CleanSpark Whitepaper

Bitcoin mining strategy and CLSK participation framework

Abstract

CleanSpark is a Bitcoin mining company that pairs real-world hashrate with CLSK, a fixed-supply participation token on BNB Smart Chain. CLSK is intended to align community engagement and disclosures with mining milestones — not to represent equity or a direct claim on mining revenue unless expressly stated in formal legal documents.

Bitcoin mining model

Operations focus on efficient ASIC deployment, disciplined power procurement, uptime, and joules-per-terahash improvement over time. Target fleet figures communicated on the website are illustrative until verified in audited or management-prepared statements.

Energy & sustainability

CleanSpark evaluates power purchase structures, curtailment programs, and where applicable lower-carbon energy sources. Public communications should avoid greenwashing; actual mix and emissions reporting will depend on host geography and contracts.

CLSK token design

CLSK uses a fixed supply with transparent allocation categories (community, liquidity, ecosystem, etc.) as shown in project tokenomics. Governance may propose uses of ecosystem allocations subject to legal and technical constraints.

Risk factors

Bitcoin price volatility, halving schedule, difficulty increases, regulatory change, counterparty failure, and force majeure can all affect mining economics. Token liquidity and bridge/exchange risks apply separately to CLSK markets.

Contact & updates

Published materials will be updated as operations mature. Refer to cleansparkcoin.com and official social channels for notices. Verify all contract addresses via BscScan before interacting.

Extended topic 1 — Corporate structure

This section elaborates on entities, jurisdictions, and disclosure responsibilities for CleanSpark readers who want depth beyond the homepage. It is descriptive, not prescriptive legal or investment advice.

Management may update strategies as markets, hosts, and regulations evolve. When material changes occur, CleanSpark should communicate them through official channels and, where required, file or publish notices appropriate to each jurisdiction.

CLSK holders and mining counterparties should perform independent diligence. No projection of yield, payback period, or token appreciation is implied. Past network conditions do not predict future Bitcoin price or difficulty.

Extended topic 2 — Hashrate economics

This section elaborates on difficulty, fees, block rewards, and halving exposure for CleanSpark readers who want depth beyond the homepage. It is descriptive, not prescriptive legal or investment advice.

Management may update strategies as markets, hosts, and regulations evolve. When material changes occur, CleanSpark should communicate them through official channels and, where required, file or publish notices appropriate to each jurisdiction.

CLSK holders and mining counterparties should perform independent diligence. No projection of yield, payback period, or token appreciation is implied. Past network conditions do not predict future Bitcoin price or difficulty.

Extended topic 3 — Hosting & colocation

This section elaborates on racks, SLAs, remote hands, and spare-parts strategy for CleanSpark readers who want depth beyond the homepage. It is descriptive, not prescriptive legal or investment advice.

Management may update strategies as markets, hosts, and regulations evolve. When material changes occur, CleanSpark should communicate them through official channels and, where required, file or publish notices appropriate to each jurisdiction.

CLSK holders and mining counterparties should perform independent diligence. No projection of yield, payback period, or token appreciation is implied. Past network conditions do not predict future Bitcoin price or difficulty.

Extended topic 4 — Fleet procurement

This section elaborates on vendor selection, warranty claims, and depreciation for CleanSpark readers who want depth beyond the homepage. It is descriptive, not prescriptive legal or investment advice.

Management may update strategies as markets, hosts, and regulations evolve. When material changes occur, CleanSpark should communicate them through official channels and, where required, file or publish notices appropriate to each jurisdiction.

CLSK holders and mining counterparties should perform independent diligence. No projection of yield, payback period, or token appreciation is implied. Past network conditions do not predict future Bitcoin price or difficulty.

Extended topic 5 — Treasury policy

This section elaborates on BTC retention, stablecoin use, and hedging philosophy for CleanSpark readers who want depth beyond the homepage. It is descriptive, not prescriptive legal or investment advice.

Management may update strategies as markets, hosts, and regulations evolve. When material changes occur, CleanSpark should communicate them through official channels and, where required, file or publish notices appropriate to each jurisdiction.

CLSK holders and mining counterparties should perform independent diligence. No projection of yield, payback period, or token appreciation is implied. Past network conditions do not predict future Bitcoin price or difficulty.

Extended topic 6 — On-chain transparency

This section elaborates on what is published on-chain vs off-chain for CleanSpark readers who want depth beyond the homepage. It is descriptive, not prescriptive legal or investment advice.

Management may update strategies as markets, hosts, and regulations evolve. When material changes occur, CleanSpark should communicate them through official channels and, where required, file or publish notices appropriate to each jurisdiction.

CLSK holders and mining counterparties should perform independent diligence. No projection of yield, payback period, or token appreciation is implied. Past network conditions do not predict future Bitcoin price or difficulty.

Extended topic 7 — Governance roadmap

This section elaborates on CLSK voting scope and legal limitations for CleanSpark readers who want depth beyond the homepage. It is descriptive, not prescriptive legal or investment advice.

Management may update strategies as markets, hosts, and regulations evolve. When material changes occur, CleanSpark should communicate them through official channels and, where required, file or publish notices appropriate to each jurisdiction.

CLSK holders and mining counterparties should perform independent diligence. No projection of yield, payback period, or token appreciation is implied. Past network conditions do not predict future Bitcoin price or difficulty.

Extended topic 8 — Regulatory watchlist

This section elaborates on mining and token rules across key markets for CleanSpark readers who want depth beyond the homepage. It is descriptive, not prescriptive legal or investment advice.

Management may update strategies as markets, hosts, and regulations evolve. When material changes occur, CleanSpark should communicate them through official channels and, where required, file or publish notices appropriate to each jurisdiction.

CLSK holders and mining counterparties should perform independent diligence. No projection of yield, payback period, or token appreciation is implied. Past network conditions do not predict future Bitcoin price or difficulty.

Extended topic 9 — Security culture

This section elaborates on training, phishing resistance, and access reviews for CleanSpark readers who want depth beyond the homepage. It is descriptive, not prescriptive legal or investment advice.

Management may update strategies as markets, hosts, and regulations evolve. When material changes occur, CleanSpark should communicate them through official channels and, where required, file or publish notices appropriate to each jurisdiction.

CLSK holders and mining counterparties should perform independent diligence. No projection of yield, payback period, or token appreciation is implied. Past network conditions do not predict future Bitcoin price or difficulty.

Extended topic 10 — Community communications

This section elaborates on announcements, support, and escalation for CleanSpark readers who want depth beyond the homepage. It is descriptive, not prescriptive legal or investment advice.

Management may update strategies as markets, hosts, and regulations evolve. When material changes occur, CleanSpark should communicate them through official channels and, where required, file or publish notices appropriate to each jurisdiction.

CLSK holders and mining counterparties should perform independent diligence. No projection of yield, payback period, or token appreciation is implied. Past network conditions do not predict future Bitcoin price or difficulty.

WP 1.1 — Network economics & block space

This subsection (1.1) addresses whitepaper narrative within the CleanSpark Extended Security & Audit Assessment dated 2026. The assessment covers Bitcoin mining operations, hosting relationships, treasury workflows, and CLSK on BNB Smart Chain as described in the system boundary statement. Procedures performed were limited to inquiry, observation, inspection of selected artifacts, and agreed-upon analytics where noted. No opinion on financial statements is expressed.

Management is responsible for design, implementation, and operating effectiveness of controls. Assessors relied on representations regarding scope completeness and should be engaged to re-perform or expand testing when architecture, custodians, contracts, or token logic materially change. Residual risk may remain even when controls appear suitably designed; compensating controls must be explicitly documented.

Key considerations for network economics & block space include segregation of duties, least-privilege access, audit logging with tamper-evident retention, encryption in transit and at rest for sensitive payloads, and periodic independent validation of backups and recovery paths. For mining infrastructure, assessors evaluated logical access to management interfaces, change tickets for firmware or pool configuration, and alignment with vendor hardening baselines.

Observations are classified per the severity model in Section 23. Informational items improve maturity; medium and above require tracked remediation with target completion dates and evidence packs. CleanSpark should maintain a continuous monitoring calendar covering certificate expiry, access recertification, dependency advisories, and hashrate anomaly detection correlated with power telemetry.

Cross-dependencies: findings in custody and key management may amplify smart-contract operational risks if administrative keys overlap with deployer roles. CleanSpark should enforce role separation between mining treasury keys, token admin keys (if any), and routine payroll or vendor payment keys. Table 1 in the evidence index references representative samples reviewed for this subsection.

WP 1.2 — Network economics & block space

This subsection (1.2) addresses whitepaper narrative within the CleanSpark Extended Security & Audit Assessment dated 2026. The assessment covers Bitcoin mining operations, hosting relationships, treasury workflows, and CLSK on BNB Smart Chain as described in the system boundary statement. Procedures performed were limited to inquiry, observation, inspection of selected artifacts, and agreed-upon analytics where noted. No opinion on financial statements is expressed.

Management is responsible for design, implementation, and operating effectiveness of controls. Assessors relied on representations regarding scope completeness and should be engaged to re-perform or expand testing when architecture, custodians, contracts, or token logic materially change. Residual risk may remain even when controls appear suitably designed; compensating controls must be explicitly documented.

Key considerations for network economics & block space include segregation of duties, least-privilege access, audit logging with tamper-evident retention, encryption in transit and at rest for sensitive payloads, and periodic independent validation of backups and recovery paths. For mining infrastructure, assessors evaluated logical access to management interfaces, change tickets for firmware or pool configuration, and alignment with vendor hardening baselines.

Observations are classified per the severity model in Section 23. Informational items improve maturity; medium and above require tracked remediation with target completion dates and evidence packs. CleanSpark should maintain a continuous monitoring calendar covering certificate expiry, access recertification, dependency advisories, and hashrate anomaly detection correlated with power telemetry.

Cross-dependencies: findings in custody and key management may amplify smart-contract operational risks if administrative keys overlap with deployer roles. CleanSpark should enforce role separation between mining treasury keys, token admin keys (if any), and routine payroll or vendor payment keys. Table 2 in the evidence index references representative samples reviewed for this subsection.

WP 1.3 — Network economics & block space

This subsection (1.3) addresses whitepaper narrative within the CleanSpark Extended Security & Audit Assessment dated 2026. The assessment covers Bitcoin mining operations, hosting relationships, treasury workflows, and CLSK on BNB Smart Chain as described in the system boundary statement. Procedures performed were limited to inquiry, observation, inspection of selected artifacts, and agreed-upon analytics where noted. No opinion on financial statements is expressed.

Management is responsible for design, implementation, and operating effectiveness of controls. Assessors relied on representations regarding scope completeness and should be engaged to re-perform or expand testing when architecture, custodians, contracts, or token logic materially change. Residual risk may remain even when controls appear suitably designed; compensating controls must be explicitly documented.

Key considerations for network economics & block space include segregation of duties, least-privilege access, audit logging with tamper-evident retention, encryption in transit and at rest for sensitive payloads, and periodic independent validation of backups and recovery paths. For mining infrastructure, assessors evaluated logical access to management interfaces, change tickets for firmware or pool configuration, and alignment with vendor hardening baselines.

Observations are classified per the severity model in Section 23. Informational items improve maturity; medium and above require tracked remediation with target completion dates and evidence packs. CleanSpark should maintain a continuous monitoring calendar covering certificate expiry, access recertification, dependency advisories, and hashrate anomaly

detection correlated with power telemetry.

Cross-dependencies: findings in custody and key management may amplify smart-contract operational risks if administrative keys overlap with deployer roles. CleanSpark should enforce role separation between mining treasury keys, token admin keys (if any), and routine payroll or vendor payment keys. Table 3 in the evidence index references representative samples reviewed for this subsection.

WP 2.1 — Mining pools & payout models

This subsection (2.1) addresses whitepaper narrative within the CleanSpark Extended Security & Audit Assessment dated 2026. The assessment covers Bitcoin mining operations, hosting relationships, treasury workflows, and CLSK on BNB Smart Chain as described in the system boundary statement. Procedures performed were limited to inquiry, observation, inspection of selected artifacts, and agreed-upon analytics where noted. No opinion on financial statements is expressed.

Management is responsible for design, implementation, and operating effectiveness of controls. Assessors relied on representations regarding scope completeness and should be engaged to re-perform or expand testing when architecture, custodians, contracts, or token logic materially change. Residual risk may remain even when controls appear suitably designed; compensating controls must be explicitly documented.

Key considerations for mining pools & payout models include segregation of duties, least-privilege access, audit logging with tamper-evident retention, encryption in transit and at rest for sensitive payloads, and periodic independent validation of backups and recovery paths. For mining infrastructure, assessors evaluated logical access to management interfaces, change tickets for firmware or pool configuration, and alignment with vendor hardening baselines.

Observations are classified per the severity model in Section 23. Informational items improve maturity; medium and above require tracked remediation with target completion dates and evidence packs. CleanSpark should maintain a continuous monitoring calendar covering certificate expiry, access recertification, dependency advisories, and hashrate anomaly detection correlated with power telemetry.

Cross-dependencies: findings in custody and key management may amplify smart-contract operational risks if administrative keys overlap with deployer roles. CleanSpark should enforce role separation between mining treasury keys, token admin keys (if any), and routine payroll or vendor payment keys. Table 11 in the evidence index references representative samples reviewed for this subsection.

WP 2.2 — Mining pools & payout models

This subsection (2.2) addresses whitepaper narrative within the CleanSpark Extended Security & Audit Assessment dated 2026. The assessment covers Bitcoin mining operations, hosting relationships, treasury workflows, and CLSK on BNB Smart Chain as described in the system boundary statement. Procedures performed were limited to inquiry, observation, inspection of selected artifacts, and agreed-upon analytics where noted. No opinion on financial statements is expressed.

Management is responsible for design, implementation, and operating effectiveness of controls. Assessors relied on representations regarding scope completeness and should be engaged to re-perform or expand testing when architecture, custodians, contracts, or token logic materially change. Residual risk may remain even when controls appear suitably designed; compensating controls must be explicitly documented.

Key considerations for mining pools & payout models include segregation of duties, least-privilege access, audit logging with tamper-evident retention, encryption in transit and at rest for sensitive payloads, and periodic independent validation of backups and recovery paths. For mining infrastructure, assessors evaluated logical access to management interfaces, change tickets for firmware or pool configuration, and alignment with vendor hardening baselines.

Observations are classified per the severity model in Section 23. Informational items improve maturity; medium and above require tracked remediation with target completion dates and evidence packs. CleanSpark should maintain a continuous monitoring calendar covering

certificate expiry, access recertification, dependency advisories, and hashrate anomaly detection correlated with power telemetry.

Cross-dependencies: findings in custody and key management may amplify smart-contract operational risks if administrative keys overlap with deployer roles. CleanSpark should enforce role separation between mining treasury keys, token admin keys (if any), and routine payroll or vendor payment keys. Table 12 in the evidence index references representative samples reviewed for this subsection.

WP 2.3 — Mining pools & payout models

This subsection (2.3) addresses whitepaper narrative within the CleanSpark Extended Security & Audit Assessment dated 2026. The assessment covers Bitcoin mining operations, hosting relationships, treasury workflows, and CLSK on BNB Smart Chain as described in the system boundary statement. Procedures performed were limited to inquiry, observation, inspection of selected artifacts, and agreed-upon analytics where noted. No opinion on financial statements is expressed.

Management is responsible for design, implementation, and operating effectiveness of controls. Assessors relied on representations regarding scope completeness and should be engaged to re-perform or expand testing when architecture, custodians, contracts, or token logic materially change. Residual risk may remain even when controls appear suitably designed; compensating controls must be explicitly documented.

Key considerations for mining pools & payout models include segregation of duties, least-privilege access, audit logging with tamper-evident retention, encryption in transit and at rest for sensitive payloads, and periodic independent validation of backups and recovery paths. For mining infrastructure, assessors evaluated logical access to management interfaces, change tickets for firmware or pool configuration, and alignment with vendor hardening baselines.

Observations are classified per the severity model in Section 23. Informational items improve maturity; medium and above require tracked remediation with target completion dates and evidence packs. CleanSpark should maintain a continuous monitoring calendar covering certificate expiry, access recertification, dependency advisories, and hashrate anomaly detection correlated with power telemetry.

Cross-dependencies: findings in custody and key management may amplify smart-contract operational risks if administrative keys overlap with deployer roles. CleanSpark should enforce role separation between mining treasury keys, token admin keys (if any), and routine payroll or vendor payment keys. Table 13 in the evidence index references representative samples reviewed for this subsection.

WP 3.1 — Difficulty adjustment & probabilistic revenue

This subsection (3.1) addresses whitepaper narrative within the CleanSpark Extended Security & Audit Assessment dated 2026. The assessment covers Bitcoin mining operations, hosting relationships, treasury workflows, and CLSK on BNB Smart Chain as described in the system boundary statement. Procedures performed were limited to inquiry, observation, inspection of selected artifacts, and agreed-upon analytics where noted. No opinion on financial statements is expressed.

Management is responsible for design, implementation, and operating effectiveness of controls. Assessors relied on representations regarding scope completeness and should be engaged to re-perform or expand testing when architecture, custodians, contracts, or token logic materially change. Residual risk may remain even when controls appear suitably designed; compensating controls must be explicitly documented.

Key considerations for difficulty adjustment & probabilistic revenue include segregation of duties, least-privilege access, audit logging with tamper-evident retention, encryption in transit and at rest for sensitive payloads, and periodic independent validation of backups and recovery paths. For mining infrastructure, assessors evaluated logical access to management interfaces, change tickets for firmware or pool configuration, and alignment with vendor hardening baselines.

Observations are classified per the severity model in Section 23. Informational items improve maturity; medium and above require tracked remediation with target completion dates

and evidence packs. CleanSpark should maintain a continuous monitoring calendar covering certificate expiry, access recertification, dependency advisories, and hashrate anomaly detection correlated with power telemetry.

Cross-dependencies: findings in custody and key management may amplify smart-contract operational risks if administrative keys overlap with deployer roles. CleanSpark should enforce role separation between mining treasury keys, token admin keys (if any), and routine payroll or vendor payment keys. Table 21 in the evidence index references representative samples reviewed for this subsection.

WP 3.2 — Difficulty adjustment & probabilistic revenue

This subsection (3.2) addresses whitepaper narrative within the CleanSpark Extended Security & Audit Assessment dated 2026. The assessment covers Bitcoin mining operations, hosting relationships, treasury workflows, and CLSK on BNB Smart Chain as described in the system boundary statement. Procedures performed were limited to inquiry, observation, inspection of selected artifacts, and agreed-upon analytics where noted. No opinion on financial statements is expressed.

Management is responsible for design, implementation, and operating effectiveness of controls. Assessors relied on representations regarding scope completeness and should be engaged to re-perform or expand testing when architecture, custodians, contracts, or token logic materially change. Residual risk may remain even when controls appear suitably designed; compensating controls must be explicitly documented.

Key considerations for difficulty adjustment & probabilistic revenue include segregation of duties, least-privilege access, audit logging with tamper-evident retention, encryption in transit and at rest for sensitive payloads, and periodic independent validation of backups and recovery paths. For mining infrastructure, assessors evaluated logical access to management interfaces, change tickets for firmware or pool configuration, and alignment with vendor hardening baselines.

Observations are classified per the severity model in Section 23. Informational items improve maturity; medium and above require tracked remediation with target completion dates and evidence packs. CleanSpark should maintain a continuous monitoring calendar covering certificate expiry, access recertification, dependency advisories, and hashrate anomaly detection correlated with power telemetry.

Cross-dependencies: findings in custody and key management may amplify smart-contract operational risks if administrative keys overlap with deployer roles. CleanSpark should enforce role separation between mining treasury keys, token admin keys (if any), and routine payroll or vendor payment keys. Table 22 in the evidence index references representative samples reviewed for this subsection.

WP 3.3 — Difficulty adjustment & probabilistic revenue

This subsection (3.3) addresses whitepaper narrative within the CleanSpark Extended Security & Audit Assessment dated 2026. The assessment covers Bitcoin mining operations, hosting relationships, treasury workflows, and CLSK on BNB Smart Chain as described in the system boundary statement. Procedures performed were limited to inquiry, observation, inspection of selected artifacts, and agreed-upon analytics where noted. No opinion on financial statements is expressed.

Management is responsible for design, implementation, and operating effectiveness of controls. Assessors relied on representations regarding scope completeness and should be engaged to re-perform or expand testing when architecture, custodians, contracts, or token logic materially change. Residual risk may remain even when controls appear suitably designed; compensating controls must be explicitly documented.

Key considerations for difficulty adjustment & probabilistic revenue include segregation of duties, least-privilege access, audit logging with tamper-evident retention, encryption in transit and at rest for sensitive payloads, and periodic independent validation of backups and recovery paths. For mining infrastructure, assessors evaluated logical access to management interfaces, change tickets for firmware or pool configuration, and alignment with vendor hardening baselines.

Observations are classified per the severity model in Section 23. Informational items

improve maturity; medium and above require tracked remediation with target completion dates and evidence packs. CleanSpark should maintain a continuous monitoring calendar covering certificate expiry, access recertification, dependency advisories, and hashrate anomaly detection correlated with power telemetry.

Cross-dependencies: findings in custody and key management may amplify smart-contract operational risks if administrative keys overlap with deployer roles. CleanSpark should enforce role separation between mining treasury keys, token admin keys (if any), and routine payroll or vendor payment keys. Table 23 in the evidence index references representative samples reviewed for this subsection.

WP 4.1 — Halving schedule & long-cycle planning

This subsection (4.1) addresses whitepaper narrative within the CleanSpark Extended Security & Audit Assessment dated 2026. The assessment covers Bitcoin mining operations, hosting relationships, treasury workflows, and CLSK on BNB Smart Chain as described in the system boundary statement. Procedures performed were limited to inquiry, observation, inspection of selected artifacts, and agreed-upon analytics where noted. No opinion on financial statements is expressed.

Management is responsible for design, implementation, and operating effectiveness of controls. Assessors relied on representations regarding scope completeness and should be engaged to re-perform or expand testing when architecture, custodians, contracts, or token logic materially change. Residual risk may remain even when controls appear suitably designed; compensating controls must be explicitly documented.

Key considerations for halving schedule & long-cycle planning include segregation of duties, least-privilege access, audit logging with tamper-evident retention, encryption in transit and at rest for sensitive payloads, and periodic independent validation of backups and recovery paths. For mining infrastructure, assessors evaluated logical access to management interfaces, change tickets for firmware or pool configuration, and alignment with vendor hardening baselines.

Observations are classified per the severity model in Section 23. Informational items improve maturity; medium and above require tracked remediation with target completion dates and evidence packs. CleanSpark should maintain a continuous monitoring calendar covering certificate expiry, access recertification, dependency advisories, and hashrate anomaly detection correlated with power telemetry.

Cross-dependencies: findings in custody and key management may amplify smart-contract operational risks if administrative keys overlap with deployer roles. CleanSpark should enforce role separation between mining treasury keys, token admin keys (if any), and routine payroll or vendor payment keys. Table 31 in the evidence index references representative samples reviewed for this subsection.

WP 4.2 — Halving schedule & long-cycle planning

This subsection (4.2) addresses whitepaper narrative within the CleanSpark Extended Security & Audit Assessment dated 2026. The assessment covers Bitcoin mining operations, hosting relationships, treasury workflows, and CLSK on BNB Smart Chain as described in the system boundary statement. Procedures performed were limited to inquiry, observation, inspection of selected artifacts, and agreed-upon analytics where noted. No opinion on financial statements is expressed.

Management is responsible for design, implementation, and operating effectiveness of controls. Assessors relied on representations regarding scope completeness and should be engaged to re-perform or expand testing when architecture, custodians, contracts, or token logic materially change. Residual risk may remain even when controls appear suitably designed; compensating controls must be explicitly documented.

Key considerations for halving schedule & long-cycle planning include segregation of duties, least-privilege access, audit logging with tamper-evident retention, encryption in transit and at rest for sensitive payloads, and periodic independent validation of backups and recovery paths. For mining infrastructure, assessors evaluated logical access to management interfaces, change tickets for firmware or pool configuration, and alignment with vendor hardening baselines.

Observations are classified per the severity model in Section 23. Informational items improve maturity; medium and above require tracked remediation with target completion dates and evidence packs. CleanSpark should maintain a continuous monitoring calendar covering certificate expiry, access recertification, dependency advisories, and hashrate anomaly detection correlated with power telemetry.

Cross-dependencies: findings in custody and key management may amplify smart-contract operational risks if administrative keys overlap with deployer roles. CleanSpark should enforce role separation between mining treasury keys, token admin keys (if any), and routine payroll or vendor payment keys. Table 32 in the evidence index references representative samples reviewed for this subsection.

WP 4.3 — Halving schedule & long-cycle planning

This subsection (4.3) addresses whitepaper narrative within the CleanSpark Extended Security & Audit Assessment dated 2026. The assessment covers Bitcoin mining operations, hosting relationships, treasury workflows, and CLSK on BNB Smart Chain as described in the system boundary statement. Procedures performed were limited to inquiry, observation, inspection of selected artifacts, and agreed-upon analytics where noted. No opinion on financial statements is expressed.

Management is responsible for design, implementation, and operating effectiveness of controls. Assessors relied on representations regarding scope completeness and should be engaged to re-perform or expand testing when architecture, custodians, contracts, or token logic materially change. Residual risk may remain even when controls appear suitably designed; compensating controls must be explicitly documented.

Key considerations for halving schedule & long-cycle planning include segregation of duties, least-privilege access, audit logging with tamper-evident retention, encryption in transit and at rest for sensitive payloads, and periodic independent validation of backups and recovery paths. For mining infrastructure, assessors evaluated logical access to management interfaces, change tickets for firmware or pool configuration, and alignment with vendor hardening baselines.

Observations are classified per the severity model in Section 23. Informational items improve maturity; medium and above require tracked remediation with target completion dates and evidence packs. CleanSpark should maintain a continuous monitoring calendar covering certificate expiry, access recertification, dependency advisories, and hashrate anomaly detection correlated with power telemetry.

Cross-dependencies: findings in custody and key management may amplify smart-contract operational risks if administrative keys overlap with deployer roles. CleanSpark should enforce role separation between mining treasury keys, token admin keys (if any), and routine payroll or vendor payment keys. Table 33 in the evidence index references representative samples reviewed for this subsection.

WP 5.1 — Hardware generations & obsolescence curves

This subsection (5.1) addresses whitepaper narrative within the CleanSpark Extended Security & Audit Assessment dated 2026. The assessment covers Bitcoin mining operations, hosting relationships, treasury workflows, and CLSK on BNB Smart Chain as described in the system boundary statement. Procedures performed were limited to inquiry, observation, inspection of selected artifacts, and agreed-upon analytics where noted. No opinion on financial statements is expressed.

Management is responsible for design, implementation, and operating effectiveness of controls. Assessors relied on representations regarding scope completeness and should be engaged to re-perform or expand testing when architecture, custodians, contracts, or token logic materially change. Residual risk may remain even when controls appear suitably designed; compensating controls must be explicitly documented.

Key considerations for hardware generations & obsolescence curves include segregation of duties, least-privilege access, audit logging with tamper-evident retention, encryption in transit and at rest for sensitive payloads, and periodic independent validation of backups and recovery paths. For mining infrastructure, assessors evaluated logical access to management interfaces, change tickets for firmware or pool configuration, and alignment with

vendor hardening baselines.

Observations are classified per the severity model in Section 23. Informational items improve maturity; medium and above require tracked remediation with target completion dates and evidence packs. CleanSpark should maintain a continuous monitoring calendar covering certificate expiry, access recertification, dependency advisories, and hashrate anomaly detection correlated with power telemetry.

Cross-dependencies: findings in custody and key management may amplify smart-contract operational risks if administrative keys overlap with deployer roles. CleanSpark should enforce role separation between mining treasury keys, token admin keys (if any), and routine payroll or vendor payment keys. Table 41 in the evidence index references representative samples reviewed for this subsection.

WP 5.2 — Hardware generations & obsolescence curves

This subsection (5.2) addresses whitepaper narrative within the CleanSpark Extended Security & Audit Assessment dated 2026. The assessment covers Bitcoin mining operations, hosting relationships, treasury workflows, and CLSK on BNB Smart Chain as described in the system boundary statement. Procedures performed were limited to inquiry, observation, inspection of selected artifacts, and agreed-upon analytics where noted. No opinion on financial statements is expressed.

Management is responsible for design, implementation, and operating effectiveness of controls. Assessors relied on representations regarding scope completeness and should be engaged to re-perform or expand testing when architecture, custodians, contracts, or token logic materially change. Residual risk may remain even when controls appear suitably designed; compensating controls must be explicitly documented.

Key considerations for hardware generations & obsolescence curves include segregation of duties, least-privilege access, audit logging with tamper-evident retention, encryption in transit and at rest for sensitive payloads, and periodic independent validation of backups and recovery paths. For mining infrastructure, assessors evaluated logical access to management interfaces, change tickets for firmware or pool configuration, and alignment with vendor hardening baselines.

Observations are classified per the severity model in Section 23. Informational items improve maturity; medium and above require tracked remediation with target completion dates and evidence packs. CleanSpark should maintain a continuous monitoring calendar covering certificate expiry, access recertification, dependency advisories, and hashrate anomaly detection correlated with power telemetry.

Cross-dependencies: findings in custody and key management may amplify smart-contract operational risks if administrative keys overlap with deployer roles. CleanSpark should enforce role separation between mining treasury keys, token admin keys (if any), and routine payroll or vendor payment keys. Table 42 in the evidence index references representative samples reviewed for this subsection.

WP 5.3 — Hardware generations & obsolescence curves

This subsection (5.3) addresses whitepaper narrative within the CleanSpark Extended Security & Audit Assessment dated 2026. The assessment covers Bitcoin mining operations, hosting relationships, treasury workflows, and CLSK on BNB Smart Chain as described in the system boundary statement. Procedures performed were limited to inquiry, observation, inspection of selected artifacts, and agreed-upon analytics where noted. No opinion on financial statements is expressed.

Management is responsible for design, implementation, and operating effectiveness of controls. Assessors relied on representations regarding scope completeness and should be engaged to re-perform or expand testing when architecture, custodians, contracts, or token logic materially change. Residual risk may remain even when controls appear suitably designed; compensating controls must be explicitly documented.

Key considerations for hardware generations & obsolescence curves include segregation of duties, least-privilege access, audit logging with tamper-evident retention, encryption in transit and at rest for sensitive payloads, and periodic independent validation of backups and recovery paths. For mining infrastructure, assessors evaluated logical access to

management interfaces, change tickets for firmware or pool configuration, and alignment with vendor hardening baselines.

Observations are classified per the severity model in Section 23. Informational items improve maturity; medium and above require tracked remediation with target completion dates and evidence packs. CleanSpark should maintain a continuous monitoring calendar covering certificate expiry, access recertification, dependency advisories, and hashrate anomaly detection correlated with power telemetry.

Cross-dependencies: findings in custody and key management may amplify smart-contract operational risks if administrative keys overlap with deployer roles. CleanSpark should enforce role separation between mining treasury keys, token admin keys (if any), and routine payroll or vendor payment keys. Table 43 in the evidence index references representative samples reviewed for this subsection.

WP 6.1 — Immersion vs air cooling tradeoffs

This subsection (6.1) addresses whitepaper narrative within the CleanSpark Extended Security & Audit Assessment dated 2026. The assessment covers Bitcoin mining operations, hosting relationships, treasury workflows, and CLSK on BNB Smart Chain as described in the system boundary statement. Procedures performed were limited to inquiry, observation, inspection of selected artifacts, and agreed-upon analytics where noted. No opinion on financial statements is expressed.

Management is responsible for design, implementation, and operating effectiveness of controls. Assessors relied on representations regarding scope completeness and should be engaged to re-perform or expand testing when architecture, custodians, contracts, or token logic materially change. Residual risk may remain even when controls appear suitably designed; compensating controls must be explicitly documented.

Key considerations for immersion vs air cooling tradeoffs include segregation of duties, least-privilege access, audit logging with tamper-evident retention, encryption in transit and at rest for sensitive payloads, and periodic independent validation of backups and recovery paths. For mining infrastructure, assessors evaluated logical access to management interfaces, change tickets for firmware or pool configuration, and alignment with vendor hardening baselines.

Observations are classified per the severity model in Section 23. Informational items improve maturity; medium and above require tracked remediation with target completion dates and evidence packs. CleanSpark should maintain a continuous monitoring calendar covering certificate expiry, access recertification, dependency advisories, and hashrate anomaly detection correlated with power telemetry.

Cross-dependencies: findings in custody and key management may amplify smart-contract operational risks if administrative keys overlap with deployer roles. CleanSpark should enforce role separation between mining treasury keys, token admin keys (if any), and routine payroll or vendor payment keys. Table 51 in the evidence index references representative samples reviewed for this subsection.

WP 6.2 — Immersion vs air cooling tradeoffs

This subsection (6.2) addresses whitepaper narrative within the CleanSpark Extended Security & Audit Assessment dated 2026. The assessment covers Bitcoin mining operations, hosting relationships, treasury workflows, and CLSK on BNB Smart Chain as described in the system boundary statement. Procedures performed were limited to inquiry, observation, inspection of selected artifacts, and agreed-upon analytics where noted. No opinion on financial statements is expressed.

Management is responsible for design, implementation, and operating effectiveness of controls. Assessors relied on representations regarding scope completeness and should be engaged to re-perform or expand testing when architecture, custodians, contracts, or token logic materially change. Residual risk may remain even when controls appear suitably designed; compensating controls must be explicitly documented.

Key considerations for immersion vs air cooling tradeoffs include segregation of duties, least-privilege access, audit logging with tamper-evident retention, encryption in transit and at rest for sensitive payloads, and periodic independent validation of backups and

recovery paths. For mining infrastructure, assessors evaluated logical access to management interfaces, change tickets for firmware or pool configuration, and alignment with vendor hardening baselines.

Observations are classified per the severity model in Section 23. Informational items improve maturity; medium and above require tracked remediation with target completion dates and evidence packs. CleanSpark should maintain a continuous monitoring calendar covering certificate expiry, access recertification, dependency advisories, and hashrate anomaly detection correlated with power telemetry.

Cross-dependencies: findings in custody and key management may amplify smart-contract operational risks if administrative keys overlap with deployer roles. CleanSpark should enforce role separation between mining treasury keys, token admin keys (if any), and routine payroll or vendor payment keys. Table 52 in the evidence index references representative samples reviewed for this subsection.

WP 6.3 — Immersion vs air cooling tradeoffs

This subsection (6.3) addresses whitepaper narrative within the CleanSpark Extended Security & Audit Assessment dated 2026. The assessment covers Bitcoin mining operations, hosting relationships, treasury workflows, and CLSK on BNB Smart Chain as described in the system boundary statement. Procedures performed were limited to inquiry, observation, inspection of selected artifacts, and agreed-upon analytics where noted. No opinion on financial statements is expressed.

Management is responsible for design, implementation, and operating effectiveness of controls. Assessors relied on representations regarding scope completeness and should be engaged to re-perform or expand testing when architecture, custodians, contracts, or token logic materially change. Residual risk may remain even when controls appear suitably designed; compensating controls must be explicitly documented.

Key considerations for immersion vs air cooling tradeoffs include segregation of duties, least-privilege access, audit logging with tamper-evident retention, encryption in transit and at rest for sensitive payloads, and periodic independent validation of backups and recovery paths. For mining infrastructure, assessors evaluated logical access to management interfaces, change tickets for firmware or pool configuration, and alignment with vendor hardening baselines.

Observations are classified per the severity model in Section 23. Informational items improve maturity; medium and above require tracked remediation with target completion dates and evidence packs. CleanSpark should maintain a continuous monitoring calendar covering certificate expiry, access recertification, dependency advisories, and hashrate anomaly detection correlated with power telemetry.

Cross-dependencies: findings in custody and key management may amplify smart-contract operational risks if administrative keys overlap with deployer roles. CleanSpark should enforce role separation between mining treasury keys, token admin keys (if any), and routine payroll or vendor payment keys. Table 53 in the evidence index references representative samples reviewed for this subsection.

WP 7.1 — Site selection & interconnection queues

This subsection (7.1) addresses whitepaper narrative within the CleanSpark Extended Security & Audit Assessment dated 2026. The assessment covers Bitcoin mining operations, hosting relationships, treasury workflows, and CLSK on BNB Smart Chain as described in the system boundary statement. Procedures performed were limited to inquiry, observation, inspection of selected artifacts, and agreed-upon analytics where noted. No opinion on financial statements is expressed.

Management is responsible for design, implementation, and operating effectiveness of controls. Assessors relied on representations regarding scope completeness and should be engaged to re-perform or expand testing when architecture, custodians, contracts, or token logic materially change. Residual risk may remain even when controls appear suitably designed; compensating controls must be explicitly documented.

Key considerations for site selection & interconnection queues include segregation of duties, least-privilege access, audit logging with tamper-evident retention, encryption in

transit and at rest for sensitive payloads, and periodic independent validation of backups and recovery paths. For mining infrastructure, assessors evaluated logical access to management interfaces, change tickets for firmware or pool configuration, and alignment with vendor hardening baselines.

Observations are classified per the severity model in Section 23. Informational items improve maturity; medium and above require tracked remediation with target completion dates and evidence packs. CleanSpark should maintain a continuous monitoring calendar covering certificate expiry, access recertification, dependency advisories, and hashrate anomaly detection correlated with power telemetry.

Cross-dependencies: findings in custody and key management may amplify smart-contract operational risks if administrative keys overlap with deployer roles. CleanSpark should enforce role separation between mining treasury keys, token admin keys (if any), and routine payroll or vendor payment keys. Table 61 in the evidence index references representative samples reviewed for this subsection.

WP 7.2 — Site selection & interconnection queues

This subsection (7.2) addresses whitepaper narrative within the CleanSpark Extended Security & Audit Assessment dated 2026. The assessment covers Bitcoin mining operations, hosting relationships, treasury workflows, and CLSK on BNB Smart Chain as described in the system boundary statement. Procedures performed were limited to inquiry, observation, inspection of selected artifacts, and agreed-upon analytics where noted. No opinion on financial statements is expressed.

Management is responsible for design, implementation, and operating effectiveness of controls. Assessors relied on representations regarding scope completeness and should be engaged to re-perform or expand testing when architecture, custodians, contracts, or token logic materially change. Residual risk may remain even when controls appear suitably designed; compensating controls must be explicitly documented.

Key considerations for site selection & interconnection queues include segregation of duties, least-privilege access, audit logging with tamper-evident retention, encryption in transit and at rest for sensitive payloads, and periodic independent validation of backups and recovery paths. For mining infrastructure, assessors evaluated logical access to management interfaces, change tickets for firmware or pool configuration, and alignment with vendor hardening baselines.

Observations are classified per the severity model in Section 23. Informational items improve maturity; medium and above require tracked remediation with target completion dates and evidence packs. CleanSpark should maintain a continuous monitoring calendar covering certificate expiry, access recertification, dependency advisories, and hashrate anomaly detection correlated with power telemetry.

Cross-dependencies: findings in custody and key management may amplify smart-contract operational risks if administrative keys overlap with deployer roles. CleanSpark should enforce role separation between mining treasury keys, token admin keys (if any), and routine payroll or vendor payment keys. Table 62 in the evidence index references representative samples reviewed for this subsection.

WP 7.3 — Site selection & interconnection queues

This subsection (7.3) addresses whitepaper narrative within the CleanSpark Extended Security & Audit Assessment dated 2026. The assessment covers Bitcoin mining operations, hosting relationships, treasury workflows, and CLSK on BNB Smart Chain as described in the system boundary statement. Procedures performed were limited to inquiry, observation, inspection of selected artifacts, and agreed-upon analytics where noted. No opinion on financial statements is expressed.

Management is responsible for design, implementation, and operating effectiveness of controls. Assessors relied on representations regarding scope completeness and should be engaged to re-perform or expand testing when architecture, custodians, contracts, or token logic materially change. Residual risk may remain even when controls appear suitably designed; compensating controls must be explicitly documented.

Key considerations for site selection & interconnection queues include segregation of

duties, least-privilege access, audit logging with tamper-evident retention, encryption in transit and at rest for sensitive payloads, and periodic independent validation of backups and recovery paths. For mining infrastructure, assessors evaluated logical access to management interfaces, change tickets for firmware or pool configuration, and alignment with vendor hardening baselines.

Observations are classified per the severity model in Section 23. Informational items improve maturity; medium and above require tracked remediation with target completion dates and evidence packs. CleanSpark should maintain a continuous monitoring calendar covering certificate expiry, access recertification, dependency advisories, and hashrate anomaly detection correlated with power telemetry.

Cross-dependencies: findings in custody and key management may amplify smart-contract operational risks if administrative keys overlap with deployer roles. CleanSpark should enforce role separation between mining treasury keys, token admin keys (if any), and routine payroll or vendor payment keys. Table 63 in the evidence index references representative samples reviewed for this subsection.

WP 8.1 — Demand response & curtailment revenue

This subsection (8.1) addresses whitepaper narrative within the CleanSpark Extended Security & Audit Assessment dated 2026. The assessment covers Bitcoin mining operations, hosting relationships, treasury workflows, and CLSK on BNB Smart Chain as described in the system boundary statement. Procedures performed were limited to inquiry, observation, inspection of selected artifacts, and agreed-upon analytics where noted. No opinion on financial statements is expressed.

Management is responsible for design, implementation, and operating effectiveness of controls. Assessors relied on representations regarding scope completeness and should be engaged to re-perform or expand testing when architecture, custodians, contracts, or token logic materially change. Residual risk may remain even when controls appear suitably designed; compensating controls must be explicitly documented.

Key considerations for demand response & curtailment revenue include segregation of duties, least-privilege access, audit logging with tamper-evident retention, encryption in transit and at rest for sensitive payloads, and periodic independent validation of backups and recovery paths. For mining infrastructure, assessors evaluated logical access to management interfaces, change tickets for firmware or pool configuration, and alignment with vendor hardening baselines.

Observations are classified per the severity model in Section 23. Informational items improve maturity; medium and above require tracked remediation with target completion dates and evidence packs. CleanSpark should maintain a continuous monitoring calendar covering certificate expiry, access recertification, dependency advisories, and hashrate anomaly detection correlated with power telemetry.

Cross-dependencies: findings in custody and key management may amplify smart-contract operational risks if administrative keys overlap with deployer roles. CleanSpark should enforce role separation between mining treasury keys, token admin keys (if any), and routine payroll or vendor payment keys. Table 71 in the evidence index references representative samples reviewed for this subsection.

WP 8.2 — Demand response & curtailment revenue

This subsection (8.2) addresses whitepaper narrative within the CleanSpark Extended Security & Audit Assessment dated 2026. The assessment covers Bitcoin mining operations, hosting relationships, treasury workflows, and CLSK on BNB Smart Chain as described in the system boundary statement. Procedures performed were limited to inquiry, observation, inspection of selected artifacts, and agreed-upon analytics where noted. No opinion on financial statements is expressed.

Management is responsible for design, implementation, and operating effectiveness of controls. Assessors relied on representations regarding scope completeness and should be engaged to re-perform or expand testing when architecture, custodians, contracts, or token logic materially change. Residual risk may remain even when controls appear suitably designed; compensating controls must be explicitly documented.

Key considerations for demand response & curtailment revenue include segregation of duties, least-privilege access, audit logging with tamper-evident retention, encryption in transit and at rest for sensitive payloads, and periodic independent validation of backups and recovery paths. For mining infrastructure, assessors evaluated logical access to management interfaces, change tickets for firmware or pool configuration, and alignment with vendor hardening baselines.

Observations are classified per the severity model in Section 23. Informational items improve maturity; medium and above require tracked remediation with target completion dates and evidence packs. CleanSpark should maintain a continuous monitoring calendar covering certificate expiry, access recertification, dependency advisories, and hashrate anomaly detection correlated with power telemetry.

Cross-dependencies: findings in custody and key management may amplify smart-contract operational risks if administrative keys overlap with deployer roles. CleanSpark should enforce role separation between mining treasury keys, token admin keys (if any), and routine payroll or vendor payment keys. Table 72 in the evidence index references representative samples reviewed for this subsection.

WP 8.3 — Demand response & curtailment revenue

This subsection (8.3) addresses whitepaper narrative within the CleanSpark Extended Security & Audit Assessment dated 2026. The assessment covers Bitcoin mining operations, hosting relationships, treasury workflows, and CLSK on BNB Smart Chain as described in the system boundary statement. Procedures performed were limited to inquiry, observation, inspection of selected artifacts, and agreed-upon analytics where noted. No opinion on financial statements is expressed.

Management is responsible for design, implementation, and operating effectiveness of controls. Assessors relied on representations regarding scope completeness and should be engaged to re-perform or expand testing when architecture, custodians, contracts, or token logic materially change. Residual risk may remain even when controls appear suitably designed; compensating controls must be explicitly documented.

Key considerations for demand response & curtailment revenue include segregation of duties, least-privilege access, audit logging with tamper-evident retention, encryption in transit and at rest for sensitive payloads, and periodic independent validation of backups and recovery paths. For mining infrastructure, assessors evaluated logical access to management interfaces, change tickets for firmware or pool configuration, and alignment with vendor hardening baselines.

Observations are classified per the severity model in Section 23. Informational items improve maturity; medium and above require tracked remediation with target completion dates and evidence packs. CleanSpark should maintain a continuous monitoring calendar covering certificate expiry, access recertification, dependency advisories, and hashrate anomaly detection correlated with power telemetry.

Cross-dependencies: findings in custody and key management may amplify smart-contract operational risks if administrative keys overlap with deployer roles. CleanSpark should enforce role separation between mining treasury keys, token admin keys (if any), and routine payroll or vendor payment keys. Table 73 in the evidence index references representative samples reviewed for this subsection.

WP 9.1 — Renewable credits & attribute claims

This subsection (9.1) addresses whitepaper narrative within the CleanSpark Extended Security & Audit Assessment dated 2026. The assessment covers Bitcoin mining operations, hosting relationships, treasury workflows, and CLSK on BNB Smart Chain as described in the system boundary statement. Procedures performed were limited to inquiry, observation, inspection of selected artifacts, and agreed-upon analytics where noted. No opinion on financial statements is expressed.

Management is responsible for design, implementation, and operating effectiveness of controls. Assessors relied on representations regarding scope completeness and should be engaged to re-perform or expand testing when architecture, custodians, contracts, or token logic materially change. Residual risk may remain even when controls appear suitably

designed; compensating controls must be explicitly documented.

Key considerations for renewable credits & attribute claims include segregation of duties, least-privilege access, audit logging with tamper-evident retention, encryption in transit and at rest for sensitive payloads, and periodic independent validation of backups and recovery paths. For mining infrastructure, assessors evaluated logical access to management interfaces, change tickets for firmware or pool configuration, and alignment with vendor hardening baselines.

Observations are classified per the severity model in Section 23. Informational items improve maturity; medium and above require tracked remediation with target completion dates and evidence packs. CleanSpark should maintain a continuous monitoring calendar covering certificate expiry, access recertification, dependency advisories, and hashrate anomaly detection correlated with power telemetry.

Cross-dependencies: findings in custody and key management may amplify smart-contract operational risks if administrative keys overlap with deployer roles. CleanSpark should enforce role separation between mining treasury keys, token admin keys (if any), and routine payroll or vendor payment keys. Table 81 in the evidence index references representative samples reviewed for this subsection.

WP 9.2 — Renewable credits & attribute claims

This subsection (9.2) addresses whitepaper narrative within the CleanSpark Extended Security & Audit Assessment dated 2026. The assessment covers Bitcoin mining operations, hosting relationships, treasury workflows, and CLSK on BNB Smart Chain as described in the system boundary statement. Procedures performed were limited to inquiry, observation, inspection of selected artifacts, and agreed-upon analytics where noted. No opinion on financial statements is expressed.

Management is responsible for design, implementation, and operating effectiveness of controls. Assessors relied on representations regarding scope completeness and should be engaged to re-perform or expand testing when architecture, custodians, contracts, or token logic materially change. Residual risk may remain even when controls appear suitably designed; compensating controls must be explicitly documented.

Key considerations for renewable credits & attribute claims include segregation of duties, least-privilege access, audit logging with tamper-evident retention, encryption in transit and at rest for sensitive payloads, and periodic independent validation of backups and recovery paths. For mining infrastructure, assessors evaluated logical access to management interfaces, change tickets for firmware or pool configuration, and alignment with vendor hardening baselines.

Observations are classified per the severity model in Section 23. Informational items improve maturity; medium and above require tracked remediation with target completion dates and evidence packs. CleanSpark should maintain a continuous monitoring calendar covering certificate expiry, access recertification, dependency advisories, and hashrate anomaly detection correlated with power telemetry.

Cross-dependencies: findings in custody and key management may amplify smart-contract operational risks if administrative keys overlap with deployer roles. CleanSpark should enforce role separation between mining treasury keys, token admin keys (if any), and routine payroll or vendor payment keys. Table 82 in the evidence index references representative samples reviewed for this subsection.

WP 9.3 — Renewable credits & attribute claims

This subsection (9.3) addresses whitepaper narrative within the CleanSpark Extended Security & Audit Assessment dated 2026. The assessment covers Bitcoin mining operations, hosting relationships, treasury workflows, and CLSK on BNB Smart Chain as described in the system boundary statement. Procedures performed were limited to inquiry, observation, inspection of selected artifacts, and agreed-upon analytics where noted. No opinion on financial statements is expressed.

Management is responsible for design, implementation, and operating effectiveness of controls. Assessors relied on representations regarding scope completeness and should be engaged to re-perform or expand testing when architecture, custodians, contracts, or token

logic materially change. Residual risk may remain even when controls appear suitably designed; compensating controls must be explicitly documented.

Key considerations for renewable credits & attribute claims include segregation of duties, least-privilege access, audit logging with tamper-evident retention, encryption in transit and at rest for sensitive payloads, and periodic independent validation of backups and recovery paths. For mining infrastructure, assessors evaluated logical access to management interfaces, change tickets for firmware or pool configuration, and alignment with vendor hardening baselines.

Observations are classified per the severity model in Section 23. Informational items improve maturity; medium and above require tracked remediation with target completion dates and evidence packs. CleanSpark should maintain a continuous monitoring calendar covering certificate expiry, access recertification, dependency advisories, and hashrate anomaly detection correlated with power telemetry.

Cross-dependencies: findings in custody and key management may amplify smart-contract operational risks if administrative keys overlap with deployer roles. CleanSpark should enforce role separation between mining treasury keys, token admin keys (if any), and routine payroll or vendor payment keys. Table 83 in the evidence index references representative samples reviewed for this subsection.

WP 10.1 — Grid stability & ancillary services

This subsection (10.1) addresses whitepaper narrative within the CleanSpark Extended Security & Audit Assessment dated 2026. The assessment covers Bitcoin mining operations, hosting relationships, treasury workflows, and CLSK on BNB Smart Chain as described in the system boundary statement. Procedures performed were limited to inquiry, observation, inspection of selected artifacts, and agreed-upon analytics where noted. No opinion on financial statements is expressed.

Management is responsible for design, implementation, and operating effectiveness of controls. Assessors relied on representations regarding scope completeness and should be engaged to re-perform or expand testing when architecture, custodians, contracts, or token logic materially change. Residual risk may remain even when controls appear suitably designed; compensating controls must be explicitly documented.

Key considerations for grid stability & ancillary services include segregation of duties, least-privilege access, audit logging with tamper-evident retention, encryption in transit and at rest for sensitive payloads, and periodic independent validation of backups and recovery paths. For mining infrastructure, assessors evaluated logical access to management interfaces, change tickets for firmware or pool configuration, and alignment with vendor hardening baselines.

Observations are classified per the severity model in Section 23. Informational items improve maturity; medium and above require tracked remediation with target completion dates and evidence packs. CleanSpark should maintain a continuous monitoring calendar covering certificate expiry, access recertification, dependency advisories, and hashrate anomaly detection correlated with power telemetry.

Cross-dependencies: findings in custody and key management may amplify smart-contract operational risks if administrative keys overlap with deployer roles. CleanSpark should enforce role separation between mining treasury keys, token admin keys (if any), and routine payroll or vendor payment keys. Table 91 in the evidence index references representative samples reviewed for this subsection.

WP 10.2 — Grid stability & ancillary services

This subsection (10.2) addresses whitepaper narrative within the CleanSpark Extended Security & Audit Assessment dated 2026. The assessment covers Bitcoin mining operations, hosting relationships, treasury workflows, and CLSK on BNB Smart Chain as described in the system boundary statement. Procedures performed were limited to inquiry, observation, inspection of selected artifacts, and agreed-upon analytics where noted. No opinion on financial statements is expressed.

Management is responsible for design, implementation, and operating effectiveness of controls. Assessors relied on representations regarding scope completeness and should be

engaged to re-perform or expand testing when architecture, custodians, contracts, or token logic materially change. Residual risk may remain even when controls appear suitably designed; compensating controls must be explicitly documented.

Key considerations for grid stability & ancillary services include segregation of duties, least-privilege access, audit logging with tamper-evident retention, encryption in transit and at rest for sensitive payloads, and periodic independent validation of backups and recovery paths. For mining infrastructure, assessors evaluated logical access to management interfaces, change tickets for firmware or pool configuration, and alignment with vendor hardening baselines.

Observations are classified per the severity model in Section 23. Informational items improve maturity; medium and above require tracked remediation with target completion dates and evidence packs. CleanSpark should maintain a continuous monitoring calendar covering certificate expiry, access recertification, dependency advisories, and hashrate anomaly detection correlated with power telemetry.

Cross-dependencies: findings in custody and key management may amplify smart-contract operational risks if administrative keys overlap with deployer roles. CleanSpark should enforce role separation between mining treasury keys, token admin keys (if any), and routine payroll or vendor payment keys. Table 92 in the evidence index references representative samples reviewed for this subsection.

WP 10.3 — Grid stability & ancillary services

This subsection (10.3) addresses whitepaper narrative within the CleanSpark Extended Security & Audit Assessment dated 2026. The assessment covers Bitcoin mining operations, hosting relationships, treasury workflows, and CLSK on BNB Smart Chain as described in the system boundary statement. Procedures performed were limited to inquiry, observation, inspection of selected artifacts, and agreed-upon analytics where noted. No opinion on financial statements is expressed.

Management is responsible for design, implementation, and operating effectiveness of controls. Assessors relied on representations regarding scope completeness and should be engaged to re-perform or expand testing when architecture, custodians, contracts, or token logic materially change. Residual risk may remain even when controls appear suitably designed; compensating controls must be explicitly documented.

Key considerations for grid stability & ancillary services include segregation of duties, least-privilege access, audit logging with tamper-evident retention, encryption in transit and at rest for sensitive payloads, and periodic independent validation of backups and recovery paths. For mining infrastructure, assessors evaluated logical access to management interfaces, change tickets for firmware or pool configuration, and alignment with vendor hardening baselines.

Observations are classified per the severity model in Section 23. Informational items improve maturity; medium and above require tracked remediation with target completion dates and evidence packs. CleanSpark should maintain a continuous monitoring calendar covering certificate expiry, access recertification, dependency advisories, and hashrate anomaly detection correlated with power telemetry.

Cross-dependencies: findings in custody and key management may amplify smart-contract operational risks if administrative keys overlap with deployer roles. CleanSpark should enforce role separation between mining treasury keys, token admin keys (if any), and routine payroll or vendor payment keys. Table 93 in the evidence index references representative samples reviewed for this subsection.

WP 11.1 — Natural gas & stranded energy partnerships

This subsection (11.1) addresses whitepaper narrative within the CleanSpark Extended Security & Audit Assessment dated 2026. The assessment covers Bitcoin mining operations, hosting relationships, treasury workflows, and CLSK on BNB Smart Chain as described in the system boundary statement. Procedures performed were limited to inquiry, observation, inspection of selected artifacts, and agreed-upon analytics where noted. No opinion on financial statements is expressed.

Management is responsible for design, implementation, and operating effectiveness of

controls. Assessors relied on representations regarding scope completeness and should be engaged to re-perform or expand testing when architecture, custodians, contracts, or token logic materially change. Residual risk may remain even when controls appear suitably designed; compensating controls must be explicitly documented.

Key considerations for natural gas & stranded energy partnerships include segregation of duties, least-privilege access, audit logging with tamper-evident retention, encryption in transit and at rest for sensitive payloads, and periodic independent validation of backups and recovery paths. For mining infrastructure, assessors evaluated logical access to management interfaces, change tickets for firmware or pool configuration, and alignment with vendor hardening baselines.

Observations are classified per the severity model in Section 23. Informational items improve maturity; medium and above require tracked remediation with target completion dates and evidence packs. CleanSpark should maintain a continuous monitoring calendar covering certificate expiry, access recertification, dependency advisories, and hashrate anomaly detection correlated with power telemetry.

Cross-dependencies: findings in custody and key management may amplify smart-contract operational risks if administrative keys overlap with deployer roles. CleanSpark should enforce role separation between mining treasury keys, token admin keys (if any), and routine payroll or vendor payment keys. Table 101 in the evidence index references representative samples reviewed for this subsection.

WP 11.2 — Natural gas & stranded energy partnerships

This subsection (11.2) addresses whitepaper narrative within the CleanSpark Extended Security & Audit Assessment dated 2026. The assessment covers Bitcoin mining operations, hosting relationships, treasury workflows, and CLSK on BNB Smart Chain as described in the system boundary statement. Procedures performed were limited to inquiry, observation, inspection of selected artifacts, and agreed-upon analytics where noted. No opinion on financial statements is expressed.

Management is responsible for design, implementation, and operating effectiveness of controls. Assessors relied on representations regarding scope completeness and should be engaged to re-perform or expand testing when architecture, custodians, contracts, or token logic materially change. Residual risk may remain even when controls appear suitably designed; compensating controls must be explicitly documented.

Key considerations for natural gas & stranded energy partnerships include segregation of duties, least-privilege access, audit logging with tamper-evident retention, encryption in transit and at rest for sensitive payloads, and periodic independent validation of backups and recovery paths. For mining infrastructure, assessors evaluated logical access to management interfaces, change tickets for firmware or pool configuration, and alignment with vendor hardening baselines.

Observations are classified per the severity model in Section 23. Informational items improve maturity; medium and above require tracked remediation with target completion dates and evidence packs. CleanSpark should maintain a continuous monitoring calendar covering certificate expiry, access recertification, dependency advisories, and hashrate anomaly detection correlated with power telemetry.

Cross-dependencies: findings in custody and key management may amplify smart-contract operational risks if administrative keys overlap with deployer roles. CleanSpark should enforce role separation between mining treasury keys, token admin keys (if any), and routine payroll or vendor payment keys. Table 102 in the evidence index references representative samples reviewed for this subsection.

WP 11.3 — Natural gas & stranded energy partnerships

This subsection (11.3) addresses whitepaper narrative within the CleanSpark Extended Security & Audit Assessment dated 2026. The assessment covers Bitcoin mining operations, hosting relationships, treasury workflows, and CLSK on BNB Smart Chain as described in the system boundary statement. Procedures performed were limited to inquiry, observation, inspection of selected artifacts, and agreed-upon analytics where noted. No opinion on financial statements is expressed.

Management is responsible for design, implementation, and operating effectiveness of controls. Assessors relied on representations regarding scope completeness and should be engaged to re-perform or expand testing when architecture, custodians, contracts, or token logic materially change. Residual risk may remain even when controls appear suitably designed; compensating controls must be explicitly documented.

Key considerations for natural gas & stranded energy partnerships include segregation of duties, least-privilege access, audit logging with tamper-evident retention, encryption in transit and at rest for sensitive payloads, and periodic independent validation of backups and recovery paths. For mining infrastructure, assessors evaluated logical access to management interfaces, change tickets for firmware or pool configuration, and alignment with vendor hardening baselines.

Observations are classified per the severity model in Section 23. Informational items improve maturity; medium and above require tracked remediation with target completion dates and evidence packs. CleanSpark should maintain a continuous monitoring calendar covering certificate expiry, access recertification, dependency advisories, and hashrate anomaly detection correlated with power telemetry.

Cross-dependencies: findings in custody and key management may amplify smart-contract operational risks if administrative keys overlap with deployer roles. CleanSpark should enforce role separation between mining treasury keys, token admin keys (if any), and routine payroll or vendor payment keys. Table 103 in the evidence index references representative samples reviewed for this subsection.

WP 12.1 — Nuclear & baseload offtake considerations

This subsection (12.1) addresses whitepaper narrative within the CleanSpark Extended Security & Audit Assessment dated 2026. The assessment covers Bitcoin mining operations, hosting relationships, treasury workflows, and CLSK on BNB Smart Chain as described in the system boundary statement. Procedures performed were limited to inquiry, observation, inspection of selected artifacts, and agreed-upon analytics where noted. No opinion on financial statements is expressed.

Management is responsible for design, implementation, and operating effectiveness of controls. Assessors relied on representations regarding scope completeness and should be engaged to re-perform or expand testing when architecture, custodians, contracts, or token logic materially change. Residual risk may remain even when controls appear suitably designed; compensating controls must be explicitly documented.

Key considerations for nuclear & baseload offtake considerations include segregation of duties, least-privilege access, audit logging with tamper-evident retention, encryption in transit and at rest for sensitive payloads, and periodic independent validation of backups and recovery paths. For mining infrastructure, assessors evaluated logical access to management interfaces, change tickets for firmware or pool configuration, and alignment with vendor hardening baselines.

Observations are classified per the severity model in Section 23. Informational items improve maturity; medium and above require tracked remediation with target completion dates and evidence packs. CleanSpark should maintain a continuous monitoring calendar covering certificate expiry, access recertification, dependency advisories, and hashrate anomaly detection correlated with power telemetry.

Cross-dependencies: findings in custody and key management may amplify smart-contract operational risks if administrative keys overlap with deployer roles. CleanSpark should enforce role separation between mining treasury keys, token admin keys (if any), and routine payroll or vendor payment keys. Table 111 in the evidence index references representative samples reviewed for this subsection.

WP 12.2 — Nuclear & baseload offtake considerations

This subsection (12.2) addresses whitepaper narrative within the CleanSpark Extended Security & Audit Assessment dated 2026. The assessment covers Bitcoin mining operations, hosting relationships, treasury workflows, and CLSK on BNB Smart Chain as described in the system boundary statement. Procedures performed were limited to inquiry, observation, inspection of selected artifacts, and agreed-upon analytics where noted. No opinion on

financial statements is expressed.

Management is responsible for design, implementation, and operating effectiveness of controls. Assessors relied on representations regarding scope completeness and should be engaged to re-perform or expand testing when architecture, custodians, contracts, or token logic materially change. Residual risk may remain even when controls appear suitably designed; compensating controls must be explicitly documented.

Key considerations for nuclear & baseload offtake considerations include segregation of duties, least-privilege access, audit logging with tamper-evident retention, encryption in transit and at rest for sensitive payloads, and periodic independent validation of backups and recovery paths. For mining infrastructure, assessors evaluated logical access to management interfaces, change tickets for firmware or pool configuration, and alignment with vendor hardening baselines.

Observations are classified per the severity model in Section 23. Informational items improve maturity; medium and above require tracked remediation with target completion dates and evidence packs. CleanSpark should maintain a continuous monitoring calendar covering certificate expiry, access recertification, dependency advisories, and hashrate anomaly detection correlated with power telemetry.

Cross-dependencies: findings in custody and key management may amplify smart-contract operational risks if administrative keys overlap with deployer roles. CleanSpark should enforce role separation between mining treasury keys, token admin keys (if any), and routine payroll or vendor payment keys. Table 112 in the evidence index references representative samples reviewed for this subsection.

WP 12.3 — Nuclear & baseload offtake considerations

This subsection (12.3) addresses whitepaper narrative within the CleanSpark Extended Security & Audit Assessment dated 2026. The assessment covers Bitcoin mining operations, hosting relationships, treasury workflows, and CLSK on BNB Smart Chain as described in the system boundary statement. Procedures performed were limited to inquiry, observation, inspection of selected artifacts, and agreed-upon analytics where noted. No opinion on financial statements is expressed.

Management is responsible for design, implementation, and operating effectiveness of controls. Assessors relied on representations regarding scope completeness and should be engaged to re-perform or expand testing when architecture, custodians, contracts, or token logic materially change. Residual risk may remain even when controls appear suitably designed; compensating controls must be explicitly documented.

Key considerations for nuclear & baseload offtake considerations include segregation of duties, least-privilege access, audit logging with tamper-evident retention, encryption in transit and at rest for sensitive payloads, and periodic independent validation of backups and recovery paths. For mining infrastructure, assessors evaluated logical access to management interfaces, change tickets for firmware or pool configuration, and alignment with vendor hardening baselines.

Observations are classified per the severity model in Section 23. Informational items improve maturity; medium and above require tracked remediation with target completion dates and evidence packs. CleanSpark should maintain a continuous monitoring calendar covering certificate expiry, access recertification, dependency advisories, and hashrate anomaly detection correlated with power telemetry.

Cross-dependencies: findings in custody and key management may amplify smart-contract operational risks if administrative keys overlap with deployer roles. CleanSpark should enforce role separation between mining treasury keys, token admin keys (if any), and routine payroll or vendor payment keys. Table 113 in the evidence index references representative samples reviewed for this subsection.

WP 13.1 — International logistics & tariffs

This subsection (13.1) addresses whitepaper narrative within the CleanSpark Extended Security & Audit Assessment dated 2026. The assessment covers Bitcoin mining operations, hosting relationships, treasury workflows, and CLSK on BNB Smart Chain as described in the system boundary statement. Procedures performed were limited to inquiry, observation,

inspection of selected artifacts, and agreed-upon analytics where noted. No opinion on financial statements is expressed.

Management is responsible for design, implementation, and operating effectiveness of controls. Assessors relied on representations regarding scope completeness and should be engaged to re-perform or expand testing when architecture, custodians, contracts, or token logic materially change. Residual risk may remain even when controls appear suitably designed; compensating controls must be explicitly documented.

Key considerations for international logistics & tariffs include segregation of duties, least-privilege access, audit logging with tamper-evident retention, encryption in transit and at rest for sensitive payloads, and periodic independent validation of backups and recovery paths. For mining infrastructure, assessors evaluated logical access to management interfaces, change tickets for firmware or pool configuration, and alignment with vendor hardening baselines.

Observations are classified per the severity model in Section 23. Informational items improve maturity; medium and above require tracked remediation with target completion dates and evidence packs. CleanSpark should maintain a continuous monitoring calendar covering certificate expiry, access recertification, dependency advisories, and hashrate anomaly detection correlated with power telemetry.

Cross-dependencies: findings in custody and key management may amplify smart-contract operational risks if administrative keys overlap with deployer roles. CleanSpark should enforce role separation between mining treasury keys, token admin keys (if any), and routine payroll or vendor payment keys. Table 121 in the evidence index references representative samples reviewed for this subsection.

WP 13.2 — International logistics & tariffs

This subsection (13.2) addresses whitepaper narrative within the CleanSpark Extended Security & Audit Assessment dated 2026. The assessment covers Bitcoin mining operations, hosting relationships, treasury workflows, and CLSK on BNB Smart Chain as described in the system boundary statement. Procedures performed were limited to inquiry, observation, inspection of selected artifacts, and agreed-upon analytics where noted. No opinion on financial statements is expressed.

Management is responsible for design, implementation, and operating effectiveness of controls. Assessors relied on representations regarding scope completeness and should be engaged to re-perform or expand testing when architecture, custodians, contracts, or token logic materially change. Residual risk may remain even when controls appear suitably designed; compensating controls must be explicitly documented.

Key considerations for international logistics & tariffs include segregation of duties, least-privilege access, audit logging with tamper-evident retention, encryption in transit and at rest for sensitive payloads, and periodic independent validation of backups and recovery paths. For mining infrastructure, assessors evaluated logical access to management interfaces, change tickets for firmware or pool configuration, and alignment with vendor hardening baselines.

Observations are classified per the severity model in Section 23. Informational items improve maturity; medium and above require tracked remediation with target completion dates and evidence packs. CleanSpark should maintain a continuous monitoring calendar covering certificate expiry, access recertification, dependency advisories, and hashrate anomaly detection correlated with power telemetry.

Cross-dependencies: findings in custody and key management may amplify smart-contract operational risks if administrative keys overlap with deployer roles. CleanSpark should enforce role separation between mining treasury keys, token admin keys (if any), and routine payroll or vendor payment keys. Table 122 in the evidence index references representative samples reviewed for this subsection.

WP 13.3 — International logistics & tariffs

This subsection (13.3) addresses whitepaper narrative within the CleanSpark Extended Security & Audit Assessment dated 2026. The assessment covers Bitcoin mining operations, hosting relationships, treasury workflows, and CLSK on BNB Smart Chain as described in the

system boundary statement. Procedures performed were limited to inquiry, observation, inspection of selected artifacts, and agreed-upon analytics where noted. No opinion on financial statements is expressed.

Management is responsible for design, implementation, and operating effectiveness of controls. Assessors relied on representations regarding scope completeness and should be engaged to re-perform or expand testing when architecture, custodians, contracts, or token logic materially change. Residual risk may remain even when controls appear suitably designed; compensating controls must be explicitly documented.

Key considerations for international logistics & tariffs include segregation of duties, least-privilege access, audit logging with tamper-evident retention, encryption in transit and at rest for sensitive payloads, and periodic independent validation of backups and recovery paths. For mining infrastructure, assessors evaluated logical access to management interfaces, change tickets for firmware or pool configuration, and alignment with vendor hardening baselines.

Observations are classified per the severity model in Section 23. Informational items improve maturity; medium and above require tracked remediation with target completion dates and evidence packs. CleanSpark should maintain a continuous monitoring calendar covering certificate expiry, access recertification, dependency advisories, and hashrate anomaly detection correlated with power telemetry.

Cross-dependencies: findings in custody and key management may amplify smart-contract operational risks if administrative keys overlap with deployer roles. CleanSpark should enforce role separation between mining treasury keys, token admin keys (if any), and routine payroll or vendor payment keys. Table 123 in the evidence index references representative samples reviewed for this subsection.

WP 14.1 — Spare inventory & RMA workflows

This subsection (14.1) addresses whitepaper narrative within the CleanSpark Extended Security & Audit Assessment dated 2026. The assessment covers Bitcoin mining operations, hosting relationships, treasury workflows, and CLSK on BNB Smart Chain as described in the system boundary statement. Procedures performed were limited to inquiry, observation, inspection of selected artifacts, and agreed-upon analytics where noted. No opinion on financial statements is expressed.

Management is responsible for design, implementation, and operating effectiveness of controls. Assessors relied on representations regarding scope completeness and should be engaged to re-perform or expand testing when architecture, custodians, contracts, or token logic materially change. Residual risk may remain even when controls appear suitably designed; compensating controls must be explicitly documented.

Key considerations for spare inventory & rma workflows include segregation of duties, least-privilege access, audit logging with tamper-evident retention, encryption in transit and at rest for sensitive payloads, and periodic independent validation of backups and recovery paths. For mining infrastructure, assessors evaluated logical access to management interfaces, change tickets for firmware or pool configuration, and alignment with vendor hardening baselines.

Observations are classified per the severity model in Section 23. Informational items improve maturity; medium and above require tracked remediation with target completion dates and evidence packs. CleanSpark should maintain a continuous monitoring calendar covering certificate expiry, access recertification, dependency advisories, and hashrate anomaly detection correlated with power telemetry.

Cross-dependencies: findings in custody and key management may amplify smart-contract operational risks if administrative keys overlap with deployer roles. CleanSpark should enforce role separation between mining treasury keys, token admin keys (if any), and routine payroll or vendor payment keys. Table 131 in the evidence index references representative samples reviewed for this subsection.

WP 14.2 — Spare inventory & RMA workflows

This subsection (14.2) addresses whitepaper narrative within the CleanSpark Extended Security & Audit Assessment dated 2026. The assessment covers Bitcoin mining operations,

hosting relationships, treasury workflows, and CLSK on BNB Smart Chain as described in the system boundary statement. Procedures performed were limited to inquiry, observation, inspection of selected artifacts, and agreed-upon analytics where noted. No opinion on financial statements is expressed.

Management is responsible for design, implementation, and operating effectiveness of controls. Assessors relied on representations regarding scope completeness and should be engaged to re-perform or expand testing when architecture, custodians, contracts, or token logic materially change. Residual risk may remain even when controls appear suitably designed; compensating controls must be explicitly documented.

Key considerations for spare inventory & rma workflows include segregation of duties, least-privilege access, audit logging with tamper-evident retention, encryption in transit and at rest for sensitive payloads, and periodic independent validation of backups and recovery paths. For mining infrastructure, assessors evaluated logical access to management interfaces, change tickets for firmware or pool configuration, and alignment with vendor hardening baselines.

Observations are classified per the severity model in Section 23. Informational items improve maturity; medium and above require tracked remediation with target completion dates and evidence packs. CleanSpark should maintain a continuous monitoring calendar covering certificate expiry, access recertification, dependency advisories, and hashrate anomaly detection correlated with power telemetry.

Cross-dependencies: findings in custody and key management may amplify smart-contract operational risks if administrative keys overlap with deployer roles. CleanSpark should enforce role separation between mining treasury keys, token admin keys (if any), and routine payroll or vendor payment keys. Table 132 in the evidence index references representative samples reviewed for this subsection.

WP 14.3 — Spare inventory & RMA workflows

This subsection (14.3) addresses whitepaper narrative within the CleanSpark Extended Security & Audit Assessment dated 2026. The assessment covers Bitcoin mining operations, hosting relationships, treasury workflows, and CLSK on BNB Smart Chain as described in the system boundary statement. Procedures performed were limited to inquiry, observation, inspection of selected artifacts, and agreed-upon analytics where noted. No opinion on financial statements is expressed.

Management is responsible for design, implementation, and operating effectiveness of controls. Assessors relied on representations regarding scope completeness and should be engaged to re-perform or expand testing when architecture, custodians, contracts, or token logic materially change. Residual risk may remain even when controls appear suitably designed; compensating controls must be explicitly documented.

Key considerations for spare inventory & rma workflows include segregation of duties, least-privilege access, audit logging with tamper-evident retention, encryption in transit and at rest for sensitive payloads, and periodic independent validation of backups and recovery paths. For mining infrastructure, assessors evaluated logical access to management interfaces, change tickets for firmware or pool configuration, and alignment with vendor hardening baselines.

Observations are classified per the severity model in Section 23. Informational items improve maturity; medium and above require tracked remediation with target completion dates and evidence packs. CleanSpark should maintain a continuous monitoring calendar covering certificate expiry, access recertification, dependency advisories, and hashrate anomaly detection correlated with power telemetry.

Cross-dependencies: findings in custody and key management may amplify smart-contract operational risks if administrative keys overlap with deployer roles. CleanSpark should enforce role separation between mining treasury keys, token admin keys (if any), and routine payroll or vendor payment keys. Table 133 in the evidence index references representative samples reviewed for this subsection.

WP 15.1 — Firmware security & supply chain

This subsection (15.1) addresses whitepaper narrative within the CleanSpark Extended

Security & Audit Assessment dated 2026. The assessment covers Bitcoin mining operations, hosting relationships, treasury workflows, and CLSK on BNB Smart Chain as described in the system boundary statement. Procedures performed were limited to inquiry, observation, inspection of selected artifacts, and agreed-upon analytics where noted. No opinion on financial statements is expressed.

Management is responsible for design, implementation, and operating effectiveness of controls. Assessors relied on representations regarding scope completeness and should be engaged to re-perform or expand testing when architecture, custodians, contracts, or token logic materially change. Residual risk may remain even when controls appear suitably designed; compensating controls must be explicitly documented.

Key considerations for firmware security & supply chain include segregation of duties, least-privilege access, audit logging with tamper-evident retention, encryption in transit and at rest for sensitive payloads, and periodic independent validation of backups and recovery paths. For mining infrastructure, assessors evaluated logical access to management interfaces, change tickets for firmware or pool configuration, and alignment with vendor hardening baselines.

Observations are classified per the severity model in Section 23. Informational items improve maturity; medium and above require tracked remediation with target completion dates and evidence packs. CleanSpark should maintain a continuous monitoring calendar covering certificate expiry, access recertification, dependency advisories, and hashrate anomaly detection correlated with power telemetry.

Cross-dependencies: findings in custody and key management may amplify smart-contract operational risks if administrative keys overlap with deployer roles. CleanSpark should enforce role separation between mining treasury keys, token admin keys (if any), and routine payroll or vendor payment keys. Table 141 in the evidence index references representative samples reviewed for this subsection.

WP 15.2 — Firmware security & supply chain

This subsection (15.2) addresses whitepaper narrative within the CleanSpark Extended Security & Audit Assessment dated 2026. The assessment covers Bitcoin mining operations, hosting relationships, treasury workflows, and CLSK on BNB Smart Chain as described in the system boundary statement. Procedures performed were limited to inquiry, observation, inspection of selected artifacts, and agreed-upon analytics where noted. No opinion on financial statements is expressed.

Management is responsible for design, implementation, and operating effectiveness of controls. Assessors relied on representations regarding scope completeness and should be engaged to re-perform or expand testing when architecture, custodians, contracts, or token logic materially change. Residual risk may remain even when controls appear suitably designed; compensating controls must be explicitly documented.

Key considerations for firmware security & supply chain include segregation of duties, least-privilege access, audit logging with tamper-evident retention, encryption in transit and at rest for sensitive payloads, and periodic independent validation of backups and recovery paths. For mining infrastructure, assessors evaluated logical access to management interfaces, change tickets for firmware or pool configuration, and alignment with vendor hardening baselines.

Observations are classified per the severity model in Section 23. Informational items improve maturity; medium and above require tracked remediation with target completion dates and evidence packs. CleanSpark should maintain a continuous monitoring calendar covering certificate expiry, access recertification, dependency advisories, and hashrate anomaly detection correlated with power telemetry.

Cross-dependencies: findings in custody and key management may amplify smart-contract operational risks if administrative keys overlap with deployer roles. CleanSpark should enforce role separation between mining treasury keys, token admin keys (if any), and routine payroll or vendor payment keys. Table 142 in the evidence index references representative samples reviewed for this subsection.

WP 15.3 — Firmware security & supply chain

This subsection (15.3) addresses whitepaper narrative within the CleanSpark Extended Security & Audit Assessment dated 2026. The assessment covers Bitcoin mining operations, hosting relationships, treasury workflows, and CLSK on BNB Smart Chain as described in the system boundary statement. Procedures performed were limited to inquiry, observation, inspection of selected artifacts, and agreed-upon analytics where noted. No opinion on financial statements is expressed.

Management is responsible for design, implementation, and operating effectiveness of controls. Assessors relied on representations regarding scope completeness and should be engaged to re-perform or expand testing when architecture, custodians, contracts, or token logic materially change. Residual risk may remain even when controls appear suitably designed; compensating controls must be explicitly documented.

Key considerations for firmware security & supply chain include segregation of duties, least-privilege access, audit logging with tamper-evident retention, encryption in transit and at rest for sensitive payloads, and periodic independent validation of backups and recovery paths. For mining infrastructure, assessors evaluated logical access to management interfaces, change tickets for firmware or pool configuration, and alignment with vendor hardening baselines.

Observations are classified per the severity model in Section 23. Informational items improve maturity; medium and above require tracked remediation with target completion dates and evidence packs. CleanSpark should maintain a continuous monitoring calendar covering certificate expiry, access recertification, dependency advisories, and hashrate anomaly detection correlated with power telemetry.

Cross-dependencies: findings in custody and key management may amplify smart-contract operational risks if administrative keys overlap with deployer roles. CleanSpark should enforce role separation between mining treasury keys, token admin keys (if any), and routine payroll or vendor payment keys. Table 143 in the evidence index references representative samples reviewed for this subsection.

WP 16.1 — Monitoring stacks & time-series telemetry

This subsection (16.1) addresses whitepaper narrative within the CleanSpark Extended Security & Audit Assessment dated 2026. The assessment covers Bitcoin mining operations, hosting relationships, treasury workflows, and CLSK on BNB Smart Chain as described in the system boundary statement. Procedures performed were limited to inquiry, observation, inspection of selected artifacts, and agreed-upon analytics where noted. No opinion on financial statements is expressed.

Management is responsible for design, implementation, and operating effectiveness of controls. Assessors relied on representations regarding scope completeness and should be engaged to re-perform or expand testing when architecture, custodians, contracts, or token logic materially change. Residual risk may remain even when controls appear suitably designed; compensating controls must be explicitly documented.

Key considerations for monitoring stacks & time-series telemetry include segregation of duties, least-privilege access, audit logging with tamper-evident retention, encryption in transit and at rest for sensitive payloads, and periodic independent validation of backups and recovery paths. For mining infrastructure, assessors evaluated logical access to management interfaces, change tickets for firmware or pool configuration, and alignment with vendor hardening baselines.

Observations are classified per the severity model in Section 23. Informational items improve maturity; medium and above require tracked remediation with target completion dates and evidence packs. CleanSpark should maintain a continuous monitoring calendar covering certificate expiry, access recertification, dependency advisories, and hashrate anomaly detection correlated with power telemetry.

Cross-dependencies: findings in custody and key management may amplify smart-contract operational risks if administrative keys overlap with deployer roles. CleanSpark should enforce role separation between mining treasury keys, token admin keys (if any), and routine payroll or vendor payment keys. Table 151 in the evidence index references representative samples reviewed for this subsection.

WP 16.2 — Monitoring stacks & time-series telemetry

This subsection (16.2) addresses whitepaper narrative within the CleanSpark Extended Security & Audit Assessment dated 2026. The assessment covers Bitcoin mining operations, hosting relationships, treasury workflows, and CLSK on BNB Smart Chain as described in the system boundary statement. Procedures performed were limited to inquiry, observation, inspection of selected artifacts, and agreed-upon analytics where noted. No opinion on financial statements is expressed.

Management is responsible for design, implementation, and operating effectiveness of controls. Assessors relied on representations regarding scope completeness and should be engaged to re-perform or expand testing when architecture, custodians, contracts, or token logic materially change. Residual risk may remain even when controls appear suitably designed; compensating controls must be explicitly documented.

Key considerations for monitoring stacks & time-series telemetry include segregation of duties, least-privilege access, audit logging with tamper-evident retention, encryption in transit and at rest for sensitive payloads, and periodic independent validation of backups and recovery paths. For mining infrastructure, assessors evaluated logical access to management interfaces, change tickets for firmware or pool configuration, and alignment with vendor hardening baselines.

Observations are classified per the severity model in Section 23. Informational items improve maturity; medium and above require tracked remediation with target completion dates and evidence packs. CleanSpark should maintain a continuous monitoring calendar covering certificate expiry, access recertification, dependency advisories, and hashrate anomaly detection correlated with power telemetry.

Cross-dependencies: findings in custody and key management may amplify smart-contract operational risks if administrative keys overlap with deployer roles. CleanSpark should enforce role separation between mining treasury keys, token admin keys (if any), and routine payroll or vendor payment keys. Table 152 in the evidence index references representative samples reviewed for this subsection.

WP 16.3 — Monitoring stacks & time-series telemetry

This subsection (16.3) addresses whitepaper narrative within the CleanSpark Extended Security & Audit Assessment dated 2026. The assessment covers Bitcoin mining operations, hosting relationships, treasury workflows, and CLSK on BNB Smart Chain as described in the system boundary statement. Procedures performed were limited to inquiry, observation, inspection of selected artifacts, and agreed-upon analytics where noted. No opinion on financial statements is expressed.

Management is responsible for design, implementation, and operating effectiveness of controls. Assessors relied on representations regarding scope completeness and should be engaged to re-perform or expand testing when architecture, custodians, contracts, or token logic materially change. Residual risk may remain even when controls appear suitably designed; compensating controls must be explicitly documented.

Key considerations for monitoring stacks & time-series telemetry include segregation of duties, least-privilege access, audit logging with tamper-evident retention, encryption in transit and at rest for sensitive payloads, and periodic independent validation of backups and recovery paths. For mining infrastructure, assessors evaluated logical access to management interfaces, change tickets for firmware or pool configuration, and alignment with vendor hardening baselines.

Observations are classified per the severity model in Section 23. Informational items improve maturity; medium and above require tracked remediation with target completion dates and evidence packs. CleanSpark should maintain a continuous monitoring calendar covering certificate expiry, access recertification, dependency advisories, and hashrate anomaly detection correlated with power telemetry.

Cross-dependencies: findings in custody and key management may amplify smart-contract operational risks if administrative keys overlap with deployer roles. CleanSpark should enforce role separation between mining treasury keys, token admin keys (if any), and routine payroll or vendor payment keys. Table 153 in the evidence index references representative samples reviewed for this subsection.

WP 17.1 — Incident command & communications

This subsection (17.1) addresses whitepaper narrative within the CleanSpark Extended Security & Audit Assessment dated 2026. The assessment covers Bitcoin mining operations, hosting relationships, treasury workflows, and CLSK on BNB Smart Chain as described in the system boundary statement. Procedures performed were limited to inquiry, observation, inspection of selected artifacts, and agreed-upon analytics where noted. No opinion on financial statements is expressed.

Management is responsible for design, implementation, and operating effectiveness of controls. Assessors relied on representations regarding scope completeness and should be engaged to re-perform or expand testing when architecture, custodians, contracts, or token logic materially change. Residual risk may remain even when controls appear suitably designed; compensating controls must be explicitly documented.

Key considerations for incident command & communications include segregation of duties, least-privilege access, audit logging with tamper-evident retention, encryption in transit and at rest for sensitive payloads, and periodic independent validation of backups and recovery paths. For mining infrastructure, assessors evaluated logical access to management interfaces, change tickets for firmware or pool configuration, and alignment with vendor hardening baselines.

Observations are classified per the severity model in Section 23. Informational items improve maturity; medium and above require tracked remediation with target completion dates and evidence packs. CleanSpark should maintain a continuous monitoring calendar covering certificate expiry, access recertification, dependency advisories, and hashrate anomaly detection correlated with power telemetry.

Cross-dependencies: findings in custody and key management may amplify smart-contract operational risks if administrative keys overlap with deployer roles. CleanSpark should enforce role separation between mining treasury keys, token admin keys (if any), and routine payroll or vendor payment keys. Table 161 in the evidence index references representative samples reviewed for this subsection.

WP 17.2 — Incident command & communications

This subsection (17.2) addresses whitepaper narrative within the CleanSpark Extended Security & Audit Assessment dated 2026. The assessment covers Bitcoin mining operations, hosting relationships, treasury workflows, and CLSK on BNB Smart Chain as described in the system boundary statement. Procedures performed were limited to inquiry, observation, inspection of selected artifacts, and agreed-upon analytics where noted. No opinion on financial statements is expressed.

Management is responsible for design, implementation, and operating effectiveness of controls. Assessors relied on representations regarding scope completeness and should be engaged to re-perform or expand testing when architecture, custodians, contracts, or token logic materially change. Residual risk may remain even when controls appear suitably designed; compensating controls must be explicitly documented.

Key considerations for incident command & communications include segregation of duties, least-privilege access, audit logging with tamper-evident retention, encryption in transit and at rest for sensitive payloads, and periodic independent validation of backups and recovery paths. For mining infrastructure, assessors evaluated logical access to management interfaces, change tickets for firmware or pool configuration, and alignment with vendor hardening baselines.

Observations are classified per the severity model in Section 23. Informational items improve maturity; medium and above require tracked remediation with target completion dates and evidence packs. CleanSpark should maintain a continuous monitoring calendar covering certificate expiry, access recertification, dependency advisories, and hashrate anomaly detection correlated with power telemetry.

Cross-dependencies: findings in custody and key management may amplify smart-contract operational risks if administrative keys overlap with deployer roles. CleanSpark should enforce role separation between mining treasury keys, token admin keys (if any), and routine payroll or vendor payment keys. Table 162 in the evidence index references representative samples reviewed for this subsection.

WP 17.3 — Incident command & communications

This subsection (17.3) addresses whitepaper narrative within the CleanSpark Extended Security & Audit Assessment dated 2026. The assessment covers Bitcoin mining operations, hosting relationships, treasury workflows, and CLSK on BNB Smart Chain as described in the system boundary statement. Procedures performed were limited to inquiry, observation, inspection of selected artifacts, and agreed-upon analytics where noted. No opinion on financial statements is expressed.

Management is responsible for design, implementation, and operating effectiveness of controls. Assessors relied on representations regarding scope completeness and should be engaged to re-perform or expand testing when architecture, custodians, contracts, or token logic materially change. Residual risk may remain even when controls appear suitably designed; compensating controls must be explicitly documented.

Key considerations for incident command & communications include segregation of duties, least-privilege access, audit logging with tamper-evident retention, encryption in transit and at rest for sensitive payloads, and periodic independent validation of backups and recovery paths. For mining infrastructure, assessors evaluated logical access to management interfaces, change tickets for firmware or pool configuration, and alignment with vendor hardening baselines.

Observations are classified per the severity model in Section 23. Informational items improve maturity; medium and above require tracked remediation with target completion dates and evidence packs. CleanSpark should maintain a continuous monitoring calendar covering certificate expiry, access recertification, dependency advisories, and hashrate anomaly detection correlated with power telemetry.

Cross-dependencies: findings in custody and key management may amplify smart-contract operational risks if administrative keys overlap with deployer roles. CleanSpark should enforce role separation between mining treasury keys, token admin keys (if any), and routine payroll or vendor payment keys. Table 163 in the evidence index references representative samples reviewed for this subsection.

WP 18.1 — Insurance & business continuity

This subsection (18.1) addresses whitepaper narrative within the CleanSpark Extended Security & Audit Assessment dated 2026. The assessment covers Bitcoin mining operations, hosting relationships, treasury workflows, and CLSK on BNB Smart Chain as described in the system boundary statement. Procedures performed were limited to inquiry, observation, inspection of selected artifacts, and agreed-upon analytics where noted. No opinion on financial statements is expressed.

Management is responsible for design, implementation, and operating effectiveness of controls. Assessors relied on representations regarding scope completeness and should be engaged to re-perform or expand testing when architecture, custodians, contracts, or token logic materially change. Residual risk may remain even when controls appear suitably designed; compensating controls must be explicitly documented.

Key considerations for insurance & business continuity include segregation of duties, least-privilege access, audit logging with tamper-evident retention, encryption in transit and at rest for sensitive payloads, and periodic independent validation of backups and recovery paths. For mining infrastructure, assessors evaluated logical access to management interfaces, change tickets for firmware or pool configuration, and alignment with vendor hardening baselines.

Observations are classified per the severity model in Section 23. Informational items improve maturity; medium and above require tracked remediation with target completion dates and evidence packs. CleanSpark should maintain a continuous monitoring calendar covering certificate expiry, access recertification, dependency advisories, and hashrate anomaly detection correlated with power telemetry.

Cross-dependencies: findings in custody and key management may amplify smart-contract operational risks if administrative keys overlap with deployer roles. CleanSpark should enforce role separation between mining treasury keys, token admin keys (if any), and routine payroll or vendor payment keys. Table 171 in the evidence index references representative samples reviewed for this subsection.

WP 18.2 — Insurance & business continuity

This subsection (18.2) addresses whitepaper narrative within the CleanSpark Extended Security & Audit Assessment dated 2026. The assessment covers Bitcoin mining operations, hosting relationships, treasury workflows, and CLSK on BNB Smart Chain as described in the system boundary statement. Procedures performed were limited to inquiry, observation, inspection of selected artifacts, and agreed-upon analytics where noted. No opinion on financial statements is expressed.

Management is responsible for design, implementation, and operating effectiveness of controls. Assessors relied on representations regarding scope completeness and should be engaged to re-perform or expand testing when architecture, custodians, contracts, or token logic materially change. Residual risk may remain even when controls appear suitably designed; compensating controls must be explicitly documented.

Key considerations for insurance & business continuity include segregation of duties, least-privilege access, audit logging with tamper-evident retention, encryption in transit and at rest for sensitive payloads, and periodic independent validation of backups and recovery paths. For mining infrastructure, assessors evaluated logical access to management interfaces, change tickets for firmware or pool configuration, and alignment with vendor hardening baselines.

Observations are classified per the severity model in Section 23. Informational items improve maturity; medium and above require tracked remediation with target completion dates and evidence packs. CleanSpark should maintain a continuous monitoring calendar covering certificate expiry, access recertification, dependency advisories, and hashrate anomaly detection correlated with power telemetry.

Cross-dependencies: findings in custody and key management may amplify smart-contract operational risks if administrative keys overlap with deployer roles. CleanSpark should enforce role separation between mining treasury keys, token admin keys (if any), and routine payroll or vendor payment keys. Table 172 in the evidence index references representative samples reviewed for this subsection.

WP 18.3 — Insurance & business continuity

This subsection (18.3) addresses whitepaper narrative within the CleanSpark Extended Security & Audit Assessment dated 2026. The assessment covers Bitcoin mining operations, hosting relationships, treasury workflows, and CLSK on BNB Smart Chain as described in the system boundary statement. Procedures performed were limited to inquiry, observation, inspection of selected artifacts, and agreed-upon analytics where noted. No opinion on financial statements is expressed.

Management is responsible for design, implementation, and operating effectiveness of controls. Assessors relied on representations regarding scope completeness and should be engaged to re-perform or expand testing when architecture, custodians, contracts, or token logic materially change. Residual risk may remain even when controls appear suitably designed; compensating controls must be explicitly documented.

Key considerations for insurance & business continuity include segregation of duties, least-privilege access, audit logging with tamper-evident retention, encryption in transit and at rest for sensitive payloads, and periodic independent validation of backups and recovery paths. For mining infrastructure, assessors evaluated logical access to management interfaces, change tickets for firmware or pool configuration, and alignment with vendor hardening baselines.

Observations are classified per the severity model in Section 23. Informational items improve maturity; medium and above require tracked remediation with target completion dates and evidence packs. CleanSpark should maintain a continuous monitoring calendar covering certificate expiry, access recertification, dependency advisories, and hashrate anomaly detection correlated with power telemetry.

Cross-dependencies: findings in custody and key management may amplify smart-contract operational risks if administrative keys overlap with deployer roles. CleanSpark should enforce role separation between mining treasury keys, token admin keys (if any), and routine payroll or vendor payment keys. Table 173 in the evidence index references representative samples reviewed for this subsection.

WP 19.1 — Tax & transfer pricing overview

This subsection (19.1) addresses whitepaper narrative within the CleanSpark Extended Security & Audit Assessment dated 2026. The assessment covers Bitcoin mining operations, hosting relationships, treasury workflows, and CLSK on BNB Smart Chain as described in the system boundary statement. Procedures performed were limited to inquiry, observation, inspection of selected artifacts, and agreed-upon analytics where noted. No opinion on financial statements is expressed.

Management is responsible for design, implementation, and operating effectiveness of controls. Assessors relied on representations regarding scope completeness and should be engaged to re-perform or expand testing when architecture, custodians, contracts, or token logic materially change. Residual risk may remain even when controls appear suitably designed; compensating controls must be explicitly documented.

Key considerations for tax & transfer pricing overview include segregation of duties, least-privilege access, audit logging with tamper-evident retention, encryption in transit and at rest for sensitive payloads, and periodic independent validation of backups and recovery paths. For mining infrastructure, assessors evaluated logical access to management interfaces, change tickets for firmware or pool configuration, and alignment with vendor hardening baselines.

Observations are classified per the severity model in Section 23. Informational items improve maturity; medium and above require tracked remediation with target completion dates and evidence packs. CleanSpark should maintain a continuous monitoring calendar covering certificate expiry, access recertification, dependency advisories, and hashrate anomaly detection correlated with power telemetry.

Cross-dependencies: findings in custody and key management may amplify smart-contract operational risks if administrative keys overlap with deployer roles. CleanSpark should enforce role separation between mining treasury keys, token admin keys (if any), and routine payroll or vendor payment keys. Table 181 in the evidence index references representative samples reviewed for this subsection.

WP 19.2 — Tax & transfer pricing overview

This subsection (19.2) addresses whitepaper narrative within the CleanSpark Extended Security & Audit Assessment dated 2026. The assessment covers Bitcoin mining operations, hosting relationships, treasury workflows, and CLSK on BNB Smart Chain as described in the system boundary statement. Procedures performed were limited to inquiry, observation, inspection of selected artifacts, and agreed-upon analytics where noted. No opinion on financial statements is expressed.

Management is responsible for design, implementation, and operating effectiveness of controls. Assessors relied on representations regarding scope completeness and should be engaged to re-perform or expand testing when architecture, custodians, contracts, or token logic materially change. Residual risk may remain even when controls appear suitably designed; compensating controls must be explicitly documented.

Key considerations for tax & transfer pricing overview include segregation of duties, least-privilege access, audit logging with tamper-evident retention, encryption in transit and at rest for sensitive payloads, and periodic independent validation of backups and recovery paths. For mining infrastructure, assessors evaluated logical access to management interfaces, change tickets for firmware or pool configuration, and alignment with vendor hardening baselines.

Observations are classified per the severity model in Section 23. Informational items improve maturity; medium and above require tracked remediation with target completion dates and evidence packs. CleanSpark should maintain a continuous monitoring calendar covering certificate expiry, access recertification, dependency advisories, and hashrate anomaly detection correlated with power telemetry.

Cross-dependencies: findings in custody and key management may amplify smart-contract operational risks if administrative keys overlap with deployer roles. CleanSpark should enforce role separation between mining treasury keys, token admin keys (if any), and routine payroll or vendor payment keys. Table 182 in the evidence index references representative samples reviewed for this subsection.

WP 19.3 — Tax & transfer pricing overview

This subsection (19.3) addresses whitepaper narrative within the CleanSpark Extended Security & Audit Assessment dated 2026. The assessment covers Bitcoin mining operations, hosting relationships, treasury workflows, and CLSK on BNB Smart Chain as described in the system boundary statement. Procedures performed were limited to inquiry, observation, inspection of selected artifacts, and agreed-upon analytics where noted. No opinion on financial statements is expressed.

Management is responsible for design, implementation, and operating effectiveness of controls. Assessors relied on representations regarding scope completeness and should be engaged to re-perform or expand testing when architecture, custodians, contracts, or token logic materially change. Residual risk may remain even when controls appear suitably designed; compensating controls must be explicitly documented.

Key considerations for tax & transfer pricing overview include segregation of duties, least-privilege access, audit logging with tamper-evident retention, encryption in transit and at rest for sensitive payloads, and periodic independent validation of backups and recovery paths. For mining infrastructure, assessors evaluated logical access to management interfaces, change tickets for firmware or pool configuration, and alignment with vendor hardening baselines.

Observations are classified per the severity model in Section 23. Informational items improve maturity; medium and above require tracked remediation with target completion dates and evidence packs. CleanSpark should maintain a continuous monitoring calendar covering certificate expiry, access recertification, dependency advisories, and hashrate anomaly detection correlated with power telemetry.

Cross-dependencies: findings in custody and key management may amplify smart-contract operational risks if administrative keys overlap with deployer roles. CleanSpark should enforce role separation between mining treasury keys, token admin keys (if any), and routine payroll or vendor payment keys. Table 183 in the evidence index references representative samples reviewed for this subsection.

WP 20.1 — Sanctions & counterparty screening

This subsection (20.1) addresses whitepaper narrative within the CleanSpark Extended Security & Audit Assessment dated 2026. The assessment covers Bitcoin mining operations, hosting relationships, treasury workflows, and CLSK on BNB Smart Chain as described in the system boundary statement. Procedures performed were limited to inquiry, observation, inspection of selected artifacts, and agreed-upon analytics where noted. No opinion on financial statements is expressed.

Management is responsible for design, implementation, and operating effectiveness of controls. Assessors relied on representations regarding scope completeness and should be engaged to re-perform or expand testing when architecture, custodians, contracts, or token logic materially change. Residual risk may remain even when controls appear suitably designed; compensating controls must be explicitly documented.

Key considerations for sanctions & counterparty screening include segregation of duties, least-privilege access, audit logging with tamper-evident retention, encryption in transit and at rest for sensitive payloads, and periodic independent validation of backups and recovery paths. For mining infrastructure, assessors evaluated logical access to management interfaces, change tickets for firmware or pool configuration, and alignment with vendor hardening baselines.

Observations are classified per the severity model in Section 23. Informational items improve maturity; medium and above require tracked remediation with target completion dates and evidence packs. CleanSpark should maintain a continuous monitoring calendar covering certificate expiry, access recertification, dependency advisories, and hashrate anomaly detection correlated with power telemetry.

Cross-dependencies: findings in custody and key management may amplify smart-contract operational risks if administrative keys overlap with deployer roles. CleanSpark should enforce role separation between mining treasury keys, token admin keys (if any), and routine payroll or vendor payment keys. Table 191 in the evidence index references representative samples reviewed for this subsection.

WP 20.2 — Sanctions & counterparty screening

This subsection (20.2) addresses whitepaper narrative within the CleanSpark Extended Security & Audit Assessment dated 2026. The assessment covers Bitcoin mining operations, hosting relationships, treasury workflows, and CLSK on BNB Smart Chain as described in the system boundary statement. Procedures performed were limited to inquiry, observation, inspection of selected artifacts, and agreed-upon analytics where noted. No opinion on financial statements is expressed.

Management is responsible for design, implementation, and operating effectiveness of controls. Assessors relied on representations regarding scope completeness and should be engaged to re-perform or expand testing when architecture, custodians, contracts, or token logic materially change. Residual risk may remain even when controls appear suitably designed; compensating controls must be explicitly documented.

Key considerations for sanctions & counterparty screening include segregation of duties, least-privilege access, audit logging with tamper-evident retention, encryption in transit and at rest for sensitive payloads, and periodic independent validation of backups and recovery paths. For mining infrastructure, assessors evaluated logical access to management interfaces, change tickets for firmware or pool configuration, and alignment with vendor hardening baselines.

Observations are classified per the severity model in Section 23. Informational items improve maturity; medium and above require tracked remediation with target completion dates and evidence packs. CleanSpark should maintain a continuous monitoring calendar covering certificate expiry, access recertification, dependency advisories, and hashrate anomaly detection correlated with power telemetry.

Cross-dependencies: findings in custody and key management may amplify smart-contract operational risks if administrative keys overlap with deployer roles. CleanSpark should enforce role separation between mining treasury keys, token admin keys (if any), and routine payroll or vendor payment keys. Table 192 in the evidence index references representative samples reviewed for this subsection.

WP 20.3 — Sanctions & counterparty screening

This subsection (20.3) addresses whitepaper narrative within the CleanSpark Extended Security & Audit Assessment dated 2026. The assessment covers Bitcoin mining operations, hosting relationships, treasury workflows, and CLSK on BNB Smart Chain as described in the system boundary statement. Procedures performed were limited to inquiry, observation, inspection of selected artifacts, and agreed-upon analytics where noted. No opinion on financial statements is expressed.

Management is responsible for design, implementation, and operating effectiveness of controls. Assessors relied on representations regarding scope completeness and should be engaged to re-perform or expand testing when architecture, custodians, contracts, or token logic materially change. Residual risk may remain even when controls appear suitably designed; compensating controls must be explicitly documented.

Key considerations for sanctions & counterparty screening include segregation of duties, least-privilege access, audit logging with tamper-evident retention, encryption in transit and at rest for sensitive payloads, and periodic independent validation of backups and recovery paths. For mining infrastructure, assessors evaluated logical access to management interfaces, change tickets for firmware or pool configuration, and alignment with vendor hardening baselines.

Observations are classified per the severity model in Section 23. Informational items improve maturity; medium and above require tracked remediation with target completion dates and evidence packs. CleanSpark should maintain a continuous monitoring calendar covering certificate expiry, access recertification, dependency advisories, and hashrate anomaly detection correlated with power telemetry.

Cross-dependencies: findings in custody and key management may amplify smart-contract operational risks if administrative keys overlap with deployer roles. CleanSpark should enforce role separation between mining treasury keys, token admin keys (if any), and routine payroll or vendor payment keys. Table 193 in the evidence index references representative samples reviewed for this subsection.

WP 21.1 — Token liquidity programs & DEX venues

This subsection (21.1) addresses whitepaper narrative within the CleanSpark Extended Security & Audit Assessment dated 2026. The assessment covers Bitcoin mining operations, hosting relationships, treasury workflows, and CLSK on BNB Smart Chain as described in the system boundary statement. Procedures performed were limited to inquiry, observation, inspection of selected artifacts, and agreed-upon analytics where noted. No opinion on financial statements is expressed.

Management is responsible for design, implementation, and operating effectiveness of controls. Assessors relied on representations regarding scope completeness and should be engaged to re-perform or expand testing when architecture, custodians, contracts, or token logic materially change. Residual risk may remain even when controls appear suitably designed; compensating controls must be explicitly documented.

Key considerations for token liquidity programs & dex venues include segregation of duties, least-privilege access, audit logging with tamper-evident retention, encryption in transit and at rest for sensitive payloads, and periodic independent validation of backups and recovery paths. For mining infrastructure, assessors evaluated logical access to management interfaces, change tickets for firmware or pool configuration, and alignment with vendor hardening baselines.

Observations are classified per the severity model in Section 23. Informational items improve maturity; medium and above require tracked remediation with target completion dates and evidence packs. CleanSpark should maintain a continuous monitoring calendar covering certificate expiry, access recertification, dependency advisories, and hashrate anomaly detection correlated with power telemetry.

Cross-dependencies: findings in custody and key management may amplify smart-contract operational risks if administrative keys overlap with deployer roles. CleanSpark should enforce role separation between mining treasury keys, token admin keys (if any), and routine payroll or vendor payment keys. Table 201 in the evidence index references representative samples reviewed for this subsection.

WP 21.2 — Token liquidity programs & DEX venues

This subsection (21.2) addresses whitepaper narrative within the CleanSpark Extended Security & Audit Assessment dated 2026. The assessment covers Bitcoin mining operations, hosting relationships, treasury workflows, and CLSK on BNB Smart Chain as described in the system boundary statement. Procedures performed were limited to inquiry, observation, inspection of selected artifacts, and agreed-upon analytics where noted. No opinion on financial statements is expressed.

Management is responsible for design, implementation, and operating effectiveness of controls. Assessors relied on representations regarding scope completeness and should be engaged to re-perform or expand testing when architecture, custodians, contracts, or token logic materially change. Residual risk may remain even when controls appear suitably designed; compensating controls must be explicitly documented.

Key considerations for token liquidity programs & dex venues include segregation of duties, least-privilege access, audit logging with tamper-evident retention, encryption in transit and at rest for sensitive payloads, and periodic independent validation of backups and recovery paths. For mining infrastructure, assessors evaluated logical access to management interfaces, change tickets for firmware or pool configuration, and alignment with vendor hardening baselines.

Observations are classified per the severity model in Section 23. Informational items improve maturity; medium and above require tracked remediation with target completion dates and evidence packs. CleanSpark should maintain a continuous monitoring calendar covering certificate expiry, access recertification, dependency advisories, and hashrate anomaly detection correlated with power telemetry.

Cross-dependencies: findings in custody and key management may amplify smart-contract operational risks if administrative keys overlap with deployer roles. CleanSpark should enforce role separation between mining treasury keys, token admin keys (if any), and routine payroll or vendor payment keys. Table 202 in the evidence index references representative samples reviewed for this subsection.

WP 21.3 — Token liquidity programs & DEX venues

This subsection (21.3) addresses whitepaper narrative within the CleanSpark Extended Security & Audit Assessment dated 2026. The assessment covers Bitcoin mining operations, hosting relationships, treasury workflows, and CLSK on BNB Smart Chain as described in the system boundary statement. Procedures performed were limited to inquiry, observation, inspection of selected artifacts, and agreed-upon analytics where noted. No opinion on financial statements is expressed.

Management is responsible for design, implementation, and operating effectiveness of controls. Assessors relied on representations regarding scope completeness and should be engaged to re-perform or expand testing when architecture, custodians, contracts, or token logic materially change. Residual risk may remain even when controls appear suitably designed; compensating controls must be explicitly documented.

Key considerations for token liquidity programs & dex venues include segregation of duties, least-privilege access, audit logging with tamper-evident retention, encryption in transit and at rest for sensitive payloads, and periodic independent validation of backups and recovery paths. For mining infrastructure, assessors evaluated logical access to management interfaces, change tickets for firmware or pool configuration, and alignment with vendor hardening baselines.

Observations are classified per the severity model in Section 23. Informational items improve maturity; medium and above require tracked remediation with target completion dates and evidence packs. CleanSpark should maintain a continuous monitoring calendar covering certificate expiry, access recertification, dependency advisories, and hashrate anomaly detection correlated with power telemetry.

Cross-dependencies: findings in custody and key management may amplify smart-contract operational risks if administrative keys overlap with deployer roles. CleanSpark should enforce role separation between mining treasury keys, token admin keys (if any), and routine payroll or vendor payment keys. Table 203 in the evidence index references representative samples reviewed for this subsection.

WP 22.1 — Bridge risk & wrapped asset caveats

This subsection (22.1) addresses whitepaper narrative within the CleanSpark Extended Security & Audit Assessment dated 2026. The assessment covers Bitcoin mining operations, hosting relationships, treasury workflows, and CLSK on BNB Smart Chain as described in the system boundary statement. Procedures performed were limited to inquiry, observation, inspection of selected artifacts, and agreed-upon analytics where noted. No opinion on financial statements is expressed.

Management is responsible for design, implementation, and operating effectiveness of controls. Assessors relied on representations regarding scope completeness and should be engaged to re-perform or expand testing when architecture, custodians, contracts, or token logic materially change. Residual risk may remain even when controls appear suitably designed; compensating controls must be explicitly documented.

Key considerations for bridge risk & wrapped asset caveats include segregation of duties, least-privilege access, audit logging with tamper-evident retention, encryption in transit and at rest for sensitive payloads, and periodic independent validation of backups and recovery paths. For mining infrastructure, assessors evaluated logical access to management interfaces, change tickets for firmware or pool configuration, and alignment with vendor hardening baselines.

Observations are classified per the severity model in Section 23. Informational items improve maturity; medium and above require tracked remediation with target completion dates and evidence packs. CleanSpark should maintain a continuous monitoring calendar covering certificate expiry, access recertification, dependency advisories, and hashrate anomaly detection correlated with power telemetry.

Cross-dependencies: findings in custody and key management may amplify smart-contract operational risks if administrative keys overlap with deployer roles. CleanSpark should enforce role separation between mining treasury keys, token admin keys (if any), and routine payroll or vendor payment keys. Table 211 in the evidence index references representative samples reviewed for this subsection.

WP 22.2 — Bridge risk & wrapped asset caveats

This subsection (22.2) addresses whitepaper narrative within the CleanSpark Extended Security & Audit Assessment dated 2026. The assessment covers Bitcoin mining operations, hosting relationships, treasury workflows, and CLSK on BNB Smart Chain as described in the system boundary statement. Procedures performed were limited to inquiry, observation, inspection of selected artifacts, and agreed-upon analytics where noted. No opinion on financial statements is expressed.

Management is responsible for design, implementation, and operating effectiveness of controls. Assessors relied on representations regarding scope completeness and should be engaged to re-perform or expand testing when architecture, custodians, contracts, or token logic materially change. Residual risk may remain even when controls appear suitably designed; compensating controls must be explicitly documented.

Key considerations for bridge risk & wrapped asset caveats include segregation of duties, least-privilege access, audit logging with tamper-evident retention, encryption in transit and at rest for sensitive payloads, and periodic independent validation of backups and recovery paths. For mining infrastructure, assessors evaluated logical access to management interfaces, change tickets for firmware or pool configuration, and alignment with vendor hardening baselines.

Observations are classified per the severity model in Section 23. Informational items improve maturity; medium and above require tracked remediation with target completion dates and evidence packs. CleanSpark should maintain a continuous monitoring calendar covering certificate expiry, access recertification, dependency advisories, and hashrate anomaly detection correlated with power telemetry.

Cross-dependencies: findings in custody and key management may amplify smart-contract operational risks if administrative keys overlap with deployer roles. CleanSpark should enforce role separation between mining treasury keys, token admin keys (if any), and routine payroll or vendor payment keys. Table 212 in the evidence index references representative samples reviewed for this subsection.

WP 22.3 — Bridge risk & wrapped asset caveats

This subsection (22.3) addresses whitepaper narrative within the CleanSpark Extended Security & Audit Assessment dated 2026. The assessment covers Bitcoin mining operations, hosting relationships, treasury workflows, and CLSK on BNB Smart Chain as described in the system boundary statement. Procedures performed were limited to inquiry, observation, inspection of selected artifacts, and agreed-upon analytics where noted. No opinion on financial statements is expressed.

Management is responsible for design, implementation, and operating effectiveness of controls. Assessors relied on representations regarding scope completeness and should be engaged to re-perform or expand testing when architecture, custodians, contracts, or token logic materially change. Residual risk may remain even when controls appear suitably designed; compensating controls must be explicitly documented.

Key considerations for bridge risk & wrapped asset caveats include segregation of duties, least-privilege access, audit logging with tamper-evident retention, encryption in transit and at rest for sensitive payloads, and periodic independent validation of backups and recovery paths. For mining infrastructure, assessors evaluated logical access to management interfaces, change tickets for firmware or pool configuration, and alignment with vendor hardening baselines.

Observations are classified per the severity model in Section 23. Informational items improve maturity; medium and above require tracked remediation with target completion dates and evidence packs. CleanSpark should maintain a continuous monitoring calendar covering certificate expiry, access recertification, dependency advisories, and hashrate anomaly detection correlated with power telemetry.

Cross-dependencies: findings in custody and key management may amplify smart-contract operational risks if administrative keys overlap with deployer roles. CleanSpark should enforce role separation between mining treasury keys, token admin keys (if any), and routine payroll or vendor payment keys. Table 213 in the evidence index references representative samples reviewed for this subsection.

WP 23.1 — Staking & governance interfaces (future)

This subsection (23.1) addresses whitepaper narrative within the CleanSpark Extended Security & Audit Assessment dated 2026. The assessment covers Bitcoin mining operations, hosting relationships, treasury workflows, and CLSK on BNB Smart Chain as described in the system boundary statement. Procedures performed were limited to inquiry, observation, inspection of selected artifacts, and agreed-upon analytics where noted. No opinion on financial statements is expressed.

Management is responsible for design, implementation, and operating effectiveness of controls. Assessors relied on representations regarding scope completeness and should be engaged to re-perform or expand testing when architecture, custodians, contracts, or token logic materially change. Residual risk may remain even when controls appear suitably designed; compensating controls must be explicitly documented.

Key considerations for staking & governance interfaces (future) include segregation of duties, least-privilege access, audit logging with tamper-evident retention, encryption in transit and at rest for sensitive payloads, and periodic independent validation of backups and recovery paths. For mining infrastructure, assessors evaluated logical access to management interfaces, change tickets for firmware or pool configuration, and alignment with vendor hardening baselines.

Observations are classified per the severity model in Section 23. Informational items improve maturity; medium and above require tracked remediation with target completion dates and evidence packs. CleanSpark should maintain a continuous monitoring calendar covering certificate expiry, access recertification, dependency advisories, and hashrate anomaly detection correlated with power telemetry.

Cross-dependencies: findings in custody and key management may amplify smart-contract operational risks if administrative keys overlap with deployer roles. CleanSpark should enforce role separation between mining treasury keys, token admin keys (if any), and routine payroll or vendor payment keys. Table 221 in the evidence index references representative samples reviewed for this subsection.

WP 23.2 — Staking & governance interfaces (future)

This subsection (23.2) addresses whitepaper narrative within the CleanSpark Extended Security & Audit Assessment dated 2026. The assessment covers Bitcoin mining operations, hosting relationships, treasury workflows, and CLSK on BNB Smart Chain as described in the system boundary statement. Procedures performed were limited to inquiry, observation, inspection of selected artifacts, and agreed-upon analytics where noted. No opinion on financial statements is expressed.

Management is responsible for design, implementation, and operating effectiveness of controls. Assessors relied on representations regarding scope completeness and should be engaged to re-perform or expand testing when architecture, custodians, contracts, or token logic materially change. Residual risk may remain even when controls appear suitably designed; compensating controls must be explicitly documented.

Key considerations for staking & governance interfaces (future) include segregation of duties, least-privilege access, audit logging with tamper-evident retention, encryption in transit and at rest for sensitive payloads, and periodic independent validation of backups and recovery paths. For mining infrastructure, assessors evaluated logical access to management interfaces, change tickets for firmware or pool configuration, and alignment with vendor hardening baselines.

Observations are classified per the severity model in Section 23. Informational items improve maturity; medium and above require tracked remediation with target completion dates and evidence packs. CleanSpark should maintain a continuous monitoring calendar covering certificate expiry, access recertification, dependency advisories, and hashrate anomaly detection correlated with power telemetry.

Cross-dependencies: findings in custody and key management may amplify smart-contract operational risks if administrative keys overlap with deployer roles. CleanSpark should enforce role separation between mining treasury keys, token admin keys (if any), and routine payroll or vendor payment keys. Table 222 in the evidence index references representative samples reviewed for this subsection.

WP 23.3 — Staking & governance interfaces (future)

This subsection (23.3) addresses whitepaper narrative within the CleanSpark Extended Security & Audit Assessment dated 2026. The assessment covers Bitcoin mining operations, hosting relationships, treasury workflows, and CLSK on BNB Smart Chain as described in the system boundary statement. Procedures performed were limited to inquiry, observation, inspection of selected artifacts, and agreed-upon analytics where noted. No opinion on financial statements is expressed.

Management is responsible for design, implementation, and operating effectiveness of controls. Assessors relied on representations regarding scope completeness and should be engaged to re-perform or expand testing when architecture, custodians, contracts, or token logic materially change. Residual risk may remain even when controls appear suitably designed; compensating controls must be explicitly documented.

Key considerations for staking & governance interfaces (future) include segregation of duties, least-privilege access, audit logging with tamper-evident retention, encryption in transit and at rest for sensitive payloads, and periodic independent validation of backups and recovery paths. For mining infrastructure, assessors evaluated logical access to management interfaces, change tickets for firmware or pool configuration, and alignment with vendor hardening baselines.

Observations are classified per the severity model in Section 23. Informational items improve maturity; medium and above require tracked remediation with target completion dates and evidence packs. CleanSpark should maintain a continuous monitoring calendar covering certificate expiry, access recertification, dependency advisories, and hashrate anomaly detection correlated with power telemetry.

Cross-dependencies: findings in custody and key management may amplify smart-contract operational risks if administrative keys overlap with deployer roles. CleanSpark should enforce role separation between mining treasury keys, token admin keys (if any), and routine payroll or vendor payment keys. Table 223 in the evidence index references representative samples reviewed for this subsection.

WP 24.1 — Data room standards for partners

This subsection (24.1) addresses whitepaper narrative within the CleanSpark Extended Security & Audit Assessment dated 2026. The assessment covers Bitcoin mining operations, hosting relationships, treasury workflows, and CLSK on BNB Smart Chain as described in the system boundary statement. Procedures performed were limited to inquiry, observation, inspection of selected artifacts, and agreed-upon analytics where noted. No opinion on financial statements is expressed.

Management is responsible for design, implementation, and operating effectiveness of controls. Assessors relied on representations regarding scope completeness and should be engaged to re-perform or expand testing when architecture, custodians, contracts, or token logic materially change. Residual risk may remain even when controls appear suitably designed; compensating controls must be explicitly documented.

Key considerations for data room standards for partners include segregation of duties, least-privilege access, audit logging with tamper-evident retention, encryption in transit and at rest for sensitive payloads, and periodic independent validation of backups and recovery paths. For mining infrastructure, assessors evaluated logical access to management interfaces, change tickets for firmware or pool configuration, and alignment with vendor hardening baselines.

Observations are classified per the severity model in Section 23. Informational items improve maturity; medium and above require tracked remediation with target completion dates and evidence packs. CleanSpark should maintain a continuous monitoring calendar covering certificate expiry, access recertification, dependency advisories, and hashrate anomaly detection correlated with power telemetry.

Cross-dependencies: findings in custody and key management may amplify smart-contract operational risks if administrative keys overlap with deployer roles. CleanSpark should enforce role separation between mining treasury keys, token admin keys (if any), and routine payroll or vendor payment keys. Table 231 in the evidence index references representative samples reviewed for this subsection.

WP 24.2 — Data room standards for partners

This subsection (24.2) addresses whitepaper narrative within the CleanSpark Extended Security & Audit Assessment dated 2026. The assessment covers Bitcoin mining operations, hosting relationships, treasury workflows, and CLSK on BNB Smart Chain as described in the system boundary statement. Procedures performed were limited to inquiry, observation, inspection of selected artifacts, and agreed-upon analytics where noted. No opinion on financial statements is expressed.

Management is responsible for design, implementation, and operating effectiveness of controls. Assessors relied on representations regarding scope completeness and should be engaged to re-perform or expand testing when architecture, custodians, contracts, or token logic materially change. Residual risk may remain even when controls appear suitably designed; compensating controls must be explicitly documented.

Key considerations for data room standards for partners include segregation of duties, least-privilege access, audit logging with tamper-evident retention, encryption in transit and at rest for sensitive payloads, and periodic independent validation of backups and recovery paths. For mining infrastructure, assessors evaluated logical access to management interfaces, change tickets for firmware or pool configuration, and alignment with vendor hardening baselines.

Observations are classified per the severity model in Section 23. Informational items improve maturity; medium and above require tracked remediation with target completion dates and evidence packs. CleanSpark should maintain a continuous monitoring calendar covering certificate expiry, access recertification, dependency advisories, and hashrate anomaly detection correlated with power telemetry.

Cross-dependencies: findings in custody and key management may amplify smart-contract operational risks if administrative keys overlap with deployer roles. CleanSpark should enforce role separation between mining treasury keys, token admin keys (if any), and routine payroll or vendor payment keys. Table 232 in the evidence index references representative samples reviewed for this subsection.

WP 24.3 — Data room standards for partners

This subsection (24.3) addresses whitepaper narrative within the CleanSpark Extended Security & Audit Assessment dated 2026. The assessment covers Bitcoin mining operations, hosting relationships, treasury workflows, and CLSK on BNB Smart Chain as described in the system boundary statement. Procedures performed were limited to inquiry, observation, inspection of selected artifacts, and agreed-upon analytics where noted. No opinion on financial statements is expressed.

Management is responsible for design, implementation, and operating effectiveness of controls. Assessors relied on representations regarding scope completeness and should be engaged to re-perform or expand testing when architecture, custodians, contracts, or token logic materially change. Residual risk may remain even when controls appear suitably designed; compensating controls must be explicitly documented.

Key considerations for data room standards for partners include segregation of duties, least-privilege access, audit logging with tamper-evident retention, encryption in transit and at rest for sensitive payloads, and periodic independent validation of backups and recovery paths. For mining infrastructure, assessors evaluated logical access to management interfaces, change tickets for firmware or pool configuration, and alignment with vendor hardening baselines.

Observations are classified per the severity model in Section 23. Informational items improve maturity; medium and above require tracked remediation with target completion dates and evidence packs. CleanSpark should maintain a continuous monitoring calendar covering certificate expiry, access recertification, dependency advisories, and hashrate anomaly detection correlated with power telemetry.

Cross-dependencies: findings in custody and key management may amplify smart-contract operational risks if administrative keys overlap with deployer roles. CleanSpark should enforce role separation between mining treasury keys, token admin keys (if any), and routine payroll or vendor payment keys. Table 233 in the evidence index references representative samples reviewed for this subsection.

WP 25.1 — ESG reporting boundaries

This subsection (25.1) addresses whitepaper narrative within the CleanSpark Extended Security & Audit Assessment dated 2026. The assessment covers Bitcoin mining operations, hosting relationships, treasury workflows, and CLSK on BNB Smart Chain as described in the system boundary statement. Procedures performed were limited to inquiry, observation, inspection of selected artifacts, and agreed-upon analytics where noted. No opinion on financial statements is expressed.

Management is responsible for design, implementation, and operating effectiveness of controls. Assessors relied on representations regarding scope completeness and should be engaged to re-perform or expand testing when architecture, custodians, contracts, or token logic materially change. Residual risk may remain even when controls appear suitably designed; compensating controls must be explicitly documented.

Key considerations for esg reporting boundaries include segregation of duties, least-privilege access, audit logging with tamper-evident retention, encryption in transit and at rest for sensitive payloads, and periodic independent validation of backups and recovery paths. For mining infrastructure, assessors evaluated logical access to management interfaces, change tickets for firmware or pool configuration, and alignment with vendor hardening baselines.

Observations are classified per the severity model in Section 23. Informational items improve maturity; medium and above require tracked remediation with target completion dates and evidence packs. CleanSpark should maintain a continuous monitoring calendar covering certificate expiry, access recertification, dependency advisories, and hashrate anomaly detection correlated with power telemetry.

Cross-dependencies: findings in custody and key management may amplify smart-contract operational risks if administrative keys overlap with deployer roles. CleanSpark should enforce role separation between mining treasury keys, token admin keys (if any), and routine payroll or vendor payment keys. Table 241 in the evidence index references representative samples reviewed for this subsection.

WP 25.2 — ESG reporting boundaries

This subsection (25.2) addresses whitepaper narrative within the CleanSpark Extended Security & Audit Assessment dated 2026. The assessment covers Bitcoin mining operations, hosting relationships, treasury workflows, and CLSK on BNB Smart Chain as described in the system boundary statement. Procedures performed were limited to inquiry, observation, inspection of selected artifacts, and agreed-upon analytics where noted. No opinion on financial statements is expressed.

Management is responsible for design, implementation, and operating effectiveness of controls. Assessors relied on representations regarding scope completeness and should be engaged to re-perform or expand testing when architecture, custodians, contracts, or token logic materially change. Residual risk may remain even when controls appear suitably designed; compensating controls must be explicitly documented.

Key considerations for esg reporting boundaries include segregation of duties, least-privilege access, audit logging with tamper-evident retention, encryption in transit and at rest for sensitive payloads, and periodic independent validation of backups and recovery paths. For mining infrastructure, assessors evaluated logical access to management interfaces, change tickets for firmware or pool configuration, and alignment with vendor hardening baselines.

Observations are classified per the severity model in Section 23. Informational items improve maturity; medium and above require tracked remediation with target completion dates and evidence packs. CleanSpark should maintain a continuous monitoring calendar covering certificate expiry, access recertification, dependency advisories, and hashrate anomaly detection correlated with power telemetry.

Cross-dependencies: findings in custody and key management may amplify smart-contract operational risks if administrative keys overlap with deployer roles. CleanSpark should enforce role separation between mining treasury keys, token admin keys (if any), and routine payroll or vendor payment keys. Table 242 in the evidence index references representative samples reviewed for this subsection.

WP 25.3 — ESG reporting boundaries

This subsection (25.3) addresses whitepaper narrative within the CleanSpark Extended Security & Audit Assessment dated 2026. The assessment covers Bitcoin mining operations, hosting relationships, treasury workflows, and CLSK on BNB Smart Chain as described in the system boundary statement. Procedures performed were limited to inquiry, observation, inspection of selected artifacts, and agreed-upon analytics where noted. No opinion on financial statements is expressed.

Management is responsible for design, implementation, and operating effectiveness of controls. Assessors relied on representations regarding scope completeness and should be engaged to re-perform or expand testing when architecture, custodians, contracts, or token logic materially change. Residual risk may remain even when controls appear suitably designed; compensating controls must be explicitly documented.

Key considerations for esg reporting boundaries include segregation of duties, least-privilege access, audit logging with tamper-evident retention, encryption in transit and at rest for sensitive payloads, and periodic independent validation of backups and recovery paths. For mining infrastructure, assessors evaluated logical access to management interfaces, change tickets for firmware or pool configuration, and alignment with vendor hardening baselines.

Observations are classified per the severity model in Section 23. Informational items improve maturity; medium and above require tracked remediation with target completion dates and evidence packs. CleanSpark should maintain a continuous monitoring calendar covering certificate expiry, access recertification, dependency advisories, and hashrate anomaly detection correlated with power telemetry.

Cross-dependencies: findings in custody and key management may amplify smart-contract operational risks if administrative keys overlap with deployer roles. CleanSpark should enforce role separation between mining treasury keys, token admin keys (if any), and routine payroll or vendor payment keys. Table 243 in the evidence index references representative samples reviewed for this subsection.

WP 26.1 — Community grants & ecosystem budget

This subsection (26.1) addresses whitepaper narrative within the CleanSpark Extended Security & Audit Assessment dated 2026. The assessment covers Bitcoin mining operations, hosting relationships, treasury workflows, and CLSK on BNB Smart Chain as described in the system boundary statement. Procedures performed were limited to inquiry, observation, inspection of selected artifacts, and agreed-upon analytics where noted. No opinion on financial statements is expressed.

Management is responsible for design, implementation, and operating effectiveness of controls. Assessors relied on representations regarding scope completeness and should be engaged to re-perform or expand testing when architecture, custodians, contracts, or token logic materially change. Residual risk may remain even when controls appear suitably designed; compensating controls must be explicitly documented.

Key considerations for community grants & ecosystem budget include segregation of duties, least-privilege access, audit logging with tamper-evident retention, encryption in transit and at rest for sensitive payloads, and periodic independent validation of backups and recovery paths. For mining infrastructure, assessors evaluated logical access to management interfaces, change tickets for firmware or pool configuration, and alignment with vendor hardening baselines.

Observations are classified per the severity model in Section 23. Informational items improve maturity; medium and above require tracked remediation with target completion dates and evidence packs. CleanSpark should maintain a continuous monitoring calendar covering certificate expiry, access recertification, dependency advisories, and hashrate anomaly detection correlated with power telemetry.

Cross-dependencies: findings in custody and key management may amplify smart-contract operational risks if administrative keys overlap with deployer roles. CleanSpark should enforce role separation between mining treasury keys, token admin keys (if any), and routine payroll or vendor payment keys. Table 251 in the evidence index references representative samples reviewed for this subsection.

WP 26.2 — Community grants & ecosystem budget

This subsection (26.2) addresses whitepaper narrative within the CleanSpark Extended Security & Audit Assessment dated 2026. The assessment covers Bitcoin mining operations, hosting relationships, treasury workflows, and CLSK on BNB Smart Chain as described in the system boundary statement. Procedures performed were limited to inquiry, observation, inspection of selected artifacts, and agreed-upon analytics where noted. No opinion on financial statements is expressed.

Management is responsible for design, implementation, and operating effectiveness of controls. Assessors relied on representations regarding scope completeness and should be engaged to re-perform or expand testing when architecture, custodians, contracts, or token logic materially change. Residual risk may remain even when controls appear suitably designed; compensating controls must be explicitly documented.

Key considerations for community grants & ecosystem budget include segregation of duties, least-privilege access, audit logging with tamper-evident retention, encryption in transit and at rest for sensitive payloads, and periodic independent validation of backups and recovery paths. For mining infrastructure, assessors evaluated logical access to management interfaces, change tickets for firmware or pool configuration, and alignment with vendor hardening baselines.

Observations are classified per the severity model in Section 23. Informational items improve maturity; medium and above require tracked remediation with target completion dates and evidence packs. CleanSpark should maintain a continuous monitoring calendar covering certificate expiry, access recertification, dependency advisories, and hashrate anomaly detection correlated with power telemetry.

Cross-dependencies: findings in custody and key management may amplify smart-contract operational risks if administrative keys overlap with deployer roles. CleanSpark should enforce role separation between mining treasury keys, token admin keys (if any), and routine payroll or vendor payment keys. Table 252 in the evidence index references representative samples reviewed for this subsection.

WP 26.3 — Community grants & ecosystem budget

This subsection (26.3) addresses whitepaper narrative within the CleanSpark Extended Security & Audit Assessment dated 2026. The assessment covers Bitcoin mining operations, hosting relationships, treasury workflows, and CLSK on BNB Smart Chain as described in the system boundary statement. Procedures performed were limited to inquiry, observation, inspection of selected artifacts, and agreed-upon analytics where noted. No opinion on financial statements is expressed.

Management is responsible for design, implementation, and operating effectiveness of controls. Assessors relied on representations regarding scope completeness and should be engaged to re-perform or expand testing when architecture, custodians, contracts, or token logic materially change. Residual risk may remain even when controls appear suitably designed; compensating controls must be explicitly documented.

Key considerations for community grants & ecosystem budget include segregation of duties, least-privilege access, audit logging with tamper-evident retention, encryption in transit and at rest for sensitive payloads, and periodic independent validation of backups and recovery paths. For mining infrastructure, assessors evaluated logical access to management interfaces, change tickets for firmware or pool configuration, and alignment with vendor hardening baselines.

Observations are classified per the severity model in Section 23. Informational items improve maturity; medium and above require tracked remediation with target completion dates and evidence packs. CleanSpark should maintain a continuous monitoring calendar covering certificate expiry, access recertification, dependency advisories, and hashrate anomaly detection correlated with power telemetry.

Cross-dependencies: findings in custody and key management may amplify smart-contract operational risks if administrative keys overlap with deployer roles. CleanSpark should enforce role separation between mining treasury keys, token admin keys (if any), and routine payroll or vendor payment keys. Table 253 in the evidence index references representative samples reviewed for this subsection.

WP 27.1 — Brand protection & impersonation response

This subsection (27.1) addresses whitepaper narrative within the CleanSpark Extended Security & Audit Assessment dated 2026. The assessment covers Bitcoin mining operations, hosting relationships, treasury workflows, and CLSK on BNB Smart Chain as described in the system boundary statement. Procedures performed were limited to inquiry, observation, inspection of selected artifacts, and agreed-upon analytics where noted. No opinion on financial statements is expressed.

Management is responsible for design, implementation, and operating effectiveness of controls. Assessors relied on representations regarding scope completeness and should be engaged to re-perform or expand testing when architecture, custodians, contracts, or token logic materially change. Residual risk may remain even when controls appear suitably designed; compensating controls must be explicitly documented.

Key considerations for brand protection & impersonation response include segregation of duties, least-privilege access, audit logging with tamper-evident retention, encryption in transit and at rest for sensitive payloads, and periodic independent validation of backups and recovery paths. For mining infrastructure, assessors evaluated logical access to management interfaces, change tickets for firmware or pool configuration, and alignment with vendor hardening baselines.

Observations are classified per the severity model in Section 23. Informational items improve maturity; medium and above require tracked remediation with target completion dates and evidence packs. CleanSpark should maintain a continuous monitoring calendar covering certificate expiry, access recertification, dependency advisories, and hashrate anomaly detection correlated with power telemetry.

Cross-dependencies: findings in custody and key management may amplify smart-contract operational risks if administrative keys overlap with deployer roles. CleanSpark should enforce role separation between mining treasury keys, token admin keys (if any), and routine payroll or vendor payment keys. Table 261 in the evidence index references representative samples reviewed for this subsection.

WP 27.2 — Brand protection & impersonation response

This subsection (27.2) addresses whitepaper narrative within the CleanSpark Extended Security & Audit Assessment dated 2026. The assessment covers Bitcoin mining operations, hosting relationships, treasury workflows, and CLSK on BNB Smart Chain as described in the system boundary statement. Procedures performed were limited to inquiry, observation, inspection of selected artifacts, and agreed-upon analytics where noted. No opinion on financial statements is expressed.

Management is responsible for design, implementation, and operating effectiveness of controls. Assessors relied on representations regarding scope completeness and should be engaged to re-perform or expand testing when architecture, custodians, contracts, or token logic materially change. Residual risk may remain even when controls appear suitably designed; compensating controls must be explicitly documented.

Key considerations for brand protection & impersonation response include segregation of duties, least-privilege access, audit logging with tamper-evident retention, encryption in transit and at rest for sensitive payloads, and periodic independent validation of backups and recovery paths. For mining infrastructure, assessors evaluated logical access to management interfaces, change tickets for firmware or pool configuration, and alignment with vendor hardening baselines.

Observations are classified per the severity model in Section 23. Informational items improve maturity; medium and above require tracked remediation with target completion dates and evidence packs. CleanSpark should maintain a continuous monitoring calendar covering certificate expiry, access recertification, dependency advisories, and hashrate anomaly detection correlated with power telemetry.

Cross-dependencies: findings in custody and key management may amplify smart-contract operational risks if administrative keys overlap with deployer roles. CleanSpark should enforce role separation between mining treasury keys, token admin keys (if any), and routine payroll or vendor payment keys. Table 262 in the evidence index references representative samples reviewed for this subsection.

WP 27.3 — Brand protection & impersonation response

This subsection (27.3) addresses whitepaper narrative within the CleanSpark Extended Security & Audit Assessment dated 2026. The assessment covers Bitcoin mining operations, hosting relationships, treasury workflows, and CLSK on BNB Smart Chain as described in the system boundary statement. Procedures performed were limited to inquiry, observation, inspection of selected artifacts, and agreed-upon analytics where noted. No opinion on financial statements is expressed.

Management is responsible for design, implementation, and operating effectiveness of controls. Assessors relied on representations regarding scope completeness and should be engaged to re-perform or expand testing when architecture, custodians, contracts, or token logic materially change. Residual risk may remain even when controls appear suitably designed; compensating controls must be explicitly documented.

Key considerations for brand protection & impersonation response include segregation of duties, least-privilege access, audit logging with tamper-evident retention, encryption in transit and at rest for sensitive payloads, and periodic independent validation of backups and recovery paths. For mining infrastructure, assessors evaluated logical access to management interfaces, change tickets for firmware or pool configuration, and alignment with vendor hardening baselines.

Observations are classified per the severity model in Section 23. Informational items improve maturity; medium and above require tracked remediation with target completion dates and evidence packs. CleanSpark should maintain a continuous monitoring calendar covering certificate expiry, access recertification, dependency advisories, and hashrate anomaly detection correlated with power telemetry.

Cross-dependencies: findings in custody and key management may amplify smart-contract operational risks if administrative keys overlap with deployer roles. CleanSpark should enforce role separation between mining treasury keys, token admin keys (if any), and routine payroll or vendor payment keys. Table 263 in the evidence index references representative samples reviewed for this subsection.

WP 28.1 — Roadmap communication discipline

This subsection (28.1) addresses whitepaper narrative within the CleanSpark Extended Security & Audit Assessment dated 2026. The assessment covers Bitcoin mining operations, hosting relationships, treasury workflows, and CLSK on BNB Smart Chain as described in the system boundary statement. Procedures performed were limited to inquiry, observation, inspection of selected artifacts, and agreed-upon analytics where noted. No opinion on financial statements is expressed.

Management is responsible for design, implementation, and operating effectiveness of controls. Assessors relied on representations regarding scope completeness and should be engaged to re-perform or expand testing when architecture, custodians, contracts, or token logic materially change. Residual risk may remain even when controls appear suitably designed; compensating controls must be explicitly documented.

Key considerations for roadmap communication discipline include segregation of duties, least-privilege access, audit logging with tamper-evident retention, encryption in transit and at rest for sensitive payloads, and periodic independent validation of backups and recovery paths. For mining infrastructure, assessors evaluated logical access to management interfaces, change tickets for firmware or pool configuration, and alignment with vendor hardening baselines.

Observations are classified per the severity model in Section 23. Informational items improve maturity; medium and above require tracked remediation with target completion dates and evidence packs. CleanSpark should maintain a continuous monitoring calendar covering certificate expiry, access recertification, dependency advisories, and hashrate anomaly detection correlated with power telemetry.

Cross-dependencies: findings in custody and key management may amplify smart-contract operational risks if administrative keys overlap with deployer roles. CleanSpark should enforce role separation between mining treasury keys, token admin keys (if any), and routine payroll or vendor payment keys. Table 271 in the evidence index references representative samples reviewed for this subsection.

WP 28.2 — Roadmap communication discipline

This subsection (28.2) addresses whitepaper narrative within the CleanSpark Extended Security & Audit Assessment dated 2026. The assessment covers Bitcoin mining operations, hosting relationships, treasury workflows, and CLSK on BNB Smart Chain as described in the system boundary statement. Procedures performed were limited to inquiry, observation, inspection of selected artifacts, and agreed-upon analytics where noted. No opinion on financial statements is expressed.

Management is responsible for design, implementation, and operating effectiveness of controls. Assessors relied on representations regarding scope completeness and should be engaged to re-perform or expand testing when architecture, custodians, contracts, or token logic materially change. Residual risk may remain even when controls appear suitably designed; compensating controls must be explicitly documented.

Key considerations for roadmap communication discipline include segregation of duties, least-privilege access, audit logging with tamper-evident retention, encryption in transit and at rest for sensitive payloads, and periodic independent validation of backups and recovery paths. For mining infrastructure, assessors evaluated logical access to management interfaces, change tickets for firmware or pool configuration, and alignment with vendor hardening baselines.

Observations are classified per the severity model in Section 23. Informational items improve maturity; medium and above require tracked remediation with target completion dates and evidence packs. CleanSpark should maintain a continuous monitoring calendar covering certificate expiry, access recertification, dependency advisories, and hashrate anomaly detection correlated with power telemetry.

Cross-dependencies: findings in custody and key management may amplify smart-contract operational risks if administrative keys overlap with deployer roles. CleanSpark should enforce role separation between mining treasury keys, token admin keys (if any), and routine payroll or vendor payment keys. Table 272 in the evidence index references representative samples reviewed for this subsection.

WP 28.3 — Roadmap communication discipline

This subsection (28.3) addresses whitepaper narrative within the CleanSpark Extended Security & Audit Assessment dated 2026. The assessment covers Bitcoin mining operations, hosting relationships, treasury workflows, and CLSK on BNB Smart Chain as described in the system boundary statement. Procedures performed were limited to inquiry, observation, inspection of selected artifacts, and agreed-upon analytics where noted. No opinion on financial statements is expressed.

Management is responsible for design, implementation, and operating effectiveness of controls. Assessors relied on representations regarding scope completeness and should be engaged to re-perform or expand testing when architecture, custodians, contracts, or token logic materially change. Residual risk may remain even when controls appear suitably designed; compensating controls must be explicitly documented.

Key considerations for roadmap communication discipline include segregation of duties, least-privilege access, audit logging with tamper-evident retention, encryption in transit and at rest for sensitive payloads, and periodic independent validation of backups and recovery paths. For mining infrastructure, assessors evaluated logical access to management interfaces, change tickets for firmware or pool configuration, and alignment with vendor hardening baselines.

Observations are classified per the severity model in Section 23. Informational items improve maturity; medium and above require tracked remediation with target completion dates and evidence packs. CleanSpark should maintain a continuous monitoring calendar covering certificate expiry, access recertification, dependency advisories, and hashrate anomaly detection correlated with power telemetry.

Cross-dependencies: findings in custody and key management may amplify smart-contract operational risks if administrative keys overlap with deployer roles. CleanSpark should enforce role separation between mining treasury keys, token admin keys (if any), and routine payroll or vendor payment keys. Table 273 in the evidence index references representative samples reviewed for this subsection.