI) and machine learning (ML), Radar detects anomalous transaction patterns indicative of fraud, theft, and sybil attacks. By continuously analyzing money movements, Radar helps enterprises remain compliant with AML regulations while identifying potential instances of payment fraud and money laundering in real-time, ensuring both operational integrity and regulatory compliance.

AuditAI and Certified Audits: Streamlining Smart Contract Auditing for Developers

As smart contracts evolve, maintaining security during updates is essential. FailSafe's AuditAI automates vulnerability detection in Solidity contracts, providing instant insights and best practice recommendations to enhance code quality. This streamlines a traditionally costly and time-consuming process, allowing developers to address security gaps proactively. For added assurance, FailSafe's certified auditors conduct manual reviews to strengthen protection, ensuring continuous compliance and minimizing exploitation risks.

© 2024, FailSafe and LDU. All Rights Reserved.

LDU

LDU offers regulatory advisory services tailored to help digital asset companies understand and comply with MAS's TRM requirements under the Payment Services Act.

Governance and Strategy Development

Comprehensive support is provided in establishing governance structures and risk management frameworks, setting up board-level oversight, and formulating compliance strategies that align with MAS guidelines. This foundational work is crucial for fostering accountability and transparency within organizations, enabling them to operate with confidence.

Risk Management and Compliance Consulting

Expert legal consulting assists companies in developing and implementing robust policies for IT security, data protection, and incident reporting. Aligning these policies with regulatory requirements such as FSM-N13 and FSM-N14 ensures that companies are not only compliant but also prepared to respond effectively to potential risks and regulatory scrutiny.

Data Protection and Privacy Services

Targeted legal consulting to ensure compliance with the PDPA as enforced by Singapore's Personal Data Protection Commission (PDPC). Our services include the support of DPO advisors, creation of data maps, drafting of data protection policies, and development of data breach response plans. Also assisting in formulating privacy policies, conducting employee training sessions on PDPA requirements, assessing management of data subjects' rights, and drafting third party data processing addendums.

Audit and Inspection Preparation

Expert guidance is available to help companies prepare for MAS audits and inspections, including conducting thorough internal audits and assembling the necessary compliance documentation. This preparation minimizes the likelihood of compliance breaches and enhances the organization's credibility during regulatory assessments.

Disclaimer: Any details provided in this publication are purely for educational and informational purposes only. This does not constitute legal or compliance advisory services in any way, shape, or form.

© 2024, FailSafe and LDU. All Rights Reserved.

Complimentary Security & Compliance Consultation

As regulatory scrutiny and cyber threats continue to increase, ensuring both security and compliance for your blockchain operations has never been more critical. FailSafe's suite of solutions including Guard, Interceptor, Radar, and AuditAI can help you safeguard your assets, prevent breaches, and meet strict compliance requirements like those outlined by MAS and other regulatory bodies.

We're offering a **complimentary 30-minute consultation** with our certified blockchain security and compliance experts to assess your current posture, identify potential vulnerabilities, and discuss tailored strategies to protect your organization while achieving full regulatory compliance.

To ensure we can address your specific needs, please fill out the form below and submit to **hello@getfailsafe.com**, which will help us prioritize your requirements and urgency.

1. Company Name:
2. HQ location:
3. Contact Person & Title:
4. Email Address:
5. Primary Concern:
    - Compliance with regulations (e.g., MAS, AML, etc.)
    - Smart contract security
    - Real-time transaction monitoring
    - Internal access controls
    - Other (please specify)
6. Are you actively looking for a security or compliance solution?
    - Yes, within the next 1-3 months
    - Yes, within the next 3-6 months
    - We're exploring options, no immediate timeline
7. Do you have a budget allocated for blockchain security and compliance?
    - Yes
    - No
    - Not sure yet
8. How would you rate the urgency of addressing these needs?
    - High — need a solution immediately
    - Medium — solution needed within 3 months
    - Low — planning for future needs

After submitting the form, our team will reach out to schedule your free consultation, providing expert guidance and actionable insights to ensure your blockchain operations are secure and fully compliant with regulatory standards. Secure your consultation today and take the next step in protecting your business and reputation.

© 2024, FailSafe and LDU. All Rights Reserved.