

EXECUTIVE DIAGNOSTIC

Key-Person Dependency Self-Check

A practical guide for identifying responsibilities, relationships, approvals, and knowledge concentrated in too few people.

THIS RESOURCE HELPS YOU

- Recognize dependency before absence, transition, or growth exposes it.
- Prioritize documentation, access, cross-training, and delegation.
- Protect continuity without creating unnecessary redundancy.

Where key-person dependency hides

Critical relationships and institutional knowledge

One person carries context, trust, history, or external relationships that others cannot access.

Approvals and decision authority

Routine work repeatedly waits for the same person because authority has not been distributed or defined.

Recurring processes and technical tasks

Only one person knows how to complete an important workflow, troubleshoot exceptions, or operate a system.

Access to files, systems, and reporting

Credentials, reports, shared folders, or data access are concentrated in one account or one individual.

Informal problem-solving

The team relies on one person to remember exceptions, resolve unusual cases, or connect disconnected parts of the work.

Warning signals to take seriously

Work pauses during ordinary absence

If a routine vacation stops critical work, the organization has a continuity gap.

Only one person can explain the process

Knowledge has not been transferred into a usable operating structure.

Everything escalates to the same leader

Authority or judgment is concentrated beyond what the work actually requires.

The same person owns the relationship and the data

A transition could remove both context and access at the same time.

Documentation exists but nobody uses it

The apparent backup is not a real backup until another person can execute the work from it.

Reduce dependency in the right order

1. Identify the highest-consequence dependency

Prioritize the dependencies that could stop critical work, weaken reporting, or disrupt key relationships.

2. Create backup access

Ensure another authorized person can reach the essential systems, files, credentials, and records.

3. Capture critical knowledge

Document the operating steps, decisions, exceptions, and context another person would need.

4. Cross-train and delegate

Move routine decisions and recurring work to appropriate roles rather than keeping everything as backup knowledge.

5. Test continuity

Use planned absence or role rotation to confirm that the work can continue without the key person intervening.