REDCREST SYSTEMS | PORTFOLIO SAMPLE

Infrastructure & Network Risk Assessment

Northstar Manufacturing Group - Fictional Sample

ENGAGEMENT	RC-000123-E01
SCOPE	2 locations | approximately 25 infrastructure assets
ASSESSMENT TYPE	Infrastructure Risk Assessment
PURPOSE	Identify technical risk, business impact, and prioritized remediation

1 EXECUTIVE SUMMARY

Redcrest Systems reviewed the documented network and infrastructure environment to identify operational risk, architecture weaknesses, lifecycle concerns, single points of failure, and opportunities to improve supportability.

OVERALL RISK	**HIGH** - The environment is operational, but resilience, lifecycle, monitoring, and documentation gaps increase avoidable service-disruption exposure.

- Core network contains single points of failure.
- Several devices are approaching or beyond preferred lifecycle.
- Uplink and power redundancy are inconsistent.
- Monitoring is primarily reactive.
- Layer 2 configuration is not consistently standardized.
- Infrastructure documentation does not fully reflect the current environment.

2 ENVIRONMENT SNAPSHOT

Area	Observed Environment
Sites	2
Network devices	Approximately 25
Internet / WAN	Primary circuits with limited path diversity
Switching	Mixed access/distribution architecture
Firewalls	Perimeter firewall pair
Routing	Combination of static and dynamic routing
Monitoring	Basic availability monitoring
Documentation	Partial diagrams and inventory
Redundancy	Inconsistent across critical infrastructure

Assessment conclusions are limited to documentation and evidence made available during the engagement.

3 KEY FINDINGS

R-01 Core Network Single Point of Failure — HIGH

Observation: Critical Layer 3 services depend on infrastructure without complete device, power, and path redundancy.

Business impact: Failure of a core component could interrupt connectivity for users, servers, Internet access, and dependent applications.

Recommendation: Move toward a redundant core/distribution pair with dual power, redundant uplinks, and validated gateway redundancy.

R-02 Aging Infrastructure — HIGH

Observation: Several infrastructure components are approaching or have exceeded preferred lifecycle and support windows.

Business impact: Hardware failure may result in longer recovery times, limited vendor support, and difficulty obtaining replacement components.

Recommendation: Create a lifecycle replacement plan prioritized by support status, business criticality, redundancy, and failure impact.

R-03	Limited Network Monitoring	MEDIUM

Observation: Monitoring provides basic availability visibility but limited capacity trending, configuration awareness, and proactive alerting.

Business impact: Issues may be identified after users experience degradation or service interruption.

Recommendation: Expand monitoring to include interface health, errors, utilization, device health, configuration changes, and trend-based alerting.

R-04	Layer 2 Resiliency and Configuration	MEDIUM

Observation: Spanning-tree and uplink configurations are not consistently optimized for deterministic failover and redundancy.

Business impact: Link or device failures may produce unnecessary service interruption or unpredictable traffic paths.

Recommendation: Standardize Layer 2 design, explicitly define spanning-tree roles, and implement redundant aggregated links where supported.

R-05	Infrastructure Documentation Gaps	MEDIUM

Observation: Available topology diagrams and inventory records do not fully represent the current environment.

Business impact: Incomplete records increase troubleshooting time, change risk, and dependency on individual staff knowledge.

Recommendation: Maintain current logical topology, physical connectivity, device inventory, circuit inventory, and configuration records.

4 PRIORITY REMEDIATION ROADMAP

Window	Primary Objective	Priority Actions
0-30 Days	Stabilize and establish visibility	Validate critical single points of failure; confirm support status; back up configurations; update inventory/topology; confirm monitoring coverage.
30-60 Days	Standardize and design	Develop redundant core architecture; standardize Layer 2/uplinks; define lifecycle priorities; expand monitoring and alerting.
60-90 Days	Execute approved improvements	Begin architecture changes; improve VLAN/subnet organization; establish configuration standards; implement recurring documentation and lifecycle reviews.

5 RECOMMENDED NEXT STEP

The immediate priority is not wholesale replacement. Address failure exposure, unsupported infrastructure, monitoring visibility, and documentation accuracy first. Once these risks are controlled, modernization can proceed through a planned roadmap rather than reactive replacement.

ACTION	Remediate high-risk findings first, then execute the 90-day infrastructure improvement roadmap.

Sample notice: All organizations, infrastructure details, findings, and recommendations in this portfolio sample are fictionalized.