IT Ops Assessment Report

Prepared for: **Company Name**

Address: Sofia, 1000

Country: Bulgaria

Session: sample

Generated: 2026-04-11T02:24:16.291150Z

Prepared by: **ZLefterov IT**

Email: zhivko@zlefterov.com

Website: https://zlefterov.com

Overall score	**48%**
Risk level	Moderate operational risk
Purchased areas	Access Control & Data Security, Business Risk & Recovery, Software Costs & Wasteful Spending

Executive summary

This report prioritizes interpreted findings and business impact. A supporting evidence appendix at the end references selected answers.

How to read this report

Each area includes interpreted findings and recommended actions. The appendix lists selected Q/A with a short business-oriented suggestion for each answer.

Top priorities

- Recovery testing is missing for critical systems.
- Access control is inconsistent across tools.
- License spend is not routinely optimized.

Key findings by area

Access Control & Data Security

Score: **42%** — Moderate operational risk.

High-impact access gaps

Access is not consistently managed via roles/groups, increasing the chance of oversharing and lingering privileges.

Limited accountability

Without periodic reviews, privileged accounts tend to accumulate and become hard to audit.

Recommended actions

- Enable MFA for all key systems and email.
- Create role-based groups (e.g., Sales, Finance, Admin) and assign access via groups.
- Run a monthly review of privileged access and remove dormant accounts.

Business Risk & Recovery

Score: **35%** — High operational risk.

Recovery is untested

Backups that are not regularly restored and verified often fail when you need them most.

Recommended actions

- Define RPO/RTO for the top systems and document a short recovery runbook.
- Test a restore quarterly and keep evidence (date, systems, outcome).

Software Costs & Wasteful Spending

Score: **68%** — Moderate operational risk.

Hidden subscription creep

Tools tend to accumulate over time; even small monthly waste compounds across teams.

Recommended actions

- Create a simple monthly license audit (owner, seats, usage).
- Introduce approval for new tools and a quarterly rationalization review.

Appendix: supporting evidence

The items below reference selected answers that informed the findings. Each includes a short observation and a suggested next step.

Access Control & Data Security

- **Q:** Do you enforce MFA for email and admin accounts?
  A: Not consistently
  Observation: This suggests partial coverage; the business is exposed during phishing or password reuse incidents.
  Suggested next step: Roll out MFA to all users first, then tighten policies for admin roles.

Business Risk & Recovery

- **Q:** When was your last successful restore test?
  A: Not sure
  Observation: This indicates a high likelihood of extended downtime during incidents.
  Suggested next step: Schedule a 60-minute restore test this month for 1 critical system (email or accounting).

Software Costs & Wasteful Spending

- **Q:** Do you review and reclaim unused licenses?
  A: Sometimes
  Observation: This suggests savings exist but aren't captured consistently.
  Suggested next step: Assign an owner and run a 15-minute monthly check on your top 10 subscriptions.