Sundial Milestone 2.7

Milestone 2.7

Risk Assessment & Security Planning:

Published risk assessment and security documentation on GitHub, Sundial's site, and/or Notion, with institutional infrastructure features to be researched to including: 1) comprehensive compliance tools, 2) sophisticated reporting systems, 3) advanced security measures, 4) research into whether to support multi-signature wallet integration, 5) detailed audit trails for all transactions, and 6) means to met stringent requirements of institutional risk management frameworks.

Table of Contents

1. Comprehensive Compliance Tools

Below is a summary of different compliance tools that Sundial may utilise to comply with regulations, security requirements, and public reporting initiatives. Each section is split into a list of different compliance providers, a summary of what they achieve, and a recommendation for Sundial.

As Sundial itself never custodies KYC'd funds or operates an order book, the Travel Rule and market-abuse surveillance fall to the front-end exchanges and liquidity providers that integrate with Sundial, and are therefore not needed in this analysis. Also, Sundial's bridge offers two modes: a public optimistic rollup path that shows every transfer on-chain, and an escape hatch path where a zero-knowledge proof validates the transfer without revealing its details. Because users can choose complete transparency or privacy-preserving proofs within the protocol, no extra privacy providers or considerations are required.

Blockchain Analytics, AML and KYT:

Because Sundial ferries value between Bitcoin and Cardano, it may be required to prove that the assets flowing through its bridge are not proceeds of crime or subject to sanctions. Real-time analytics, sanctions screening and automated suspicious activity reporting give the protocol a defensible audit trail, satisfy MiCA, FinCEN and FATF transaction monitoring rules, and reassure downstream exchanges that Sundial's liquidity is "clean" before interacting with it.

The following section of providers orchestrates real-time wallet and transaction scoring, cross-chain link analysis, and sanctions screening, ensuring the above requirements are met.

TRM Labs

TRM Labs is a SaaS platform for transaction monitoring, forensics and counterparty due diligence; easier for developers to embed and typically lower cost than other premium competitors. It is also widely used across Polygon, Unichain, Optimism, Arbitrum, Base and several zk-chains. Many L2's run two stacks in tandem: e.g., Arbitrum pairs TRM's cross-chain risk analytics with Chainalysis' sanctions oracle, whereas Base keeps Chainalysis as its primary compliance engine and supplements with TRM for deeper investigations.

Elliptic

Elliptic is a blockchain analytics company that supplies risk management, compliance, and investigation software for crypto assets. It is a trusted analytics provider used by many different industries and companies, such as Coinbase, Revolut, Stellar, and Cosmos SDK. From wallet and

transaction screening to investigator analytics, Elliptic offers a full suite of possibilities for AML analytics.

Chainalysis

Chainalysis' KYT and Reactor products monitor 200 + blockchains and L2s, providing live risk scores, sanctions alerts and case-management tooling. Because Optimism, Arbitrum, Base, Polygon zk and Babylon already feed data into Chainalysis, integrating it with Sundial would align the roll-up with expectations and give auditors the output format they already know. Chainalysis's wide variety of products would also make future adjustments or extra requirements easy to implement.

Merkle Science

Merkle Science is a predictive blockchain analytics company that supplies risk management, compliance, and forensic software for cryptoassets. It is utilised by Susquehanna, BitMEX, Hedera, and the Sui Foundation. Its features include behaviour-based transaction monitoring and sanctions screening in its Compass KYT engine, deep-dive forensic investigations with Tracker, and automated due diligence reports via KYBB.

Crystal

Crystal is a blockchain intelligence company that delivers risk management, compliance, and investigation software for digital assets. It is a trusted analytics provider utilised by institutions such as the European Central Bank, Interpol, and Europol. From real-time entity and transaction risk monitoring through its Crystal Expert platform to visual flow-of-funds investigations, Crystal offers a full suite of possibilities for AML analytics.

Lukka (Previously Coinfirm)

As a Europe-focused AML platform with native eUTxO analytics, Lukka is a sensible match for Sundial's Cardano foundation. It provides MiCA rule sets out of the box and powers AML oracles on Rootstock and Polygon zk chains. Since it has a useful set of Cardano analytics and EU regulation presets, it is a great option. Its only weaknesses are limited adoption outside Europe and a lighter brand footprint with global regulators.

Recommendation

A three-vendor stack is the best way for Sundial to cover every compliance angle without leaving blind spots. To begin, TRM Labs should supply the developer-friendly core: its lightweight APIs and predictive cross-chain analytics already protect Polygon, Optimism, Arbitrum and multiple zk-roll-ups, so it should fit into Sundial's bridge design. Adding Elliptic then adds the auditor-recognised layer, with wallet and transaction screening, sanctions detection and deep investigative graphs that external institutional reviewers already trust thanks to deployments at

Coinbase, Revolut, Stellar and Cosmos SDK. To complete the picture, Lukka would bring native eUTxO analytics and out-of-the-box MiCA/CARF rule-sets that neither TRM nor Elliptic yet provide, giving Sundial first-class Cardano coverage while simultaneously satisfying regulators.

Smart Contract Audit & Runtime monitoring

Bridges and roll-ups aggregate large balances, making them prime targets for exploits; therefore, rigorous pre-launch audits and formal verification of smart contracts are needed to surface design flaws before funds arrive. Runtime monitoring is essential to watch the codebase after mainnet, triggering alerts or automatic pauses when anomalies, such as sudden privilege changes or unplanned contract upgrades, appear. By pairing deep, up-front code reviews with continuous, on-chain surveillance, Sundial can bridge the gap between “secure at deployment” and “secure in everyday operation.”

Trail of Bits

Trail of Bits are a code and design auditor. With published research and previous audits including Optimism, Scroll zkEVM and StarkNet, they are a highly regarded firm and specialists in Bitcoin-script and bridge security work. However, they do have premium pricing and multiple-month lead times.

Coinspect

Specialising in zk-bridges, non-EVM Execution environments, and Bitcoin Script Audits, Coinspect was the lead auditor for Babylon and has worked on Zendoo, Arbitrum, and others.

Tweag

Tweag’s High-Assurance Software Group is widely regarded as the premier Cardano Native auditor. Specialising in eUTXO, the firm has produced multiple audit reports for dApps such as Minswap DEX and Genius Yield. Tweag’s combination of domain-specific expertise and a track record across multiple high-TVL Cardano projects makes it a good choice when looking for reliable Cardano auditing.

Check Point

Check Point Software Technologies is a global cybersecurity pioneer whose Web3 Security unit delivers a real-time, blockchain firewall and threat prevention platform. The system scans every pending transaction in the mempool, blocks malicious payloads before finality and applies automated kill-switches across wallets, smart contracts and validator nodes. Currently, Check Point is being integrated into Cardano L1 and has agreed to partner with Sundial.

OZ Defender (OpenZeppelin Defender)

OpenZeppelin Defender is a runtime operations platform that lets teams schedule admin actions, protect multisig keys and trigger automated pauses while emitting “Sentinel” alerts for any anomalous contract activity. It also natively supports Optimism, Arbitrum and Base, and its

move toward open-source reduces vendor lock-in. Overall, OZ Defender enforces the security controls established during the audit phase.

Certik
CertiK Skynet delivers a blend of point-in-time audits and continuous, on-chain dashboards that estimate exploit probability and rate governance risk in real time. Because it already tracks Arbitrum bridges and several Cardano projects, Skynet could give Sundial a public-facing security scorecard that investors and regulators can check at any moment, although the insight it provides ultimately depends on the depth of the underlying code review.

Recommendation

For a protocol like Sundial, the most balanced security mix would include a double audit, formal verification of smart contracts and a system for layered monitoring. Trail of Bits should lead the architecture and code review because of its work on Optimism, Scroll, and StarkNet, as well as its experience with Bitcoin script. Running in parallel, Tweag should also contribute due to its Cardano skill, Minswap and Genius Yield audits and extensive knowledge of the eUTXO model.

While we wait for the product to be released, Input Output Global (IOG) is intended to be used for formal verification of smart contracts. OPshin and TX3 could also help create this verification.

At the protocol layer, the confirmed partnership with Check Point will give Sundial a further shield. The firewall would inspect each pending transaction in the mempool, block malicious payloads before confirmation, and possibly trigger chain-wide kill switches. The preventive nature of Check Point's services would close the gap that detective tools cannot reach and require almost no maintenance from Sundial once its systems are implemented into our foundation.

On Chain Identity

On-chain identity systems embed verifiable credentials, such as proofs of KYC, residency, age, accreditation, and reputation, directly in a user’s wallet rather than on a central server. Because regulators increasingly expect DeFi protocols to bar sanctioned or underage users without reverting to custodial “walled gardens,” a self-sovereign identity layer lets participants disclose only the attribute a service needs while keeping the rest of their data private. By integrating such credentials, Sundial could enable selective access and meet compliance requirements for products built on our protocol, while keeping them optional to preserve the decentralisation and user privacy that on-chain finance promises.

Hyperledger Identus

Hyperledger Identus is a self-sovereign identity framework built on the PRISM DID method. It retains deep integration with Cardano's eUTXO model and has been deployed at a national scale (e.g., Ethiopia's student ID rollout with five million DID-backed credentials). Identus is already integrated by Cardano dApps such as Empowa and Book.io. Its GDPR-oriented design, mobile SDK, and Cardano-native approach are strong advantages, but its scope remains Cardano-centric: developers must run bridging or interoperability layers to use those credentials across other chains.

ION

ION is an open-source Sidetree network that records DID operations directly to the Bitcoin mainnet. Microsoft uses it for pilot projects such as GitHub log-ins and NHS medical-record trials, and its Bitcoin anchoring gives it unmatched immutability and brand credibility. Yet ION is a low-level registry rather than a turnkey KYC solution: systems must host, or rely on partners to host, the resolution nodes and build their own compliance workflows around the raw DIDs.

Recommendation

For Sundial, the pragmatic route is to support credentials issued under the PRISM DID standard via Hyperledger Identus for Cardano-side users, ensuring compatibility with existing wallets and dApps. At the same time, Sundial can facilitate ION-anchored DIDs as an optional proof of provenance for Bitcoin-side users who require a Bitcoin-rooted audit trail. Together, Identus and ION deliver day-one functionality with broad ecosystem reach, while giving Sundial a neutral, Bitcoin-anchored layer of trust that avoids locking the protocol into a single compliance silo.

---

2. Reporting Systems

Reporting systems ingest raw node data and mem-pool events, normalising them into user-friendly data forms and APIs that investors, developers, and regulators rely on for network-health metrics, protocol revenue, address activity, etc. In a compliance context, they produce the quarterly or ad hoc statements that banks, auditors, and institutional LPs demand before deploying capital.

For reporting systems, the only requirement is that each data explorer's needs be accounted for. The three main requirements are providing information for institutions and the public while ensuring protocol-specific details are available.

Coin Metrics

Coin Metrics is a benchmark for on-chain macro data. Founded in 2017 by MIT researchers, it ingests full-node data for more than 250 assets and reconciles it into clean, chain-agnostic, time series formats, including everything from daily active addresses to realised capitalisation and detailed miner revenues. In 2021, the team extended that framework to ADA, publishing a wide breadth of metrics. Partnering with Coin Metrics would allow Sundial to present decade-long Bitcoin histories and multi-year Cardano histories in a single, regulator-ready format. Its clients include Fidelity Digital Assets, Bitwise and Galaxy Digital, meaning that institutional investors will recognise the brand and be comfortable ingesting its CSVs or cloud API for their own risk dashboards.

Mempool.space

mempool.space is a real-time Bitcoin explorer and mempool-visualisation stack. It pulls raw block, transaction-queue and Lightning-channel data straight from a self-hosted full node and turns it into live, easy-to-read data visualisations and containers. The stack is now embedded in node distributions, and its dashboards underpin fee-selection engines at mining pools and lightning service providers worldwide. Mempool.space has also shown interest in becoming a reporting systems provider for Sundial.

Blockchain.com

Blockchain.com Charts is a macro data portal for Bitcoin and other blockchains. It's Charts & Statistics and Data APIs stream clean, minute-by-minute time-series formats for lots of data, while raw-block and address endpoints let analysts recreate full-node views without running their own infrastructure. BIS working papers and central-bank studies routinely cite blockchain.com/charts when graphing confirmation times, supply shocks or mining-hardware events, so auditors recognise the brand and accept its CSV or JSON outputs for risk dashboards and stress-tests.

Cexplorer

Cexplorer is a dedicated data portal for the Cardano blockchain. Its REST and GraphQL APIs decode second-by-second eUTxO data, while raw transaction and address endpoints let analysts rebuild full-node views without operating their own infrastructure. When integrated into Sundial’s own roll-up explorer or administrative console, Cexplorer will enable operators to view the specific outputs of any flagged transaction, a capability that generic multi-chain dashboards cannot provide. Maintained by veteran members of the Cardano community and engineered for high-volume throughput, Cexplorer offers Sundial an authoritative interface for detailed on-chain inquiries.

Recommendation

A three-vendor stack will give Sundial complete, regulator-friendly coverage without repetition. Coin Metrics can provide the institutional-grade macro layer: its long Bitcoin history and several years of Cardano time series data will satisfy auditors, analysts and liquidity partners who want clean CSVs or APIs. Mempool.space will then supply the granular real-time Bitcoin view, hoping that Sundial will receive its own dashboard for the public. Finally, to ensure Cardano data is properly presented, Cexplorer will bring native eUTxO decoding and detailed widgets. With this plan, Sundial will have the capabilities to display all forms of blockchain data, along with Bitcoin's and Cadano's data stream to anyone who may need them.

---

3. Advanced Security Measures

This section outlines the planned technical security measures that Sundial intends to implement in order to safeguard protocol operations and maintain a robust security posture.

Blockchain Security Methods

Blockchain systems on a UTXO model have specific risks that need to be addressed accordingly, along with more universal Web3 risks.

Protocol-Specific Risks

- Double Satisfaction Exploits
- Datum Overflow
- Token Dust Flooding
- Multi-Sig Bypass
- Malicious Contract Metadata
- Suspicious Cross-Chain Transaction Patterns

Universal Web3 Risks

- Phishing & Airdrop Scams
- Smart Contract Exploits
- Denial of Service (DoS)
- Oracle Manipulation

Threat Detection:

Due to Sundial's agreement with Check Point, all of the above issues can and will be addressed utilising their systems. Below are a list of features Check Point will implement with Sundial to ensure the highest level of security:

- Real-Time Blockchain Monitoring
    - Parse every Sundial block as it is produced.
    - Inspect all transactions, UTxOs, and datums for anomalies.
    - Maintain a historical threat intelligence repository.

- AI & Signature-Based Attack Vector Classifiers
    - Dedicated models for detecting Double Satisfaction, Datum Overflow, Token Dust, Multi-Sig Bypass, Malicious Metadata, and Suspicious Cross-Chain Patterns.

- Direct Infrastructure Integration
    - Connect to Sundial full nodes for low-latency analysis.
    - Provide API endpoints for operational dashboards and live SOC alerts.

Automated Analysis & Forensics:

- Static & Dynamic Smart Contract Analysis
    - Pre-deployment code scanning against known exploit patterns.
    - On-chain behaviour simulation for live contract risk scoring.
- Dynamic Transaction Simulation
    - Replay suspicious transactions in a sandbox to verify malicious impact.
- Malicious Token Fingerprinting
    - Track and block scam tokens using metadata and historical activity patterns.

These features will allow many different benefits: Quick detection of attacks or security risks, exploit prevention, transparent reporting and compliance alignment, the capability to withstand

sophisticated attacks without halting network operations and overall, provide a secure foundation to encourage ecosystem growth.

Audits

Audits are also essential to ensure that no smart contract or code written by Sundial contains exploits or problems. As mentioned above, Sundial will have double audits. Trail of Bits will lead the architecture and code review because of its experience with Bitcoin script. Running in parallel, Tweag will contribute by analysing Cardano-specific scripts.

Overview

By implementing robust blockchain security methods, continuous monitoring, and independent audits, Sundial aims to build a security framework capable of detecting, preventing, and responding to sophisticated threats. While these systems are still in the planning stage, their phased rollout will ensure that security capabilities evolve in step with protocol adoption and institutional requirements.

---

4. Multi-signature wallet integration

Multi-signature wallet support would let Sundial work with wallets that need more than one key to move funds, the standard approach for large institutions, DAO treasuries, trading desks, etc. Giving these users a frictionless path onto Sundial means more liquidity, higher transaction volume and faster growth for the L2. Regulators also like multi-control of wallets because it decreases the chance of hacks or lost keys, so having the feature in place now keeps Sundial ahead of future compliance checks.

Since Sundial is using Plutus script (which is multi-sig compatible), and Midgard already supports multi-sig wallets, this functionality is an easy, beneficial and natural extension for Sundial to implement.

---

5. Detailed audit trails for all transactions

This section aims to showcase how Sundial will provide a complete, tamper-evident, and regulator-ready record of every Sundial transaction and admin action, from a user's L1 deposit through L2 batching and L1 settlement, so auditors can independently replay, reconcile, and verify outcomes without privileged access.

What the audit trail should capture

Transaction events (user & protocol)

- L1 deposit/withdrawal txids (BTC & ADA), block heights and confirmations, as well as all tx orders
- L2 events: batch ID, rollup block, state root, fraud proof, the proof ID and verifier contract reference.

Operational & governance events

- Admin actions (pauses, parameter changes, upgrades), multisig approvals (signer set, policy ID, tx hash), firewall blocks, Check Point actions.
- Build provenance for deployed artefacts (commit, build attestation, who approved, when).

System observability

- Indexer, sequencer, prover health and version; failed/ retried jobs; latency/queue metrics snapshots for disputed intervals.

Providers & building blocks

Ledger Capture & Reconciliation (already in recommendations)

On the Bitcoin side, mempool.space will be used to capture raw mempool and block data, producing transaction and fee information for all BTC legs, and Sundial-specific information. For Cardano, Cexplorer's high-throughput REST and GraphQL APIs will decode eUTxO data, enabling auditors to traverse every input and output linked to Sundial events with precision. Finally, Coin Metrics can provide the institutional-grade macro layer.

Runtime Controls (already in recommendations)

Check Point will generate detailed decision logs for any transaction blocked or flagged at the mempool stage. These logs will include the reason for the block, detected signatures, and relevant rule identifiers, enabling deep forensic correlation between network events and security interventions.

Admin Action Logging (Native to Cardano & Bitcoin)

All privileged administrative actions will be committed directly to the Cardano blockchain as metadata conforming to the CIP-68 standard, ensuring structured, machine-readable audit entries. To enhance the immutability of this data, a cryptographic hash of each record will also

be periodically anchored to Bitcoin via an OP_RETURN output. This dual-chain anchoring provides a tamper-evident proof of both existence and timestamp. A dedicated Sundial governance indexer will continuously monitor Cardano and Bitcoin for these records, storing them in an immutable, queryable database such as AWS QLDB for regulator and auditor access. Selected entries will also be published to a public governance activity feed, reinforcing institutional trust through transparent reporting.

Why This Meets Regulator & Institutional Requirements

The combined use of Cardano metadata and Bitcoin OP_RETURN anchoring creates a dual-layer immutability framework, making the admin audit trail inherently tamper-evident. All events and transactions are also verifiable using publicly accessible block explorers (Cexexplorer and mempool.space) and Sundial's Data availability layer, allowing independent auditors to confirm transactions. Finally, the integration of Check Point security logs means that runtime metrics are always recorded, allowing for comprehensive forensic analysis into any attacks on the Sundial Protocol.

The detail captured in this plan ensures granular visibility into every transaction as well as administrative and operational change.

---

6. Means to meet stringent requirements of institutional risk management frameworks.

A Risk Management Framework (RMF) is a structured, standardised approach that organisations use to identify, assess, prioritise, mitigate, and monitor risks. Sundial’s RMF will be built on four internationally recognised institutional standards:

- ISO 27001: Security Governance: Establishes robust information security policies, controls, and audits to protect systems, data, and infrastructure.
- ISO 31000: Risk Management: Provides a systematic process for identifying, assessing, and managing risks across all operations.
- NIST Cybersecurity Framework (CSF): Operational Resilience: Embeds detection, response, and recovery capabilities to maintain service continuity during adverse events.
- COSO ERM: Governance and Internal Controls: Defines governance structures, accountability mechanisms, and internal controls to align operations with strategic

objectives.

To meet institutional risk management standards, Sundial's implementation plan integrates the following: broad operational security policies that will govern all infrastructure and workforce security, and blockchain-specific policies addressing the unique operational risks of Bitcoin, Cardano, and L2 roll-up environments. Our RMF will also apply stringent, framework-aligned requirements tailored to Sundial's five main operational areas:

1. Governance: Oversight and decision-making structures.
2. Institutional Yield Service: Infrastructure for vetted BTC-native yield providers.
3. Liquidity and Bridging: Secure cross-chain asset transfer and liquidity provision.
4. BTC Market Making: Partner-led BTC liquidity stabilisation via audited contracts.
5. SDK/API Licensing: Secure integration points for institutional clients.

The following sections provide an in-depth review of the planned policies and our five main operational areas, including their requirements, perceived risks, industry comparisons, and recommendations, in order to fully meet Sundial's risk management objectives.

Operational Security Policies

Operational security is defined as the ability of an organisation to continue delivering critical products and services despite disruptions by anticipating, preventing, responding to, and recovering from adverse events. Sundial will create full documentation that addresses these four categories.

Anticipation

- Vulnerability Management Policy: Detail how Sundial will safeguard its organisation by identifying, qualifying and mitigating vulnerabilities.
- Global Workforce Policy: Manage the operational, workforce, and cybersecurity risks posed to our organisation and workforce by working in different countries around the globe.

Prevention

- Password Attributes Standard: Provide the required password attributes for all Sundial Accounts

- Fraud Risk Management Policy: Assign roles and responsibilities, while establishing internal controls to help detect, prevent, and deter fraud or possible fraud.
- Audit & Logging Policy: Ensure that all transactions, system and application events with the potential to affect security are logged with the appropriate level of detail.
- Systems Security Policy: Outline requirements for developing, installing, maintaining, and operating IT systems securely to prevent unauthorised system use and ensure data and system security.
- Access Control Policy: Minimise the risk of unauthorised access to physical and logical systems.
- Physical Security Policy: Ensure Sundial safeguard its hardware, software, and data from exposure to persons (internal or external) who could intentionally or inadvertently harm our workforce, business or systems.
- Change Control Policy: guidance on how changes to the Sundial IT environment are requested, tested, documented and approved before operational use.

Response

- Nonconformity and Corrective Action Protocol: Document Sundial's process for managing actual and potential nonconformities, taking corrective actions to prevent recurrence, and continually improving our operations.
- Incident Response Plans: How to best respond to different IT and office security threats.

Recovering

- Business Continuity and Disaster Recovery Plan: Provide a comprehensive guide on Sundial's Business Continuity and Disaster Recovery Plan (BCP/DR) and procedures

Blockchain Security Policies

While there is currently no universally recognised risk management framework specifically for blockchain, Sundial recognises the importance of identifying and mitigating risks specifically arising from blockchain-based business operations. The following section addresses the policies and plans that will be created to address any blockchain-specific risks.

Anticipation

- Threat Intelligence & Blockchain Monitoring Policy: Define how Sundial monitors Bitcoin, Cardano, and L2 network activity for unusual patterns.

- Third-Party & Vendor Risk Management Policy: Address security requirements for exchanges, custody providers, staking partners, and oracle services.
- Cross-Chain Dependency Risk Policy: Identify operational and security risks from reliance on external L1 chains (Bitcoin and Cardano).

Prevention

- Cryptography Policy: Provide guidance that limits encryption algorithms to those that have received substantial public review and have been proven effective.
- Smart Contract Security & Upgrade Policy: Define secure coding practices, mandatory external audits (as mentioned above), on-chain upgrade procedures, and testnet/staging deployment steps. Also, require a rollback path for high-severity bugs.
- Key Management & Multi-signature Policy: Specify the secure generation, distribution, and storage of private keys for bridge multisigs, sequencer control, and admin actions. Include quorum rules, key rotation schedules, and emergency revocation procedures.
- Operational Resilience Testing Policy: Schedule and Document periodic stress testing for the Sundial Protocol

Response

- Blockchain Fork/Chain Split Response Plan: Document Sundial's operational and communications plan in case of a Bitcoin or Cardano fork. Include transaction replay prevention, user fund safety, and chain selection criteria.
- Bridge Incident Containment Policy: Define how to handle incidents, from bridging failures to smart contract exploits. Include isolation of affected assets, temporary suspension rules, and user notification timelines.

Recovering

- Cross-Chain Recovery Plan: Include recovery procedures for a prolonged Cardano or Bitcoin outage, ensuring user withdrawals are still possible.
- Protocol Restart & State Recovery Policy: Document how Sundial will safely restart after downtime while ensuring ledger integrity and avoiding double-spends.
- Post-mortem and Lessons-Learned Protocol: Formalise how to document security incidents, identify root causes, and integrate improvements into policy updates.

Operational Risk Management

Sundial will adopt a business services approach to operational risk management, in alignment with the guidance and requirements of a number of financial regulations. The following section will outline Sundial's five key services, their risk management requirements, perceived risks, and recommended actions, aligning with the globally recognised frameworks mentioned above.

1. Governance

What it means and facilitates

The governance structure defines how Sundial makes decisions, including upgrades, risk management, and operational changes. Initially, Sundial will adopt a fully centralised governance model, with all authority held by the Sundial team. This ensures fast decision-making, clear accountability, and alignment with Sundial's strategic vision. Governance will evolve over time as the protocol matures.

Risk management requirements

Governance Transparency

- Maintain a governance charter clearly defining decision-making roles, responsibilities, and authority levels.
- Publish regular governance reports covering decision-making processes, board composition, and regulatory compliance status.

Auditability

- Ensure all governance decisions have a traceable audit trail documenting the process, rationale, and outcome.
- Maintain detailed records on data integrity measures, access controls, and monitoring procedures.

Operational Resilience Measures

- Establish predefined protocols for responding to critical failures or unexpected events.
- Adopt a formal conflict-of-interest policy to safeguard impartial decision-making.
- Appoint an external advisory board to provide independent oversight and strategic guidance.

- Require multi-signature control for critical keys, with internal checks to maintain continuous oversight.
- Conduct regular governance reviews, including periodic external assessments, to validate effectiveness.

Perceived Risks

Centralisation creates a single point of failure and increases the impact of team departures. There is also a risk of resistance to change, and the potential for security breaches via internal collusion or malicious actors.

Industry examples

- Arbitrum: Transitioned from centralised to DAO governance; $ARB holders vote; elected Security Council for emergencies.
- Optimism: Bicameral governance with a Token House (token holders) and Citizens' House (reputation-based).
- Polygon: Multi-layer governance via Polygon Improvement Proposals (PIPs) reviewed by a Protocol Council with timelocks.

Recommendations

- Establish a Governance Council with defined roles and authority.
- Create a structured proposal process with review, approval, multisig requirements and optional timelocks, ensuring all proposals are stored and accessible.
- Hold quarterly governance reviews with external oversight.
- Create a structured plan for a transition to a decentralised governance system

2. Institutional Yield Service

What it means and facilitates

This service provides white-labeled infrastructure for custody providers, asset managers, and lenders to build BTC-native yield products on Sundial. Only vetted, secure providers will be integrated, enabling institutional access to compliant BTC yield offerings.

Risk management requirements

- A due diligence framework must assess provider creditworthiness, security, liquidity resilience, and regulatory compliance.
- Access controls should restrict integration to approved providers.
- Provider operations should be transparent.

Perceived risks

Regulatory and public exposure from unreliable providers, third-party misconduct, reputational damage, and contract vulnerabilities.

Industry examples

- Yearn Finance: Emergency “War Room” procedures in case of critical issues, post-mortems on issues, multiple yield strategies, audits, and risk scoring.

Recommendations

- Require standardised disclosures, audits, and risk classifications from providers.
- Establish licensing, compliance, and KYC checks in the vetting process.
- Publish relevant provider documentation.
- Maintain emergency intervention capabilities.

3. Liquidity and Bridging

What it means and facilitates

Sundial will operate bridging infrastructure and act as a liquidity provider, enabling near-instant access to cross-chain assets that typically require extended settlement periods. This improves capital efficiency for users and institutions.

Risk management requirements

- Bridge contracts should undergo formal verification and regular audits.
- Provide Liquidity reserves, fallback mechanisms, and monitoring systems.

- Procure insurance or store emergency funds that can cover transfer failures.

Perceived risks

Smart contract vulnerabilities and liquidity shortfalls.

Industry examples

- Hop Protocol: Audited contracts, fraud proofs, and early withdrawal from optimistic rollups.
- Stargate: Native asset transfers via shared liquidity pools with security layers and pause capabilities.

Recommendations

- Audit and verify all bridge contracts.
- Establish liquidity provider capital requirements.
- Maintain an emergency fund or insurance mechanism.
- Publish bridge-related risk disclosures.

4. BTC Market Making Service

What it means and facilitates

Sundial will partner with DEXs and liquidity providers to support BTC market-making through secure smart contract infrastructure.

Risk management requirements

- All market-making contracts must be externally audited.
- Performance monitoring and emergency response frameworks should be in place.
- DEX integration standards and partner due diligence are required before any integration.

Perceived risks

Malicious liquidity partners, vulnerabilities in contracts, and instability introduced through upgrades.

Industry examples

- Uniswap: Immutable, audited contracts; permissionless pool creation; oracle manipulation resistance.
- dYdX: Involves whitelisted market-makers with Service Level Agreements, on-chain risk metrics, and emergency procedures.

Recommendations

- Audit all market-making contracts.
- Publish all audits
- Set clear partner standards and SLAs.
- Establish operational failure and emergency response procedures.

5. SDK / API Licensing

What it means and facilitates

Sundial will create Software Development Kits (SDKs) and Application Programming Interfaces (APIs) for institutional clients to integrate Sundial's services into their own platforms.

Risk Management requirements

- APIs must use secure encryption, MFA and role-based access.
- Private functions should be accessible only to authorised parties via whitelisting and specific API keys.
- All API usage should be logged for audit purposes.

Perceived risks

Unauthorised access, SDK vulnerabilities, and data leaks.

Industry examples

- Fireblocks: Multi-language SDKs, IP whitelisting, and audit logs.

- Circle (USDC API): Enforces AML/KYC and continuous transaction monitoring.

Recommendations

- Apply robust security controls and whitelisting for API/SDK access.
- Maintain comprehensive access and change logs.
- Publish an API security and monitoring policy.

Summary Mapping: Operational Areas to Frameworks

Operational Area	Relevant Frameworks	Key Control Focus
Operational Security Policies	ISO 27001, NIST CSF	Access control, vulnerability management, IT systems security, physical security, incident response
Blockchain Security Policies	ISO 27001, NIST CSF	Smart contract security, key management, chain split response, cross-chain recovery
Governance	COSO ERM, ISO 31000	Decision transparency, auditability, multi-sig authority
Institutional Yield	ISO 31000, ISO 27001	Provider due diligence, access controls, disclosure
Liquidity & Bridging	ISO 27001, NIST CSF	Contract audits, liquidity reserves, failover systems

BTC Market Making	ISO 27001, ISO 31000	Partner vetting, SLA compliance, operational resilience
SDK/API Licensing	ISO 27001, COSO ERM	Access control, logging, compliance oversight