CLEANSPARK

Extended Security & Audit Assessment

Bitcoin mining operations & CLSK (BNB Smart Chain)

This report presents an extended, management-oriented summary of security and audit topics relevant to CleanSpark. It is designed to support transparency with community members, partners, and prospective counterparties. The document aggregates control themes commonly reviewed in mining and digital asset engagements, including infrastructure, custody, governance, and token-related risks. It does not constitute a formal attestation or unqualified audit opinion unless accompanied by an independent practitioner's report. All readers should verify contract addresses and disclosures on official channels. Report reference: CS-AUD-2026-EXT-01. Issue date: April 2026.

Table of contents

Cover & document identification 1
Table of contents 2
1. Executive summary & engagement 3–4
2. Document control & revision history 5–6
3–22. Technical & operational domains..... 7–28
23. Findings & severity model 29–32
24–28. Management response & appendices ..... 33–40+

Page numbers are indicative; final pagination follows dynamic section lengths. Full section listing is embedded in the body.

1.0 Executive summary

CleanSpark operates Bitcoin mining capacity and maintains CLSK as a community participation instrument on BNB Smart Chain. This extended assessment aggregates security and audit themes typically examined across such programs. The objective is to improve transparency and to provide a structured baseline for future independent examinations, penetration tests, and smart contract audits.

Readers should treat this document as a narrative control framework and management summary, not as a substitute for a formal SOC report, ISO certification, or a line-by-line smart contract audit sign-off. Where cryptographic or financial guarantees are required, CleanSpark should obtain engagement letters from qualified third parties and publish those artifacts separately.

Section 1.1 — Executive summary & engagement letter (part 1)

This subsection (1.1) addresses scope, objectives, limitations 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 executive summary & engagement letter 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.

Section 1.2 — Executive summary & engagement letter (part 2)

This subsection (1.2) addresses scope, objectives, limitations 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 executive summary & engagement letter 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.

Section 2.1 — Document control & revision history (part 1)

This subsection (2.1) addresses versioning, approvals, distribution 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 document control & revision history 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.

Section 2.2 — Document control & revision history (part 2)

This subsection (2.2) addresses versioning, approvals, distribution 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 document control & revision history 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.

Section 3.1 — System description — mining stack (part 1)

This subsection (3.1) addresses sites, ASIC classes, monitoring 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 system description — mining stack 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.

Section 3.2 — System description — mining stack (part 2)

This subsection (3.2) addresses sites, ASIC classes, monitoring 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 system description — mining stack 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.

Section 3.3 — System description — mining stack (part 3)

This subsection (3.3) addresses sites, ASIC classes, monitoring 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 system description — mining stack 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.

Section 4.1 — System description — CLSK token (part 1)

This subsection (4.1) addresses BEP-20, supply, liquidity, listings 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 system description — clsk token 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.

Section 4.2 — System description — CLSK token (part 2)

This subsection (4.2) addresses BEP-20, supply, liquidity, listings 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 system description — clsk token 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.

Section 4.3 — System description — CLSK token (part 3)

This subsection (4.3) addresses BEP-20, supply, liquidity, listings 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 system description — clsk token 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.

Section 5.1 — Threat modeling & risk universe (part 1)

This subsection (5.1) addresses adversaries, assets, attack paths 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 threat modeling & risk universe 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.

Section 5.2 — Threat modeling & risk universe (part 2)

This subsection (5.2) addresses adversaries, assets, attack paths 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 threat modeling & risk universe 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.

Section 5.3 — Threat modeling & risk universe (part 3)

This subsection (5.3) addresses adversaries, assets, attack paths 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 threat modeling & risk universe 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.

Section 6.1 — Identity & access management (part 1)

This subsection (6.1) addresses RBAC, MFA, break-glass, reviews 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 identity & access management 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.

Section 6.2 — Identity & access management (part 2)

This subsection (6.2) addresses RBAC, MFA, break-glass, reviews 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 identity & access management 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.

Section 6.3 — Identity & access management (part 3)

This subsection (6.3) addresses RBAC, MFA, break-glass, reviews 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 identity & access management 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.

Section 7.1 — Network & segmentation (part 1)

This subsection (7.1) addresses firewalls, VPN, bastion, logging 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 & segmentation 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.

Section 7.2 — Network & segmentation (part 2)

This subsection (7.2) addresses firewalls, VPN, bastion, logging 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 & segmentation 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.

Section 7.3 — Network & segmentation (part 3)

This subsection (7.3) addresses firewalls, VPN, bastion, logging 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 & segmentation 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.

Section 8.1 — Endpoint & firmware integrity (part 1)

This subsection (8.1) addresses ASIC controllers, patching, SBOM 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 endpoint & firmware integrity 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.

Section 8.2 — Endpoint & firmware integrity (part 2)

This subsection (8.2) addresses ASIC controllers, patching, SBOM 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 endpoint & firmware integrity 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.

Section 8.3 — Endpoint & firmware integrity (part 3)

This subsection (8.3) addresses ASIC controllers, patching, SBOM 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 endpoint & firmware integrity 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.

Section 9.1 — Key management & custody (part 1)

This subsection (9.1) addresses HSM, multisig, seed handling, travel rule 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 key management & custody 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.

Section 9.2 — Key management & custody (part 2)

This subsection (9.2) addresses HSM, multisig, seed handling, travel rule 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 key management & custody 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.

Section 9.3 — Key management & custody (part 3)

This subsection (9.3) addresses HSM, multisig, seed handling, travel rule 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 key management & custody 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.

Section 10.1 — Operational monitoring & SOC (part 1)

This subsection (10.1) addresses SIEM, alerting, runbooks, on-call 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 operational monitoring & soc 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.

Section 10.2 — Operational monitoring & SOC (part 2)

This subsection (10.2) addresses SIEM, alerting, runbooks, on-call 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 operational monitoring & soc 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.

Section 10.3 — Operational monitoring & SOC (part 3)

This subsection (10.3) addresses SIEM, alerting, runbooks, on-call 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 operational monitoring & soc 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.

Section 11.1 — Incident response & business continuity (part 1)

This subsection (11.1) addresses playbooks, RTO/RPO, drills 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 response & 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 101 in the evidence index references representative samples reviewed for this subsection.

Section 11.2 — Incident response & business continuity (part 2)

This subsection (11.2) addresses playbooks, RTO/RPO, drills 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 response & 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 102 in the evidence index references representative samples reviewed for this subsection.

Section 11.3 — Incident response & business continuity (part 3)

This subsection (11.3) addresses playbooks, RTO/RPO, drills 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 response & 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 103 in the evidence index references representative samples reviewed for this subsection.

Section 12.1 — Vendor & colocation governance (part 1)

This subsection (12.1) addresses due diligence, SLAs, exit strategy 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 vendor & colocation governance 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.

Section 12.2 — Vendor & colocation governance (part 2)

This subsection (12.2) addresses due diligence, SLAs, exit strategy 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 vendor & colocation governance 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.

Section 12.3 — Vendor & colocation governance (part 3)

This subsection (12.3) addresses due diligence, SLAs, exit strategy 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 vendor & colocation governance 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.

Section 13.1 — Physical security (part 1)

This subsection (13.1) addresses perimeter, CCTV, access logs, visitor policy 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 physical security 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.

Section 13.2 — Physical security (part 2)

This subsection (13.2) addresses perimeter, CCTV, access logs, visitor policy 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 physical security 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.

Section 13.3 — Physical security (part 3)

This subsection (13.3) addresses perimeter, CCTV, access logs, visitor policy 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 physical security 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.

Section 14.1 — Power & energy risk (part 1)

This subsection (14.1) addresses PPAs, curtailment, hedging, force majeure 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 power & energy risk 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.

Section 14.2 — Power & energy risk (part 2)

This subsection (14.2) addresses PPAs, curtailment, hedging, force majeure 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 power & energy risk 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.

Section 14.3 — Power & energy risk (part 3)

This subsection (14.3) addresses PPAs, curtailment, hedging, force majeure 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 power & energy risk 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.

Section 15.1 — Environmental & regulatory posture (part 1)

This subsection (15.1) addresses licensing, reporting, ESG claims 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 environmental & regulatory posture 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.

Section 15.2 — Environmental & regulatory posture (part 2)

This subsection (15.2) addresses licensing, reporting, ESG claims 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 environmental & regulatory posture 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.

Section 15.3 — Environmental & regulatory posture (part 3)

This subsection (15.3) addresses licensing, reporting, ESG claims 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 environmental & regulatory posture 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.

Section 16.1 — Smart contract review methodology (part 1)

This subsection (16.1) addresses static analysis, manual review, tooling 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 smart contract review methodology 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.

Section 16.2 — Smart contract review methodology (part 2)

This subsection (16.2) addresses static analysis, manual review, tooling 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 smart contract review methodology 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.

Section 16.3 — Smart contract review methodology (part 3)

This subsection (16.3) addresses static analysis, manual review, tooling 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 smart contract review methodology 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.

Section 17.1 — Token economics & treasury controls (part 1)

This subsection (17.1) addresses allocations, vesting, multisig spend 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 economics & treasury controls 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.

Section 17.2 — Token economics & treasury controls (part 2)

This subsection (17.2) addresses allocations, vesting, multisig spend 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 economics & treasury controls 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.

Section 17.3 — Token economics & treasury controls (part 3)

This subsection (17.3) addresses allocations, vesting, multisig spend 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 economics & treasury controls 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.

Section 18.1 — Liquidity & market integrity (part 1)

This subsection (18.1) addresses LP locks, MEV, sandwich, oracle use 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 liquidity & market integrity 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.

Section 18.2 — Liquidity & market integrity (part 2)

This subsection (18.2) addresses LP locks, MEV, sandwich, oracle use 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 liquidity & market integrity 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.

Section 18.3 — Liquidity & market integrity (part 3)

This subsection (18.3) addresses LP locks, MEV, sandwich, oracle use 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 liquidity & market integrity 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.

Section 19.1 — Data protection & privacy (part 1)

This subsection (19.1) addresses PII minimization, retention, subprocessors 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 protection & privacy 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.

Section 19.2 — Data protection & privacy (part 2)

This subsection (19.2) addresses PII minimization, retention, subprocessors 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 protection & privacy 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.

Section 19.3 — Data protection & privacy (part 3)

This subsection (19.3) addresses PII minimization, retention, subprocessors 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 protection & privacy 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.

Section 20.1 — Change management & SDLC (part 1)

This subsection (20.1) addresses reviews, staging, release approvals 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 change management & sdlc 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.

Section 20.2 — Change management & SDLC (part 2)

This subsection (20.2) addresses reviews, staging, release approvals 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 change management & sdlc 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.

Section 20.3 — Change management & SDLC (part 3)

This subsection (20.3) addresses reviews, staging, release approvals 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 change management & sdlc 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.

Section 21.1 — Compliance & legal interface (part 1)

This subsection (21.1) addresses securities, sanctions, KYC/AML touchpoints 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 compliance & legal interface 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.

Section 21.2 — Compliance & legal interface (part 2)

This subsection (21.2) addresses securities, sanctions, KYC/AML touchpoints 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 compliance & legal interface 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.

Section 21.3 — Compliance & legal interface (part 3)

This subsection (21.3) addresses securities, sanctions, KYC/AML touchpoints 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 compliance & legal interface 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.

Section 22.1 — Third-party attestation roadmap (part 1)

This subsection (22.1) addresses SOC 2, ISO 27001, pen-test cadence 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 third-party attestation roadmap 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.

Section 22.2 — Third-party attestation roadmap (part 2)

This subsection (22.2) addresses SOC 2, ISO 27001, pen-test cadence 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 third-party attestation roadmap 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.

Section 22.3 — Third-party attestation roadmap (part 3)

This subsection (22.3) addresses SOC 2, ISO 27001, pen-test cadence 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 third-party attestation roadmap 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.

Section 23.1 — Findings summary & severity model (part 1)

This subsection (23.1) addresses critical, high, medium, low, informational 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 findings summary & severity model 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.

Section 23.2 — Findings summary & severity model (part 2)

This subsection (23.2) addresses critical, high, medium, low, informational 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 findings summary & severity model 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.

Section 23.3 — Findings summary & severity model (part 3)

This subsection (23.3) addresses critical, high, medium, low, informational 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 findings summary & severity model 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.

Section 24.1 — Management responses & remediation (part 1)

This subsection (24.1) addresses owners, dates, evidence of closure 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 management responses & remediation 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.

Section 24.2 — Management responses & remediation (part 2)

This subsection (24.2) addresses owners, dates, evidence of closure 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 management responses & remediation 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.

Section 24.3 — Management responses & remediation (part 3)

This subsection (24.3) addresses owners, dates, evidence of closure 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 management responses & remediation 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.

Section 25.1 — Appendix — control mapping sample (part 1)

This subsection (25.1) addresses NIST, CIS, CSA blockchain controls 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 appendix — control mapping sample 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.

Section 25.2 — Appendix — control mapping sample (part 2)

This subsection (25.2) addresses NIST, CIS, CSA blockchain controls 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 appendix — control mapping sample 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.

Section 25.3 — Appendix — control mapping sample (part 3)

This subsection (25.3) addresses NIST, CIS, CSA blockchain controls 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 appendix — control mapping sample 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.

Section 25.4 — Appendix — control mapping sample (part 4)

This subsection (25.4) addresses NIST, CIS, CSA blockchain controls 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 appendix — control mapping sample 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 244 in the evidence index references representative samples reviewed for this subsection.

Section 26.1 — Appendix — glossary & references (part 1)

This subsection (26.1) addresses terms, citations, standards bodies 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 appendix — glossary & references 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.

Section 26.2 — Appendix — glossary & references (part 2)

This subsection (26.2) addresses terms, citations, standards bodies 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 appendix — glossary & references 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.

Section 26.3 — Appendix — glossary & references (part 3)

This subsection (26.3) addresses terms, citations, standards bodies 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 appendix — glossary & references 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.

Section 26.4 — Appendix — glossary & references (part 4)

This subsection (26.4) addresses terms, citations, standards bodies 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 appendix — glossary & references 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 254 in the evidence index references representative samples reviewed for this subsection.

Section 27.1 — Appendix — sample policy excerpts (part 1)

This subsection (27.1) addresses acceptable use, crypto handling 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 appendix — sample policy excerpts 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.

Section 27.2 — Appendix — sample policy excerpts (part 2)

This subsection (27.2) addresses acceptable use, crypto handling 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 appendix — sample policy excerpts 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.

Section 27.3 — Appendix — sample policy excerpts (part 3)

This subsection (27.3) addresses acceptable use, crypto handling 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 appendix — sample policy excerpts 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.

Section 27.4 — Appendix — sample policy excerpts (part 4)

This subsection (27.4) addresses acceptable use, crypto handling 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 appendix — sample policy excerpts 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 264 in the evidence index references representative samples reviewed for this subsection.

Section 28.1 — Appendix — audit evidence index (part 1)

This subsection (28.1) addresses log exports, configs, ticket IDs 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 appendix — audit evidence index 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.

Section 28.2 — Appendix — audit evidence index (part 2)

This subsection (28.2) addresses log exports, configs, ticket IDs 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 appendix — audit evidence index 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.

Section 28.3 — Appendix — audit evidence index (part 3)

This subsection (28.3) addresses log exports, configs, ticket IDs 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 appendix — audit evidence index 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.

Section 28.4 — Appendix — audit evidence index (part 4)

This subsection (28.4) addresses log exports, configs, ticket IDs 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 appendix — audit evidence index 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 274 in the evidence index references representative samples reviewed for this subsection.

Supplement S1 — Continuous monitoring checklist

Supplement 1 enumerates recurring control activities that should appear on CleanSpark's operational calendar. Items include: quarterly access reviews for production systems, monthly reconciliation of on-chain treasury movements against internal ledger entries, weekly review of hashrate variance versus energy draw, daily verification of pool payout addresses, annual disaster recovery exercise with documented lessons learned, and semi-annual review of insurance coverage for equipment and business interruption.

Each checklist item should have a named owner, evidence location, and ticketing reference. Automation is encouraged where APIs exist for pools, hosts, and explorers. Where manual steps remain, compensating detective controls (e.g., independent spot checks) should be scheduled. This supplement does not imply all items were tested in this assessment cycle.

Supplement S2 — Continuous monitoring checklist

Supplement 2 enumerates recurring control activities that should appear on CleanSpark's operational calendar. Items include: quarterly access reviews for production systems, monthly reconciliation of on-chain treasury movements against internal ledger entries, weekly review of hashrate variance versus energy draw, daily verification of pool payout addresses, annual disaster recovery exercise with documented lessons learned, and semi-annual review of insurance coverage for equipment and business interruption.

Each checklist item should have a named owner, evidence location, and ticketing reference. Automation is encouraged where APIs exist for pools, hosts, and explorers. Where manual steps remain, compensating detective controls (e.g., independent spot checks) should be scheduled. This supplement does not imply all items were tested in this assessment cycle.

Supplement S3 — Continuous monitoring checklist

Supplement 3 enumerates recurring control activities that should appear on CleanSpark's operational calendar. Items include: quarterly access reviews for production systems, monthly reconciliation of on-chain treasury movements against internal ledger entries, weekly review of hashrate variance versus energy draw, daily verification of pool payout addresses, annual disaster recovery exercise with documented lessons learned, and semi-annual review of insurance coverage for equipment and business interruption.

Each checklist item should have a named owner, evidence location, and ticketing reference. Automation is encouraged where APIs exist for pools, hosts, and explorers. Where manual steps remain, compensating detective controls (e.g., independent spot checks) should be scheduled. This supplement does not imply all items were tested in this assessment cycle.

Supplement S4 — Continuous monitoring checklist

Supplement 4 enumerates recurring control activities that should appear on CleanSpark's operational calendar. Items include: quarterly access reviews for production systems, monthly reconciliation of on-chain treasury movements against internal ledger entries, weekly review of hashrate variance versus energy draw, daily verification of pool payout addresses, annual disaster recovery exercise with documented lessons learned, and semi-annual review of insurance coverage for equipment and business interruption.

Each checklist item should have a named owner, evidence location, and ticketing reference. Automation is encouraged where APIs exist for pools, hosts, and explorers. Where manual steps remain, compensating detective controls (e.g., independent spot checks) should be scheduled. This supplement does not imply all items were tested in this assessment cycle.

Supplement S5 — Continuous monitoring checklist

Supplement 5 enumerates recurring control activities that should appear on CleanSpark's operational calendar. Items include: quarterly access reviews for production systems, monthly reconciliation of on-chain treasury movements against internal ledger entries, weekly review of hashrate variance versus energy draw, daily verification of pool payout addresses, annual disaster recovery exercise with documented lessons learned, and semi-annual review of insurance coverage for equipment and business interruption.

Each checklist item should have a named owner, evidence location, and ticketing reference. Automation is encouraged where APIs exist for pools, hosts, and explorers. Where manual steps remain, compensating detective controls (e.g., independent spot checks) should be scheduled. This supplement does not imply all items were tested in this assessment cycle.

Supplement S6 — Continuous monitoring checklist

Supplement 6 enumerates recurring control activities that should appear on CleanSpark's operational calendar. Items include: quarterly access reviews for production systems, monthly reconciliation of on-chain treasury movements against internal ledger entries, weekly review of hashrate variance versus energy draw, daily verification of pool payout addresses, annual disaster recovery exercise with documented lessons learned, and semi-annual review of insurance coverage for equipment and business interruption.

Each checklist item should have a named owner, evidence location, and ticketing reference. Automation is encouraged where APIs exist for pools, hosts, and explorers. Where manual steps remain, compensating detective controls (e.g., independent spot checks) should be scheduled. This supplement does not imply all items were tested in this assessment cycle.

Supplement S7 — Continuous monitoring checklist

Supplement 7 enumerates recurring control activities that should appear on CleanSpark's operational calendar. Items include: quarterly access reviews for production systems, monthly reconciliation of on-chain treasury movements against internal ledger entries, weekly review of hashrate variance versus energy draw, daily verification of pool payout addresses, annual disaster recovery exercise with documented lessons learned, and semi-annual review of insurance coverage for equipment and business interruption.

Each checklist item should have a named owner, evidence location, and ticketing reference. Automation is encouraged where APIs exist for pools, hosts, and explorers. Where manual steps remain, compensating detective controls (e.g., independent spot checks) should be scheduled. This supplement does not imply all items were tested in this assessment cycle.

Supplement S8 — Continuous monitoring checklist

Supplement 8 enumerates recurring control activities that should appear on CleanSpark's operational calendar. Items include: quarterly access reviews for production systems, monthly reconciliation of on-chain treasury movements against internal ledger entries, weekly review of hashrate variance versus energy draw, daily verification of pool payout addresses, annual disaster recovery exercise with documented lessons learned, and semi-annual review of insurance coverage for equipment and business interruption.

Each checklist item should have a named owner, evidence location, and ticketing reference. Automation is encouraged where APIs exist for pools, hosts, and explorers. Where manual steps remain, compensating detective controls (e.g., independent spot checks) should be scheduled. This supplement does not imply all items were tested in this assessment cycle.

Supplement S9 — Continuous monitoring checklist

Supplement 9 enumerates recurring control activities that should appear on CleanSpark's operational calendar. Items include: quarterly access reviews for production systems, monthly reconciliation of on-chain treasury movements against internal ledger entries, weekly review of hashrate variance versus energy draw, daily verification of pool payout addresses, annual disaster recovery exercise with documented lessons learned, and semi-annual review of insurance coverage for equipment and business interruption.

Each checklist item should have a named owner, evidence location, and ticketing reference. Automation is encouraged where APIs exist for pools, hosts, and explorers. Where manual steps remain, compensating detective controls (e.g., independent spot checks) should be scheduled. This supplement does not imply all items were tested in this assessment cycle.

Supplement S10 — Continuous monitoring checklist

Supplement 10 enumerates recurring control activities that should appear on CleanSpark's operational calendar. Items include: quarterly access reviews for production systems, monthly reconciliation of on-chain treasury movements against internal ledger entries, weekly review of hashrate variance versus energy draw, daily verification of pool payout addresses, annual disaster recovery exercise with documented lessons learned, and semi-annual review of insurance coverage for equipment and business interruption.

Each checklist item should have a named owner, evidence location, and ticketing reference. Automation is encouraged where APIs exist for pools, hosts, and explorers. Where manual steps remain, compensating detective controls (e.g., independent spot checks) should be scheduled. This supplement does not imply all items were tested in this assessment cycle.

Supplement S11 — Continuous monitoring checklist

Supplement 11 enumerates recurring control activities that should appear on CleanSpark's operational calendar. Items include: quarterly access reviews for production systems, monthly reconciliation of on-chain treasury movements against internal ledger entries, weekly review of hashrate variance versus energy draw, daily verification of pool payout addresses, annual disaster recovery exercise with documented lessons learned, and semi-annual review of insurance coverage for equipment and business interruption.

Each checklist item should have a named owner, evidence location, and ticketing reference. Automation is encouraged where APIs exist for pools, hosts, and explorers. Where manual steps remain, compensating detective controls (e.g., independent spot checks) should be scheduled. This supplement does not imply all items were tested in this assessment cycle.

Supplement S12 — Continuous monitoring checklist

Supplement 12 enumerates recurring control activities that should appear on CleanSpark's operational calendar. Items include: quarterly access reviews for production systems, monthly reconciliation of on-chain treasury movements against internal ledger entries, weekly review of hashrate variance versus energy draw, daily verification of pool payout addresses, annual disaster recovery exercise with documented lessons learned, and semi-annual review of insurance coverage for equipment and business interruption.

Each checklist item should have a named owner, evidence location, and ticketing reference. Automation is encouraged where APIs exist for pools, hosts, and explorers. Where manual steps remain, compensating detective controls (e.g., independent spot checks) should be scheduled. This supplement does not imply all items were tested in this assessment cycle.