



ARKIS SYSTEMS

ENTERPRISE NETWORK ADVISORY

FICTIONAL DEMONSTRATION

Network Baseline Review

Northstar Accounting Group

A fictional 35-user professional-services environment created to demonstrate the Arkis reporting approach. No real client, employer, device, or confidential information is represented.

Review date: 2026-07-20

Prepared by: Arkis Systems

Version: 1.0 demonstration

Important notice

This report is a limited operational baseline review based on a fictional scope and fictional information. It is not a penetration test, security audit, compliance assessment, physical wireless survey, or guarantee that any network is secure, resilient, or free from defects.

1. Executive summary

Northstar Accounting Group is a fictional 35-user professional-services firm preparing for a network refresh. The review demonstrates how a small organization can receive a clear inventory, logical diagram, evidence-backed findings, and practical roadmap.

No active critical outage is represented. The most useful improvements are operational: establish reliable configuration backups, plan for failure of the primary access switch, adopt accurate documentation, and align approved software versions during planned maintenance.

The reported meeting-room Wi-Fi concern remains unverified. Controller-visible information is useful, but physical coverage and interference require onsite measurements when remote evidence is inconclusive.

Key priorities

- Implement scheduled configuration backups and confirm a recent file is usable.
- Document recovery from failure of the primary access switch.
- Adopt the updated logical diagram and equipment inventory.
- Align approved software versions during planned maintenance.
- Investigate the meeting-room concern without assigning an artificial severity.

2. Scope and method

Included

- One fictional office with 35 users.
- One firewall or internet gateway, three managed switches, and six access points.
- Four logical VLANs: Corporate, Voice, Guest, and Management.
- Fictional inventory, sanitized configuration excerpts, controller summary, and interview responses.

Excluded

- Penetration testing, vulnerability scanning, and firewall-rule review.
- Formal security, privacy, or compliance assessment.
- Servers, endpoints, cloud applications, and Microsoft 365.
- Physical cabling, power, wireless measurements, failover tests, and implementation.

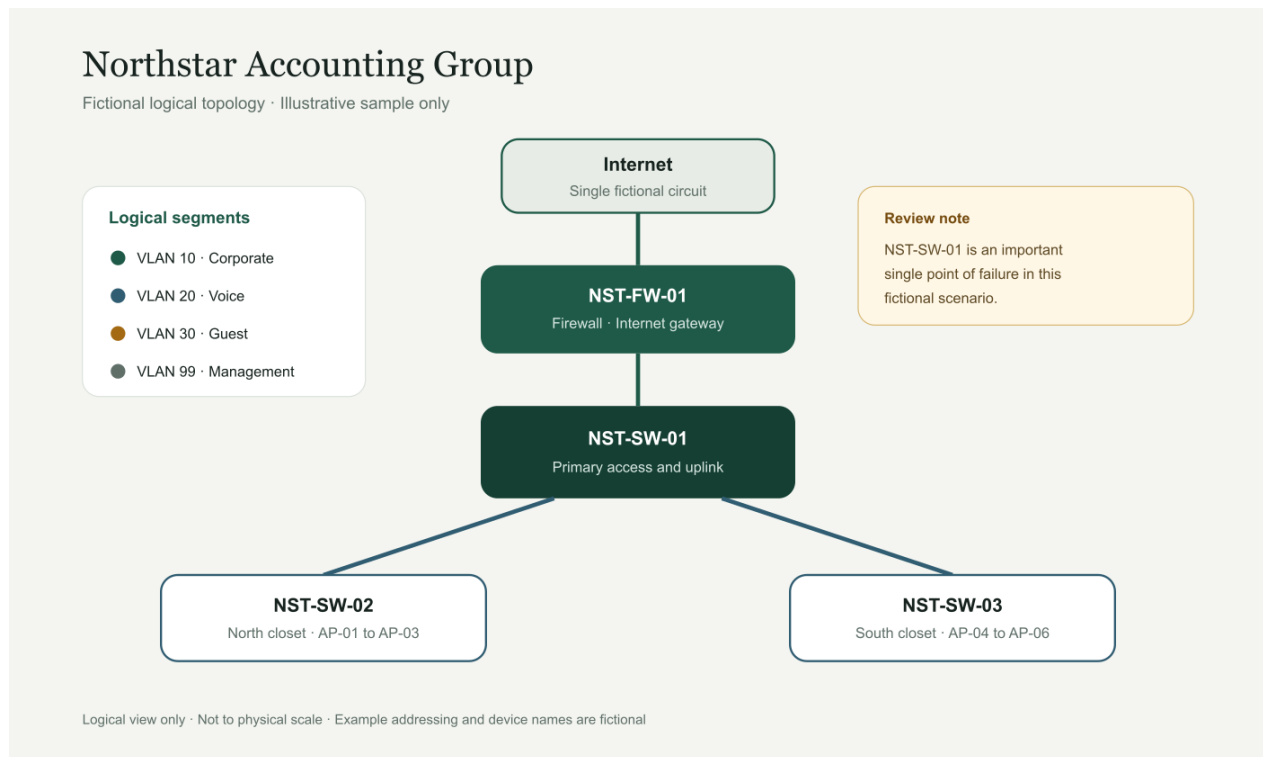
Assessment method

Each relevant checklist item was classified as Pass, Concern, Not Verified, or Not Applicable. Only confirmed concerns receive a severity. The prototype scoring output was then reviewed by a fictional human reviewer. Evidence gaps are kept visible as Further Investigation Required.

3. Environment summary

Area	Fictional baseline
Users / sites	35 users / one office
Internet	One fictional circuit
Firewall	NST-FW-01
Switching	NST-SW-01 through NST-SW-03
Wireless	Six cloud-managed fictional access points
Segments	Corporate, Voice, Guest, and Management
Support model	External IT generalist; no dedicated network engineer

4. Current-state logical diagram



Logical view only. Not to physical scale. All addressing, devices, and relationships are fictional.

5. Detailed findings

NST-001 - Configuration backups are not automated

Final severity	Medium
Category	Backups
Suggested timeline	Within 30 days

Observation: Configuration exports are manual and irregular.

Evidence: Fictional backup checklist and discovery interview.

Why it matters: A recent, identifiable configuration may not be available when a failed or replaced device needs to be restored.

Recommendation: Implement scheduled backups for the firewall and switches. Confirm that a recent backup is readable and incorporate it into a documented recovery procedure.

Limitation: No destructive restore test was performed.

NST-002 - Primary access switch is a single point of failure

Final severity	Medium
Category	Resilience
Suggested timeline	Within 90 days

Observation: Both access switches, the firewall uplink, and important office connectivity depend on NST-SW-01.

Evidence: Fictional topology and configuration relationships.

Why it matters: Failure of the primary switch would interrupt most wired and wireless access until replacement or recovery.

Recommendation: Include practical switching and uplink resilience in the planned refresh. Maintain a tested replacement and recovery procedure appropriate to the organization's size.

Limitation: No physical power or cabling inspection was performed.

NST-003 - Logical network documentation is incomplete

Final severity	Low
Category	Documentation
Suggested timeline	Within 90 days

Observation: The source diagram omits the guest VLAN mapping and one access point.

Evidence: Comparison of fictional source records with the fictional management inventory.

Why it matters: Incomplete documentation increases troubleshooting time and makes project scoping less reliable.

Recommendation: Adopt the updated diagram and inventory. Assign an owner and require updates after material network changes.

Limitation: None beyond the fictional source set.

NST-004 - Two access points run an older maintenance release

Final severity	Low
Category	Lifecycle
Suggested timeline	Within 6 to 12 months

Observation: NST-AP-05 and NST-AP-06 use fictional release 10.4.8 while the other APs use 10.5.1.

Evidence: Fictional controller inventory.

Why it matters: Version inconsistency can complicate support and change planning, although no related fault is confirmed.

Recommendation: Confirm fictional vendor guidance and align approved versions during a planned maintenance window.

Limitation: Versions and vendor guidance are fictional examples.

NST-005 - Meeting-room Wi-Fi concern requires further investigation

Status	Not Verified
Effective severity	Not Rated
Disposition	Further Investigation Required
Category	Wireless

Observation: Users reportedly experience intermittent issues during busy meetings, but the cause has not been confirmed.

Evidence: Fictional user report and limited controller-visible data.

Why it matters: The symptom could relate to capacity, placement, interference, client behaviour, or a non-wireless dependency.

Recommendation: Collect controller data during a representative busy period. If the concern continues, perform onsite measurements before prescribing hardware changes.

Limitation: A remote review cannot confirm physical coverage or interference.

Why this item is Not Rated

A missing or inconclusive evidence base should not be presented as a rated finding. The item stays visible and requires a human-reviewed investigation disposition.

6. Prioritized roadmap

Timeframe	Priority actions
Within 30 days	Schedule device configuration backups; verify a recent file; adopt the updated inventory and diagram.
Within 90 days	Document primary-switch recovery; include resilience in refresh planning; assign a documentation owner; review representative wireless data.
Within 6 to 12 months	Align approved software versions; test a recovery procedure; decide whether internet redundancy is justified.
Further investigation	Use onsite measurements if the meeting-room concern continues after representative controller data is reviewed.

7. Equipment inventory

Device	Role	Location	Software	Backup
NST-FW-01	Internet gateway	Main equipment room	8.4.2	Manual export
NST-SW-01	Primary access / uplink	Main equipment room	17.9.4	Manual export
NST-SW-02	Office access	North closet	17.9.4	Manual export
NST-SW-03	Office access	South closet	17.6.5	Manual export
NST-AP-01 to 04	Wireless access	Office areas	10.5.1	Controller managed
NST-AP-05 to 06	Wireless access	Office areas	10.4.8	Controller managed

All devices, versions, lifecycle labels, and identifiers are fictional.

8. Documentation gaps

- The source logical diagram is incomplete.
- Configuration-backup ownership and schedule are not documented.
- Recovery steps for the primary switch are not documented.
- The meeting-room wireless complaint lacks representative measurement data.

9. Limitations and assumptions

- All content is fictional and exists only to demonstrate the proposed service.
- Physical conditions, wireless coverage, and interference were not inspected or measured.
- No failover, restore, penetration, security, or compliance testing occurred.
- Device support and software versions are fictional examples and not vendor guidance.
- Recommendations require client approval, design validation, backups, testing, and change control before implementation.

10. Conclusion

The fictional environment does not require an enterprise-scale redesign. Its strongest next steps are simple and proportionate: make backups dependable, prepare for failure of the primary switch, maintain accurate documentation, and address version consistency during planned maintenance.

This sample demonstrates the intended Arkis approach: clear evidence, honest limitations, human-reviewed conclusions, and an ordered roadmap rather than unnecessary complexity.

Human-review record

Technical reviewer: Fictional reviewer

Review date: 2026-07-20

Severity overrides: None

Status: Approved as an illustrative fictional sample only