SAMPLE

IT & CYBERSECURITY EXECUTIVE HEALTH CHECK

Northstar Manufacturing, Inc.

Fictitious client used for demonstration purposes

RED	YELLOW	GREEN
3	5	6
Critical / High Risk	Needs Attention	Good / Effective

Prepared by YOUR NAME

Fractional IT Director & Cybersecurity Advisor

Assessment date: SAMPLE DATE

EXECUTIVE SUMMARY

Overall posture: YELLOW - material risks are manageable, but several require prompt action.

Northstar Manufacturing has a generally functional technology environment with several sound controls in place. However, the assessment identified three areas that create meaningful business risk: privileged Microsoft 365 access without phishing-resistant controls, backups that have not been independently restore-tested, and an aging perimeter firewall approaching end-of-support.

None of these findings indicates an active breach. The concern is resilience: a compromised administrator account, failed recovery during ransomware, or unsupported perimeter equipment could create disproportionate operational impact if an incident occurs.

Executive scorecard

Domain	Status	Executive assessment	Priority
Identity & Access	**RED**	Administrative access needs immediate strengthening.	Immediate
Backup & Recovery	**RED**	Backups exist, but recoverability is not proven.	Immediate
Network / Firewall	**RED**	Perimeter hardware lifecycle creates support risk.	30 days
Email Security	**YELLOW**	Core controls present; DMARC and impersonation protection can improve.	30-60 days
Endpoint Security	**GREEN**	Managed endpoint protection and patching appear effective.	Maintain
Business Continuity	**YELLOW**	Recovery responsibilities and testing cadence need formalization.	60 days
Vendor / MSP Oversight	**YELLOW**	Responsibilities exist but service verification is informal.	60 days
Policies / Documentation	**YELLOW**	Key procedures exist but are incomplete or inconsistent.	90 days

PRIORITY FINDINGS

RED findings - address first

Red findings represent conditions that could materially increase the probability or impact of a security incident, prolonged outage, failed recovery, or compliance/cyber-insurance issue.

R-01

Privileged Microsoft 365 accounts need stronger authentication

Business impact

Administrative accounts currently use standard MFA methods that remain susceptible to modern phishing and session theft. A compromise of a privileged account could allow an attacker to alter security settings, access mailboxes, create persistence, or interfere with recovery.

Recommended action

Require phishing-resistant authentication for privileged roles, maintain separate administrator accounts, reduce standing global administrator access, and verify emergency access accounts.

Owner: Management + MSP | Target: 0-14 days | Severity: Critical

R-02

Backup recoverability has not been independently validated

Business impact

The organization has scheduled backups, but there is no recent documented full restore test. Successful backup jobs do not prove that systems, applications, permissions, and critical data can be restored within acceptable timeframes.

Recommended action

Perform a documented restore exercise for at least one critical workload. Record actual recovery time, recovery point, dependencies, failures, and corrective actions. Establish quarterly or semiannual restore testing.

Owner: IT Provider | Target: 0-30 days | Severity: High

R-03

Perimeter firewall lifecycle / support risk

Business impact

The primary firewall is approaching a support or lifecycle milestone. If hardware fails or a critical vulnerability is discovered after support lapses, replacement options and vendor assistance may be limited during an outage.

Recommended action

Confirm exact support dates, firmware eligibility, configuration backup, spare/replacement plan, and budget. Replace or renew before support expiration.

Owner: Management + IT Provider | Target: 0-30 days | Severity: High

SUPPORTING FINDINGS

YELLOW findings - plan and improve

Finding	Why it matters	Recommended action	Target
Y-01 **DMARC policy is monitoring-only**	Email authentication is configured, but the domain is not yet enforcing a quarantine/reject policy.	Validate legitimate senders, monitor reports, then move gradually toward enforcement.	30-60 days
Y-02 **Disaster recovery responsibilities are not formally assigned**	Recovery depends on several people and vendors, but there is no concise management-level ownership matrix.	Document who declares an incident, who contacts vendors, who owns business priorities, and who communicates internally.	30-60 days
Y-03 **MSP service verification is largely trust-based**	The provider performs recurring services, but management receives limited evidence that restore tests, privileged-account reviews, and other controls are occurring.	Add a quarterly IT governance review with a short evidence-based scorecard.	60 days
Y-04 **Onboarding/offboarding process is not consistently documented**	Account creation and termination occur, but the process relies on email and institutional knowledge.	Create a single checklist covering accounts, licenses, devices, access groups, MFA, forwarding, ownership and termination verification.	60-90 days
Y-05 **Technology lifecycle planning is reactive**	Several infrastructure replacements are triggered by failure/support deadlines rather than a multi-year lifecycle plan.	Maintain a 24-36 month technology roadmap and budget forecast.	90 days

GREEN findings - retain and verify

G-01 Managed endpoint security	Endpoint protection is centrally managed and appears consistently deployed.
G-02 Patch management	Workstations and supported servers receive managed operating-system updates.
G-03 Security awareness	Employees receive recurring awareness training and phishing exercises.
G-04 Network equipment security	Core network equipment is located in restricted areas with UPS protection.
G-05 Documented ISP / vendor contacts	Key connectivity and technology vendor contacts are available for escalation.
G-06 Separate guest wireless access	Guest traffic is segmented from primary business resources.

ACTION PLAN

30 / 60 / 90-day remediation roadmap

The purpose of the roadmap is to turn the assessment into a short, accountable management plan. Dates should be adjusted to the organization's operational calendar and approved budget.

FIRST 30 DAYS

- Strengthen privileged Microsoft 365 authentication and administrator account design.
- Complete and document a representative backup restore test.
- Confirm firewall support/end-of-life dates and approve replacement/renewal path.
- Assign a named owner and due date to every Red and Yellow finding.

BY 60 DAYS

- Move email authentication toward DMARC enforcement after validating legitimate senders.
- Document disaster-recovery roles, escalation contacts, and business recovery priorities.
- Hold the first quarterly IT governance meeting with management and the IT provider.
- Formalize onboarding/offboarding workflow and verification.

BY 90 DAYS

- Publish a 24-36 month technology lifecycle and budget roadmap.
- Review open findings and document accepted residual risks.
- Establish a recurring restore-test schedule and quarterly security/IT scorecard.
- Schedule the next independent executive technology review.

Suggested quarterly management metrics

✓ Critical findings overdue	✓ Backup restore test status
✓ Privileged accounts reviewed	✓ Security incidents / material alerts
✓ Unsupported systems / lifecycle risks	✓ Open cyber-insurance requirements
✓ Top 3 upcoming IT investments	✓ MSP commitments completed vs. outstanding

APPENDIX

Scope, methodology & assessment boundaries

This sample illustrates the style and management-level output of an Independent IT & Cybersecurity Health Check. A real engagement is tailored to the client environment and may include interviews, documentation review, configuration review, screenshots/evidence supplied by the IT provider, and selected technical validation.

Typical assessment areas

- Identity and access management
- Microsoft 365 / Google Workspace security
- Email authentication and anti-phishing controls
- Endpoint protection and patch management
- Firewalls, VPNs, networks and Wi-Fi
- Backups, restore testing and disaster recovery
- Vendor/MSP responsibilities and escalation
- Technology lifecycle, licensing and budgeting
- Onboarding/offboarding and documentation
- Cyber-insurance readiness and security policies

Rating definitions

RED	**Material concern**	Requires prompt remediation, compensating controls, or explicit management risk acceptance.
YELLOW	**Needs attention**	Control exists but is incomplete, inconsistent, aging, undocumented, or should be improved.
GREEN	**Good / effective**	Control appears appropriate for the assessed environment; continue and periodically verify.

Important limitation

This assessment is an executive risk review, not a guarantee that a system is secure and not a substitute for a formal penetration test, legal opinion, regulatory audit, or compliance certification. Findings are based on the scope, evidence, access, and representations available at the time of review. Technology conditions can change after the assessment date.

For a real client report, this section should also document systems excluded from scope, evidence that could not be validated, and any assumptions relied upon.

YOUR NAME | YOUR_EMAIL | YOURDOMAIN.COM