STYN RISK MANAGEMENT FRAMEWORK

Comprehensive Risk Identification, Assessment & Mitigation

Smart Contract | Market & Liquidity | Operational & Counterparty

Risk management framework v1.1 | SYTN | May 2026

DISCLAIMER PAGE

IMPORTANT NOTICE & LEGAL DISCLAIMER

Nature of this Document

This document has been prepared by SYTN Foundation for informational and technical purposes only. It describes the risk management framework of the SYTN protocol as currently designed and implemented by the founding team. It does not constitute, and shall not be construed as, a prospectus, an offer to sell, or a solicitation of an offer to buy any securities, financial instruments, or investment products in any jurisdiction. It does not constitute financial, legal, tax, or investment advice of any kind. Readers seeking the complete investment disclaimer, token classification notice, restricted jurisdiction disclosure, and forward-looking statements notice are directed to the SYTN Protocol whitepaper, version 1.2, published May 2026 by SYTN Foundation.

No Representation on Completeness or Accuracy

While SYTN Foundation has taken reasonable care in preparing this document, no representation or warranty, express or implied, is made as to the accuracy, completeness, or fitness for any particular purpose of the information contained herein. The risk assessments, governance parameters, mitigation strategies, and architectural specifications described in this document are subject to change without notice at the discretion of SYTN Foundation and its DAO governance structure. The identification of a risk within this framework does not imply that such risk is fully mitigated or eliminated; where residual risk remains material, this document states so explicitly.

Technology and Protocol Risks

Participation in the SYTN protocol involves significant risks, including but not limited to smart contract vulnerabilities, oracle failures, collateral volatility, regulatory reclassification, liquidity constraints, and adverse market conditions. Prospective participants should carefully review the risk disclosures section of the SYTN Protocol whitepaper and conduct their own independent due diligence before making any decision to participate. SYTN Foundation accepts no liability for any loss or damage arising from reliance on this document or participation in the protocol.

Jurisdiction

This document is governed by the laws of Switzerland. SYTN Foundation, incorporated under Swiss law, is the primary legal entity responsible for protocol governance, intellectual property, and primary token issuance. Any disputes arising in connection with this document shall be subject to the exclusive jurisdiction of the competent courts of Switzerland, without prejudice to mandatory consumer protection provisions applicable in other jurisdictions.

SYTN Foundation intends to establish an Italian operational entity as part of its dual-jurisdiction legal architecture, designed to provide direct EU market access under EU Regulation 2023/1114 (MiCA) and to passport regulated crypto asset services across all European Union member states from a single point of authorisation, as described in the SYTN Protocol whitepaper, version 1.1, May 2026. Upon incorporation of the Italian operational entity and grant of Crypto Asset Service Provider authorisation

by the competent Italian authority, disputes arising from MiCA-regulated services provided to EEA participants will be subject to Italian jurisdiction and applicable EU law in accordance with MiCA Title V, which cannot be contractually derogated. Until such time, all matters remain governed exclusively by Swiss law.

INTELLECTUAL PROPERTY NOTICE

All content, methodologies, architectural designs, technical specifications, and governance innovations described in this document are the exclusive intellectual property of SYTN Foundation and its founding team, protected under applicable copyright, trade secret, and intellectual property law in Switzerland, Italy, the European Union, and other relevant jurisdictions. SYTN Foundation intends to establish an Italian operational entity as part of its dual-jurisdiction legal architecture, as described in the SYTN Protocol whitepaper, version 1.1, May 2026. Upon its incorporation, all intellectual property rights described herein will additionally benefit from the regulatory and legal framework applicable to that entity under Italian law and EU Regulation 2023/1114 (MiCA). The incorporation of any future operational entity does not constitute a transfer, division, or licensing of any intellectual property rights described herein; all proprietary innovations remain the exclusive property of SYTN Foundation regardless of the jurisdiction through which regulated services are delivered.

The following constitute proprietary governance innovations of SYTN Foundation for which all rights are expressly reserved.

Multi-signature governance architecture, the specific tripartite authority model separating operator, governor, and default admin roles within a single protocol governance system, including all associated permission hierarchies, constraint logic, and the principle that operational exposure is inversely proportional to authority level.

Institutional signer configuration framework, the criteria-based methodology for selecting and structuring independent multisig signers according to principles of institutional credibility, financial independence from protocol operations, and jurisdictional diversity, including the 3-of-5 threshold design and its associated mutual dependency logic.

DAO-to-multisig sequential validation framework, the governance architecture in which community voting via DAO precedes multisig execution as a democratic legitimacy verification layer, including all associated procedural integrity criteria and the constitutional distinction between substantive veto and procedural attestation.

Additional proprietary innovations of SYTN Foundation, including the price discovery engine, Decay-Adjusted VWAP mechanism, Decay-Adjusted TWAP fallback, universal asset wrapper, and compliance abstraction layer, are described and protected in the SYTN Protocol whitepaper and associated technical documentation. The publication of this document does not constitute a grant, waiver, or license of any intellectual property rights described above or in any other SYTN Foundation document.

Unauthorized reproduction, distribution, adaptation, or commercial use of any content or methodology described herein, in whole or in part, without prior written authorization from SYTN Foundation is strictly prohibited and may give rise to civil and criminal liability under applicable law. For licensing inquiries or institutional due diligence access: legal@sytnfinance.com

SYTN PROTOCOL

TABLE OF CONTENTS

1. Purpose & scope

This document establishes the risk management framework for the SYTN protocol. It is designed to identify, assess, mitigate, and monitor the principal risks facing the protocol across four domains: smart contract and technical infrastructure, regulatory and legal compliance, market and liquidity dynamics, and operational and counterparty exposures. The framework reflects the state of the protocol as of its first official notarised release and will be updated as the protocol matures, new risks emerge, and mitigation strategies are validated or revised through operational experience.

The framework serves two distinct but complementary purposes.
The first is operational discipline: the establishment of clear ownership, mitigation strategies, and monitoring cadences for each identified risk, ensuring that risk management is embedded in daily operations rather than treated as a periodic compliance exercise.
The second is investor and regulatory readiness: the demonstration to prospective investors, institutional partners, and regulatory authorities that SYTN approaches risk management with the rigour and transparency consistent with institutional standards.

It should be noted that the identification of a risk within this framework does not imply that such risk is fully mitigated or eliminated. Where residual risk remains material, this document states so explicitly, as candour on this point is considered essential to the integrity of the framework.

The scope of this document covers SYTN's core protocol infrastructure, encompassing the universal asset wrapper, the compliance abstraction layer, the matching and settlement engine, and the cross-chain vault network. It further covers the SYTN token and its economic mechanisms, all supported originating chains and their vault contracts, and the off-chain backend systems that orchestrate cross-chain settlement and compliance verification. Risks arising outside this perimeter, including macro-economic conditions, systemic events in the broader digital asset market, and regulatory developments not directly targeted at SYTN, are acknowledged as material but fall outside the scope of this framework's mitigation strategies.

2. Risk governance structure

Risk governance at SYTN follows a three-tier authority model, established in the protocol's multi-signature governance framework. Each tier carries defined responsibilities and clearly specified escalation thresholds, ensuring that risk events are handled at the appropriate level of authority without unnecessary delay or escalation bottlenecks.

Level	Risk responsibility	Escalation threshold
Operational	Day-to-day risk monitoring, automated alerts, incident response for low and medium severity events.	Any event exceeding medium severity or affecting more than 1% of TVL is escalated immediately.
Management	Weekly risk review, mitigation strategy ownership, resource allocation for risk reduction initiatives, regulatory engagement.	Any high severity event, any regulatory inquiry, any event requiring public communication.
Multisig	Critical risk decisions, emergency protocol pause, governance parameter changes, strategic risk acceptance decision.	Any critical severity event, any event requiring protocol pause, any risk acceptance decision with material financial or regulatory impact.

The three-tier model is designed to preserve operational agility at the lower levels while ensuring that decisions with systemic or irreversible consequences are subject to appropriate deliberation and multi-party approval. A risk acceptance decision, defined as a formal acknowledgement that a known risk will not be actively mitigated within a defined timeframe, may only be taken at the multisig level and must be documented with a written rationale that is retained in the protocol's governance record.

3. Risk assessment methodology

Each risk is assessed on two dimensions: likelihood, representing the probability of the risk materialising within a 12-month horizon, and impact, representing the severity of consequences if materialisation occurs. The product of these two dimensions yields a composite risk score that determines the risk classification and the required management response.

3.1 Likelihood scale

Level	Score	Definition
Rare	1	Less than 5% probability within 12 months. Requires exceptional circumstances.
Unlikely	2	5-20% probability. Could occur but not expected under normal conditions.
Possible	3	20-50% probability. Has occurred in comparable protocols or markets.
Likely	4	50-80% probability. Expected to occur at some point during operations.
Almost certain	5	Greater than 80% probability. Will almost certainly occur.

3.2 Impact scale

Level	Score	Definition
Negligible	1	Less than $50K financial impact. No operational disruption. No regulatory attention.
Minor	2	$50K-$500K impact. Brief operational disruption (<4 hours). Minor reputational concern.
Moderate	3	$500K-$5M impact. Significant operational disruption (4-48 hours). Regulatory inquiry possible.
Major	4	$5M-$50M impact. Extended disruption (days). Regulatory action probable. Material reputational damage.
Catastrophic	5	Greater than $50M or total loss of user funds. Protocol viability threatened. Regulatory enforcement. Existential reputational damage.

3.3 Risk rating matrix

The composite risk rating is the product of likelihood and impact scores. Ratings are classified as follows:

Critical (16-25), requiring immediate attention and active mitigation with no risk acceptance permitted;

High (10-15), requiring a management-level mitigation plan with a defined timeline;

Medium (5-9), managed through standard operational controls and reviewed monthly;

Low (1-4), accepted with monitoring and reviewed quarterly.

L \ I	Negligible (1)	Minor (2)	Moderate (3)	Major (4)	Catastrophic (5)
Rare (1)	1	2	3	4	5
Unlikely (2)	2	4	6	8	10
Possible (3)	3	6	9	12	15
Likely (4)	4	8	12	16	20
Almost certain (5)	5	10	15	20	25

4. Smart contract & technical risks

Smart contract and technical risks represent the most acute threat category for SYTN, as they can result in direct, immediate, and potentially irreversible loss of user funds. The mitigation strategies described in this section reflect a defence-in-depth philosophy: no single control is considered sufficient in isolation, and the failure of any one layer should not be capable of producing a catastrophic outcome on its own. It should be noted that even with the controls described below, residual risk cannot be reduced to zero, and the protocol acknowledges this limitation explicitly rather than presenting an artificially optimistic picture of its security posture.

SC-01: smart contract vulnerability in vault contracts

Likelihood	Impact	Rating	Owner
Possible (3)	Catastrophic (5)	Critical	CTO / Engineering Lead

A vulnerability in a vault contract on any supported chain could allow an attacker to drain the locked underlying assets. Because vaults custody the real assets backing all UAW tokens, a vault exploit would break the 1:1 backing guarantee and potentially result in total loss of the affected assets.

This risk is classified critical because the consequence of materialisation would be existential for the protocol.

The primary mitigation is a mandatory pre-deployment security process that requires all vault contracts to undergo a minimum of two independent security audits from reputable firms before deployment. This requirement is non-negotiable and admits no exception, regardless of schedule pressure.

Alongside traditional auditing, a formal verification programme is initiated for vault contracts, mathematically proving that the lock and release invariants hold under all possible inputs, a standard of assurance that goes beyond what conventional auditing can provide. To contain the blast radius of any residual vulnerability that may survive these processes, vault TVL limits are imposed during the first 90 days of deployment on each new chain, restricting maximum deposits to $10 million until the contracts have operated without incident.

A bug bounty programme with a maximum payout of 10% of TVL, capped at $1 million, is operated through the protocol's designated bug bounty programme to incentivise responsible disclosure. If an exploit does occur, the compliance and insurance fund, allocated at 5% of total token supply, provides partial coverage for affected users, though the protocol acknowledges that this fund is not sized to cover a total loss scenario.

SC-02: smart contract vulnerability in vault contracts

Likelihood	Impact	Rating	Owner
Possible (3)	Major (4)	High	Infrastructure Lead

The off-chain backend that relays burn proofs from SYTN to vault contracts on native chains could be compromised, resulting in fabricated release instructions, censored withdrawals, or delayed settlement. The critical design principle that governs this risk is the separation of relay authority from proof validity: vault contracts independently verify burn proofs before releasing assets, meaning that a compromised relayer cannot fabricate valid release instructions, it can only delay them. This constraint materially limits the severity of a relay compromise from catastrophic to operational disruption.

To address the liveness dimension of this risk, multiple authorised relayers are configured for each chain, eliminating the single point of failure that a sole relayer would represent.

A time-locked escape hatch further protects users by allowing them to submit burn proofs directly to the vault after a 72-hour delay if no relayer processes their withdrawal.

This mechanism ensures that even a complete and sustained relay failure cannot permanently prevent users from accessing their assets. All relay operations are logged immutably, enabling post-incident forensic analysis and providing regulators and auditors with a complete audit trail of settlement activity.

SC-03: update mechanism exploitation

Likelihood	Impact	Rating	Owner
Unlikely (2)	Catastrophic (5)	High	CTO / Multisig Signers

If the upgrade mechanism for vault or settlement contracts is compromised, an attacker could deploy a malicious contract version that redirects assets. The governance architecture applied to this risk reflects a deliberate trade-off between operational flexibility and security: all upgrades are governed by the Protocol Timelock with a mandatory 48-hour delay, creating a public review window during which any participant can examine the proposed change and raise an alert if the upgrade appears malicious.

Execution requires 3-of-5 multisig approval from the default admin, ensuring that no single actor, whether internal or external, can unilaterally deploy a contract change.

Upgrade proposals include the new contract bytecode hash, enabling independent verification before execution.

The most robust protection, however, is architectural: phase 1 vault contracts are intentionally non-upgradeable, meaning that immutability is the default position and upgradeability a capability introduced only in phase 2 with additional safeguards. This phased approach accepts some operational

inflexibility in exchange for a materially reduced attack surface during the period when the protocol is most vulnerable.

SC-04: oracle / price feed manipulation

Likelihood	Impact	Rating	Owner
Possible (3)	Major (4)	High	CTO

If SYTN relies on external price feeds for collateral valuation, cross-asset margining, or fee calculation, manipulation of these feeds could result in incorrect liquidations, mispriced trades, or protocol insolvency. The mitigation architecture for this risk is built around two complementary principles: statistical redundancy and circuit breaker automation.

Multiple independent oracle sources are aggregated with outlier detection, using the median of N sources and rejecting values that deviate by more than two standard deviations from the median, a design that requires an attacker to compromise or manipulate a majority of oracle sources simultaneously to produce a materially false price signal.

Automated circuit breakers halt trading if price feeds deviate by more than 10% within a five-minute window, limiting the damage window if manipulation does occur. Critically, phase 1 does not include cross-asset margining, deliberately deferring the most complex oracle dependency to phase 2 when the infrastructure is more mature and battle-tested.

SC-05: backend infrastructure failure

Likelihood	Impact	Rating	Owner
Likely (4)	Moderate (3)	High	Infrastructure Lead

The off-chain backend, encompassing the matching engine, compliance oracle, and cross-chain relayer, is a centralised component whose failure could halt trading and settlement.

The critical design constraint that governs this risk is the principle that backend failure must never result in loss of funds, only loss of service availability, a guarantee enforced by committing all critical state on-chain, so that no off-chain failure can affect the integrity of user balances.

Availability risk is managed through multi-region deployment with automatic failover, a stateless architecture for the matching engine and compliance cache that enables horizontal scaling under load, and a target uptime SLA of 99.9%, equivalent to less than 8.7 hours of downtime per year.

5. Market & liquidity risks

Market and liquidity risks are inherent to operating a secondary market for tokenized assets. These risks are amplified in the current environment by the nascent state of institutional participation in on-chain markets, the thin order books characteristic of early-stage protocols, and the cross-chain complexity of SYTN's architecture, which introduces additional friction in the liquidity aggregation process.

ML-01: liquidity cold start failure

Likelihood	Impact	Rating	Owner
Possible (3)	Catastrophic (5)	Critical	CEO / Business Development

SYTN's core value proposition depends on concentrating sufficient liquidity to produce tighter spreads than protocol-native order books. If the cold-start phase fails to attract critical mass, the platform enters a self-reinforcing deterioration dynamic: thin order books produce wide spreads, wide spreads discourage participation, and reduced participation thins the order books further. This risk is classified critical due to the existential consequences of materialisation, a protocol that cannot attract and retain liquidity has entirely different outputs.

Foundational mitigation measures

The primary liquidity bootstrap mechanism is the ecosystem incentive allocation, representing 35% of total token supply and specifically designed to incentivise market-making activity through maker rebates, liquidity provider rewards, and trading fee discounts.

This allocation is deliberately front-weighted in its release schedule to maximise its impact during the cold-start window, when liquidity is most scarce and the marginal value of each additional unit of depth is highest. Alongside the incentive allocation, the protocol commits to securing 5-10 anchor issuers as launch partners before the platform opens to the public, ensuring that a minimum set of listed assets exists from day one rather than being built post-launch under adverse conditions.

The phase 1 focuses on few asset classes, reflecting this logic: concentrating the available liquidity in one niche to achieve meaningful depth rather than distributing it thinly across multiple asset classes where it would be insufficient to produce a compelling trading experience.

Market maker engagement: initial framework

The protocol plans to engage 2-3 professional market makers under contractual obligations to provide minimum liquidity levels for an initial 12-month period. These arrangements represent the most operationally critical mitigation for ML-01, and the design of the engagement framework, including the terms of initial commitment, the mechanisms for renewal, and the structures for performance enforcement, is addressed comprehensively in Appendix B of this document. The following section

summarises the key architectural principles; readers seeking the full specification are directed to Appendix B.

Market maker renewal and preferential fee structure

The expiry of initial 12-month market maker commitments represents a structural vulnerability that the original framework did not address. If the protocol must renegotiate from a position of liquidity dependence at month twelve, the balance of negotiating power will have shifted materially in favour of the market makers, with consequences for fee conditions, volume commitments, and overall protocol economics.

The mitigation to this dynamic is the establishment of a preferential renewal fee structure, a formalised tiered rebate system in which market makers that renew their agreements receive progressively improved economic conditions relative to those applicable to new entrants.

The renewal discount is calculated as a function of two variables: the cumulative duration of the market maker's engagement with the protocol and the performance score accumulated during the preceding period. A market maker entering its second year of agreement may receive a maker rebate up to 30% more favourable than the base rate applicable in year one, conditional on having met its key performance indicators consistently throughout the initial term. This structure transforms the decision to renew from a purely commercial negotiation into an economically self-reinforcing one: the longer a market maker remains, the more favourable its conditions become, and the higher the cost-opportunity of migration to a competing platform. The renewal fee structure is codified in the market maker's registered market maker smart contract, ensuring that its application is automatic, verifiable, and not subject to discretionary modification by protocol operators.

Two-speed market maker architecture

Rather than treating all engaged market makers as interchangeable, the protocol adopts a differentiated structure that designates one entity as Primary Market Maker and one or two additional entities as Secondary Market Makers.

The Primary Market Maker carries elevated volume obligations, a larger performance bond, and access to the most favourable rebate tiers.

The Secondary Market Makers operate under reduced obligations but remain continuously active and familiar with the protocol's order book.

This architecture ensures that no single market maker departure can produce a liquidity vacuum: if the Primary Market Maker underperforms or exits, the Secondary Market Makers are already operational and can absorb a material portion of the liquidity obligation while a replacement Primary is identified and onboarded.

Liquidity incentive ratchet

The minimum performance thresholds defined in market maker agreements represent a floor, not a target. To prevent market makers from anchoring their activity precisely at the contractual minimum, the protocol implements a liquidity incentive ratchet: a dynamic mechanism under which the maker rebate increases automatically each quarter in which the market maker exceeds its volume target by a defined margin. A market maker whose guaranteed monthly volume is $10 million but who consistently delivers $15 million receives an upward ratchet of 5% on its rebate tier for the subsequent quarter. This converts the agreement from a compliance obligation into a continuous performance incentive, and it does so through on-chain automation that requires no discretionary intervention from protocol operators.

ML-02: SYTN token price volatility

Likelihood	Impact	Rating	Owner
Almost certain (5)	Moderate (3)	Critical	Treasury / CFO

Because trading fees and compliance staking are denominated in SYTN, extreme token price volatility creates unpredictable costs for users and issuers. A sharp SYTN price decline could also trigger a cascade of compliance stake liquidations.

Fee schedules are denominated in SYTN but referenced to a USD-equivalent value, with automatic adjustment mechanisms that smooth costs for users during volatile periods.

Compliance staking requirements include a buffer zone under which slashing is triggered only if the staked value falls below 80% of the required minimum, providing meaningful cushion against price fluctuations without compromising the deterrent function of the staking mechanism.

The treasury maintains a stablecoin reserve, denominated in USDC and USDT, sufficient to cover six months of operational expenses, ensuring that protocol operations can continue without interruption through extended periods of token price weakness.

These measures collectively reduce the operational sensitivity of the protocol to token price movements; however they cannot, address the underlying volatility itself, which is driven by market forces outside the protocol's control.

ML-03: cross-chain backing de-peg

Likelihood	Impact	Rating	Owner

Unlikely (2)	Catastrophic (5)	High	CTO

If the market loses confidence in the 1:1 backing of UAW tokens, whether due to a vault exploit on one chain, delayed withdrawals, or unverifiable Merkle proofs, UAW tokens could trade at a discount to their underlying assets, triggering a bank-run dynamic. The consequences of this scenario are classified catastrophic because they could undermine the foundational value proposition of the entire protocol.

The primary mitigation is continuous proof-of-reserves published on-chain, verifiable by any participant at any time, a transparency standard that eliminates the information asymmetry that typically precedes confidence crises.

Independent third-party attestation of vault balances is conducted quarterly, providing an authoritative external verification that complements the continuous on-chain data.

Circuit breakers that automatically pause wrapping and unwrapping if the UAW-to-underlying price ratio deviates by more than 2% on external markets provide a rapid-response mechanism that limits the scale of any confidence event before it becomes self-sustaining.

Pre-written crisis communication templates are maintained and tested, ensuring that the protocol can respond to a confidence event rapidly and coherently rather than improvising under pressure.

ML-04: market manipulation

Likelihood	**Impact**	**Rating**	**Owner**
likely (4)	Moderate (3)	High	Compliance / engineering

Thin order books in the early stages of the protocol are inherently vulnerable to wash trading, spoofing, layering, and other manipulative practices. If detected by regulators, such activity could result in enforcement action against SYTN regardless of whether the protocol itself was a party to or beneficiary of the manipulation.

The surveillance architecture implemented to address this risk operates in real time, monitoring continuously for wash trading patterns characterised by same-beneficiary trades, spoofing activity identified through large orders cancelled within short windows, and layering patterns that create artificial price pressure.

Mandatory identity linkage across accounts prevents the same entity from trading with itself through multiple addresses, closing the most straightforward circumvention route.

Suspicious activity reports (SARs) are filed with relevant authorities when manipulation is detected, ensuring that the protocol meets its regulatory obligations and positions itself as a cooperative participant in market integrity rather than a passive observer.

6. Operational & counterparty risks

Operational and counterparty risks encompass the human, organisational, and third-party dimensions of protocol risk, areas where smart contract design and cryptographic guarantees offer limited protection, and where the quality of people, processes, and relationships determines outcomes. These risks are in some respects more difficult to manage than technical risks precisely because they resist quantification and cannot be fully automated away.

OP-01: key person dependency

Likelihood	Impact	Rating	Owner
likely (4)	Major (4)	Critical	CEO

In an early-stage protocol, critical knowledge about architecture, key management procedures, regulatory relationships, and operational processes tends to concentrate in one or two individuals. The loss of these individuals, whether through departure, incapacitation, or any other cause, could severely impair the protocol's ability to operate, respond to incidents, and maintain regulatory relationships.

This risk receives the highest composite score among all operational risks, and the protocol does not consider any of the mitigations described below to reduce it below high. The residual risk is acknowledged explicitly, and its management is treated as a standing priority at the CEO level rather than a periodic task.

Strengthened mitigation framework

The existing multisig architecture, with its 3-of-5 signer structure, ensures that no single individual's unavailability can prevent governance decisions from being executed.

To address the knowledge concentration dimension, the protocol implements a mandatory knowledge management programme that goes beyond conventional documentation. Every critical system, procedure, and regulatory relationship is documented in structured form, and documentation updates are treated as a release requirement rather than a discretionary activity, no protocol change is considered complete until the corresponding documentation has been updated and reviewed by at least one additional team member.

The protocol further establishes a shadow role programme under which each critical position has a designated understudy who participates in all material decisions for a minimum of 90 consecutive days before being considered operationally ready.

Retention risk is addressed through a long-term incentive structure in which the vesting schedules of key personnel include cliff provisions specifically designed to make near-term departure economically costly, without creating the contractual rigidities that conflict with the protocol's need to manage underperformance decisively.

Finally, a quarterly bus factor assessment, a structured review of which systems and processes would be critically impaired by the loss of any single individual, is conducted at the management level, with the explicit mandate to identify and eliminate knowledge bottlenecks before they become operational vulnerabilities.

OP-02: third-party KYC/AML provider failure

Likelihood	Impact	Rating	Owner
Possible (3)	Moderate (3)	Medium	Compliance

SYTN's compliance architecture relies on third-party identity verification and sanctions screening providers. If a provider suffers an outage, a data breach, or delivers systematically inaccurate results, SYTN's ability to onboard users and maintain compliance is impaired.

A multi-provider architecture ensures that at least two independent KYC/AML providers are integrated with automatic failover, so that a single provider failure does not halt the onboarding.

Provider service level agreements include uptime guarantees, data accuracy commitments, and breach notification obligations, providing contractual recourse in addition to technical redundancy. A random sample of completed verifications is re-checked against independent sources on a quarterly basis, ensuring that systematic accuracy failures are detected before they produce material compliance gaps.

OP-03: counterparty risk, issuer default

Likelihood	Impact	Rating	Owner
Possible (3)	Moderate (3)	Medium	Legal

If an issuer of a tokenized asset listed on SYTN defaults, becomes insolvent, or is found to have misrepresented the underlying asset, holders of the corresponding UAW tokens suffer losses. Although SYTN operates as a marketplace and not as an issuer, the protocol acknowledges that reputational contagion from a significant issuer failure could be material regardless of the legal distinction.

Compliance staking requires issuers to lock SYTN tokens proportional to their listed asset's market capitalisation, with this stake slashable if misrepresentation is proven, providing partial compensation to affected holders while creating a direct financial disincentive against misrepresentation.

Listing conditions require issuers to provide audited financial statements, legal opinions confirming asset legitimacy, and ongoing disclosure obligations, establishing a due diligence standard comparable to that applied in regulated markets.

SYTN's terms of service and user interface clearly communicate that SYTN is a marketplace that does not guarantee the performance of listed assets, a disclosure that is considered both a legal necessity and an ethical obligation.

OP-04: multisig signer collusion or compromises

Likelihood	Impact	Rating	Owner
Rare (1)	Catastrophic (5)	Medium	All Signers

If three of the five multisig signers collude or are simultaneously compromised, an attacker would gain full default admin authority, including the ability to pause the protocol, replace the operator, and approve governance changes.

The probability of this scenario is assessed as rare, reflecting the deliberate design of the signer set: signers are distributed across different organisations, jurisdictions, and infrastructure providers, making coordinated compromise exceptionally difficult to execute.

Hardware security modules or hardware wallets are mandatory for all signers, and quarterly key rotation limits the window of exposure for any key that may have been compromised without detection.

The critical architectural constraint that bounds the impact of even a full multisig compromise is that vault releases still require verified burn proofs, meaning that a multisig compromise is a serious governance failure but not, by itself, a mechanism for fund theft.

OP-05: data breach of off-chain compliance records

Likelihood	Impact	Rating	Owner
Possible (3)	Major (4)	High	CTO

The off-chain compliance data store contains sensitive personal information including KYC documents, identity verification results, and source-of-funds data. A breach would violate GDPR, expose users to identity theft, and cause severe reputational damage.

All compliance data is encrypted at rest using AES-256 and in transit using TLS 1.3. Access is restricted through role-based access control with mandatory multi-factor authentication, ensuring that the attack surface for insider threats is minimised. All EU user data is stored exclusively in EU-based data centres in full compliance with GDPR data residency requirements

A Data Protection Officer is appointed as required under GDPR, with independent authority to audit data handling practices across the organisation. The incident response plan includes a 72-hour breach notification capability as required by GDPR Article 33, ensuring that regulatory obligations can be met even under the time pressure of an active incident.

7. Risk register summary

The following table consolidates all identified risks with their current ratings, providing a single view dashboard.

Risk ID	Description	Category	L x I	Rating	Owner
SC-01	Smart contract vulnerability in vault contracts	Technical	3 x 5= 15	Critical	CTO
SC-02	Cross-chain relay compromise	Technical	3 x 4= 12	High	Infra Lead / CTO
SC-03	Upgrade mechanism exploit	Technical	2 x 5= 10	High	CTO
SC-04	Oracle / price feed manipulation	Technical	3 x 4= 12	High	CTO
SC-05	Backend infratructure failure	Technical	4 x 3= 12	High	Infrastructure Lead
ML-01	Liquidity cold-start failure	Market	3 x 5= 15	Critical	CEO / BD
ML-02	SYTN token price volatility	Market	5 x 3= 15	Critical	Treasury
ML-03	Cross-chain backing de-peg	Market	2 x 5= 10	High	Risk
ML-04	Market manipulation	Market	4 x 3= 12	High	Compliance
OP-01	Key person dependency	Operational	4 x 4= 16	Critical	CEO
OP-02	KYC/AML provider failure	Operational	3 x 3= 9	Medium	Compliance
OP-03	Issuer default / misrepresentation	Operational	3 x 3= 9	Medium	Legal
OP-04	Multisgi signer collusion	Operational	1 x 5= 5	Medium	Legal
OP-05	Compliance data breach	Operational	3 x 4= 12	High	CTO

8. Appendix A, risk scoring matrix

The 5×5 risk scoring matrix used in this framework. Cell values represent the composite risk score (likelihood × impact). Colour coding corresponds to risk classification thresholds.

L \ I	Negligible (1)	Minor (2)	Moderate (3)	Major (4)
Rare (1)	1	2	3	4
Unlikely (2)	2	4	6	8
Possible (3)	3	6	9	12
Likely (4)	4	8	12	16
Almost certain (5)	5	10	15	20

Classification thresholds:
Critical 15-25
High 10-15
Medium 5-9
Low 1-4

9. Appendix B, market maker agreement framework

B.1 Purpose and strategic rationale

The appendix establishes the formal framework governing SYTN's engagement with professional market makers. It should be read in conjunction with section 5 of this document, specifically the mitigation architecture for ML-01 (liquidity cold-start failure), of which it constitutes the operational specification. The framework addresses four interconnected objectives: the formalisation of initial engagement terms, the structural incentivisation of long-term renewal, the enforcement of performance obligations during the agreement period, and the mitigation of systemic risks arising from market maker concentration and potential coordination.

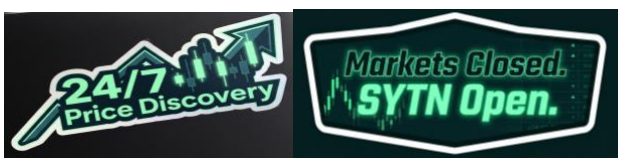
The strategic importance of this framework cannot be overstated. Market maker liquidity is not merely one input among many in SYTN's value proposition, it is the mechanism through which the protocol's core promise to users is delivered. A market maker that underperforms during a stress event, or that uses the leverage of its liquidity position to extract unfavourable renewal terms, does not simply impose a cost on the protocol: it undermines the user experience at precisely the moment when it is most critical. The framework described below is designed to make such outcomes structurally less likely, not through the optimistic assumption of aligned interests, but through the deliberate alignment of economic incentives and the clear specification of consequences when performance obligations are not met.

B.2 Market maker tiers: the two-speed architecture

The protocol designates market makers at two distinct tiers, each carrying different obligations, economic entitlements, and strategic roles.

The Primary Market Maker tier is occupied by a single entity that accepts the highest volume obligations, posts the largest performance bond, and in exchange accesses the most favourable rebate tiers available under the programme. The Primary Market Maker is expected to maintain continuous two-sided markets across all listed asset classes within its designated scope, with defined maximum spread and minimum depth requirements that always apply including periods of market stress. The designation of a single entity as primary reflects the operational reality that the most capable liquidity providers require exclusive economic recognition to commit their deepest resources; it does not imply that the protocol is operationally dependent on this single entity, because the secondary tier is specifically designed to prevent that dependency.

The Secondary Market Maker tier accommodates one or two additional entities that operate under reduced volume obligations but remain continuously active participants in the protocol's order book. Secondary Market Makers serve two simultaneous functions: they provide genuine incremental liquidity during normal operating conditions, and they constitute the protocol's primary operational



contingency in the event of Primary Market Maker underperformance or departure. Because Secondary Market Makers are already familiar with the protocol's order book structure, trading patterns, and technical interface, their activation in a contingency scenario requires no onboarding time and produces no gap in liquidity provision.

B.3 Formalisation of market maker agreements in a DeFi context

Formalising binding commitments in a decentralised protocol environment requires an approach that neither relies exclusively on traditional contractual enforcement, which is slow and jurisdictionally complex, nor on on-chain automation alone, which cannot capture the full range of performance obligations or provide the legal certainty required by institutional counterparties. The framework therefore adopts a three-layer structure that combines on-chain enforcement, traditional legal wrapper, and reputational accountability.

The first layer is the registered market maker smart contract, a dedicated on-chain contract into which the market maker deposits a performance bond denominated in SYTN, sized at a level equivalent to three to six months of the guaranteed minimum volume commitment. This deposit is actively collateral monitored by the contract, which tracks performance KPIs in real time and holds authority to execute automated slashing in the event of defined violation thresholds. The performance bond is held in a vault that is fully independent from the protocol's user asset custody infrastructure, ensuring that no market maker performance event can affect user funds. The slashing mechanism operates within the protocol's existing multisig governance framework, with the Protocol Timelock's 48-hour delay applicable to slashing decisions above defined thresholds, providing an opportunity for dispute resolution before irreversible penalties are executed.

The second layer is a traditional legal wrapper, a commercial agreement executed between the protocol's legal entity and the market maker's legal entity under a specified governing law, establishing the same KPIs monitored on-chain as legally enforceable obligations, documenting the renewal fee structure and its conditions, incorporating non-compete provisions with respect to the specific asset class covered, and specifying a binding arbitration mechanism for disputes with a defined timeline for resolution. This layer is essential for engaging institutional market makers who carry fiduciary obligations that preclude operating in environments without legal certainty, and it provides a complementary enforcement mechanism for situations where on-chain automation is insufficient or disputed.

The third layer is an on-chain performance registry, an immutable, publicly readable record of each registered market maker's performance history, including spread averages, uptime statistics, volume delivered against commitment, and any slashing events. This registry serves both as the objective basis for renewal fee calculation and as a reputational signal to the broader market. A market maker with a strong on-chain performance record accumulates reputational capital that has value beyond SYTN; one with a poor record carries a public signal that affects its ability to engage with other protocols on comparable terms.

B.4 Preferential renewal fee structure

The preferential renewal fee structure is the central retention mechanism of the framework. It operates on the principle that the economic value of a market maker relationship grows over time, through accumulated familiarity with the order book, established relationships with issuers, and demonstrated reliability under diverse market conditions, and that this growing value should be reflected in the economic terms offered at renewal.

At renewal, the market maker receives a base rebate improvement calculated as a function of two variables. The first is tenure: each completed year of continuous engagement with the protocol adds a defined increment to the maker rebate, calibrated to produce a meaningful economic advantage relative to the base rate applicable to new entrants at equivalent volume levels. The second is the performance score accumulated through the on-chain performance registry during the preceding period: market makers that have consistently exceeded their minimum obligations receive a further enhancement to their renewal terms, while those that have met but not exceeded their obligations receive the tenure increment only. Market makers that have incurred slashing events during the preceding period are subject to a review process before renewal terms are confirmed, with the specific renewal conditions determined by the nature and frequency of the violations.

B.5 Performance enforcement and slashing mechanics

The slashing framework is structured in three tiers, calibrated to the severity and pattern of the violation. The tiered structure is deliberate: it avoids the binary outcome of either no consequence or full slashing, which would create perverse incentives at both extremes, and replaces it with a proportional response architecture that is predictable, auditable, and resistant to manipulation.

Minor violations, defined as spreads exceeding the target by 20-50% for periods of less than four hours, or daily volume falling below 80% of the contractual minimum, trigger an automated on-chain warning registered in the performance registry and a temporary reduction of the rebate tier for the violation period. No slashing of the performance bond occurs at this level.

Moderate violations, defined as recurring underperformance patterns across three or more days within a calendar month, or sustained spread breaches above the target for extended periods, trigger a slashing of 10-15% of the performance bond and a temporary suspension of registered market maker status, with the associated loss of preferential rebates until performance is restored to target levels.

Severe violations, including abandonment of liquidity provision during documented stress events, behaviour identified as wash trading or market manipulation by the surveillance systems described in Section 5, or material breach of the legal wrapper, trigger full slashing of the performance bond and activation of the legal enforcement mechanism.

A critical asymmetry is built into the notice provisions of the agreement framework: the market maker that rescinds must warn with 90 days of notice, however up to the deadline it remains contractually and

on-chain obligated to maintain its minimum liquidity levels throughout that notice period under pain of progressive slashing.

B.6 Liquidity incentive ratchet

The minimum performance thresholds established in market maker agreements define the floor of acceptable performance, not the target the protocol seeks to incentivise. The liquidity incentive ratchet is an on-chain mechanism that applies upward pressure on performance above the minimum by increasing the maker rebate automatically each quarter in which the market maker's delivered volume exceeds its contractual minimum by a defined margin. A market maker with a $10 million monthly volume commitment that delivers $15 million over a quarter receives a 5% increment on its rebate tier for the subsequent quarter, compounding with each consecutive quarter of over-performance up to a defined ceiling. The ratchet resets if a quarter of underperformance is recorded, ensuring that the enhanced rebate reflects current performance rather than historical achievement.

B.7 Liquidity reserve fund

The liquidity reserve fund addresses the systemic risk that individual market maker enforcement mechanisms cannot resolve: the possibility that two or more market makers coordinate, explicitly or implicitly, to withdraw liquidity simultaneously during periods of stress, thereby acquiring leverage over the protocol's commercial and governance processes. This risk is not addressed by the slashing framework, because slashing is designed to respond to individual violations rather than coordinated behaviour, and because the damage from coordinated liquidity withdrawal during a stress event may be done before any enforcement action can be completed.
The reserve fund is capitalised from a defined allocation of the ecosystem incentive pool and managed by a dedicated sub-committee of the protocol's governance structure.

The existence of a credible reserve fund materially alters the negotiating position of market makers considering coordinated withdrawal: the protocol is no longer a counterparty that has no alternative to capitulation, and this knowledge alone is expected to reduce the probability of coordination attempts. The reserve fund's deployment triggers, sizing methodology, and replenishment process are governed by a separate operational procedure reviewed annually by the management tier of the governance structure.

B.8 Token vesting acceleration for market maker performance

A portion of the total compensation package for registered market makers is allocated in SYTN tokens subject to a standard 24-month vesting schedule. To further align the long-term interests of market makers with the health and growth of the protocol, the framework introduces a performance vesting acceleration mechanism: each quarter in which the market maker exceeds its performance targets by a defined margin reduces the remaining vesting period by one month. A market maker that consistently outperforms for 12 consecutive quarters, representing three years of above-target performance, could see its vesting obligation eliminated entirely. This mechanism creates a long-term alignment of interests that complements the short-term incentives of the rebate structure: a market maker with substantial SYTN in its vesting schedule has a direct financial interest in the appreciation of the token.

This document constitutes version 1.1 of the SYTN Risk Management Framework, published May 2026 by SYTN Foundation. All previous drafts and informal summaries are superseded by this version.

For institutional inquiries, partnership discussions, and access to supplementary technical papers:
founder@sytnfinance.com| chief.architect@sytnfinance.com

Document integrity verified on-chain. Notarify certificate available upon request.

NOTARIFY
DIGITAL CERTAINTY

Certificate of authenticity

This is to certify that the document referred hereunder was notarized by our company at the date and time printed down below.

File hash

8803a3158217b97c45520b3ae4ca1136c7169f6877eba28055466830553b0aa8

CERTIFIED BY **NOTARIFY**

File Id	d44296de652045d2b66f58a7580eee0c.pdf
Combined Hash	pending
URL Notarify	https://app.notarify.io/d/e5d714

Notarify Timestamp

Friday, May 29,
2026 18:41 UTC+2

Certified by

Notarify

NOTARIFY
DIGITAL CERTAINTY

Signatures

Signer	Timestamp	Typology	Signature hash	Document hash
SYTN protocol	Friday, May 29, 2026 18:41 UTC+2	Graphic	-	8803a3158217b97c45520b3ae4ca1136c7169f6877eba28055466830553b0aa8

Date and time

Friday, May 29,
2026 18:41 UTC+2

Certified by

Notarify

NOTARIFY
DIGITAL CERTAINTY

File logs

Full name	E-mail	Timestamp	Event
SYTN protocol	founder@sytnfinance.com	Friday, May 29, 2026 18:41 UTC+2	View

Date and time

Friday, May 29,
2026 18:41 UTC+2

Certified by

Notarify