



BOHIOSYSTEM

• INFRASTRUCTURE CHECKLIST • BOHIOSYSTEM

Infrastructure Checklist

The checklist we apply on every assessment. It also works as an internal self-diagnostic.

DOCUMENT

BS-SVC-07B

VERSION

1.0

DATE

August 1, 2026

PREPARED BY

BohioSystem

BohioSystem

bohiosystem.dev • Confidential

SELF-DIAGNOSTIC

This is the actual list we use when we walk into an organization. You can go through it yourself: every "no" is a risk that already exists, whether you are measuring it or not.

This is not a sales questionnaire. If most of the answers come out affirmative, you probably do not need to hire us, and that is exactly what we will tell you.

6

REVIEW AREAS

48

CONTROL POINTS

1 session

TYPICAL DURATION

Report

WRITTEN DELIVERABLE

01

Inventory and documentation

Assets

- An up-to-date inventory of servers and network equipment exists.
- Every asset has an assigned owner.
- End-of-support dates are known.
- Contracts and warranties are recorded along with their expiration dates.

Access

- Credentials live in a corporate password manager.
- There are no accounts shared between people.
- Access for departing staff is revoked.
- An emergency access procedure exists.

Documentation

- A current network diagram exists.
- The rack and cabling are labeled.
- A matrix of services and their dependencies exists.
- Documentation was updated within the last six months.

Vendors

- It is known who to call for each system.
- Contract numbers are accessible outside the system itself.
- An escalation path is defined with each vendor.
- Contracted response times are known.

02

Backup and continuity

Coverage

- What is backed up and what is not is clearly defined.
- Frequency reflects an agreed acceptable data loss window.
- Configurations are backed up too, not just data.
- An off-site copy exists.

Protection

- Copies are immutable or isolated.
- An encryption (ransomware) attack could not reach the backups.
- Access to the copies is restricted.
- Enough history is retained to detect delayed corruption.

Verification

- A successful restore was performed within the last six months.
- The test was documented along with its actual duration.
- Someone reviews backup failure notices.
- An alert exists if a backup does not run.

Continuity

- A written recovery plan exists.
- Target recovery times are defined.
- A full scenario has been rehearsed.
- The plan states who decides and who is notified.

03

Network and connectivity

Design

- The network is segmented by function.
- The guest network is isolated from the corporate network.
- Operational technology devices sit in their own segment.
- Controls exist between segments, not only at the perimeter.

Availability

- A secondary internet link exists.
- Failover has been tested.
- Critical equipment has redundant power.
- Spares exist for critical network equipment.

04

Servers, power and physical environment

Servers

- Operating systems receive current updates.
- Patches are applied on a defined schedule.
- Production and test environments are separated.
- Capacity is reviewed periodically.

Environment

- Server room temperature is monitored.
- Physical access is controlled and logged.
- Smoke or fire detection is in place.
- The room is not used as storage.

Power

- Power systems cover the real load.
- Batteries were tested within the last year.
- Automatic orderly shutdown exists.
- Runtime autonomy or a generator is available for extended outages.

Monitoring

- Availability, disk, memory and load are monitored.
- Alerts reach someone who acts on them.
- A warning threshold exists before the critical point.
- History is retained to analyze trends.

05

How to interpret the result

SITUATION	READING
More than 80% affirmative	Infrastructure is well managed. The remaining work is optimization, not risk. You probably do not need an intervention.
Between 50% and 80%	A reasonable foundation with specific gaps. Usually resolved with a bounded project targeting the two or three weakest areas.
Less than 50%	Real operational risk, probably underestimated. Best to start with inventory and backup before any other improvement.
Any "no" in backup	Gets addressed first, regardless of the rest of the result. It is the only point where a failure can be irreversible.

THE MOST REVEALING QUESTION

When was the last time you restored a full backup, and how long did it take? If the answer is "never" or "I would not know," the continuity plan is an assumption, not a plan.

Let's talk

NEXT STEP

Write to us and we'll schedule a working session at no cost to review your specific case.

CONTACT

contacto@bohiosystem.dev

WEB

bohiosystem.dev

DOCUMENT

BS-SVC-07B · v1.0