Push Work to the Business. Keep the Audit Trail.

Routine role changes, password resets, and access requests all funnel through a central IT team that cannot keep pace, so backlogs grow and SLAs slip while people wait for access. Delegating those tasks to managers or the help desk usually creates new risk: over-provisioned helpers, shared credentials, and broken audit trails. This blueprint shows how to move the work to the people closest to it without weakening governance or losing the audit trail.

1. What to Delegate

Bounded & repeatable tasks

- **Password resets & unlocks**
- **Group & team membership changes**
- **Scoped entitlement grants & revokes**
- **Joiner / mover / leaver steps**
- **Access-request approvals**

2. Define the Rules

Bounded & repeatable tasks

- **Grant the task, not the app.** Delegates run a specific action, never broad access to the underlying application.
- **Scope to their domain.** Tie each delegate to the OU, team, or business unit they already own, so they can only act within it.
- **No credentials, ever.** The delegate triggers the task through a form; the secret stays vaulted and is never seen or shared.
- **Time-box and expire.** Grant delegation for as long as the role requires it, not indefinitely, so authority does not accumulate.

3. Stay Audit-Ready

Prove it on demand

- **Capture every action.** Each task run is logged end to end: who initiated it, what changed, and when.
- **Record the full detail.** Inputs, outcome, and the identity behind the change are retained, not just that something happened.
- **Keep it accessible.** Pull the complete history on demand from a single audit log, ready for review at any time.
- **Review delegation on a schedule.** Confirm who holds delegated access and whether they still need it.

The Governance Guardrails

RBAC & Least Privilege
Delegates see only the tasks and resources they're permitted to touch — nothing more.

No Privilege Exposure
Dynamic forms let non-technical staff act without ever seeing backend scripts or secrets.

Full Audit Trail
Every execution is recorded end-to-end, ready for compliance review at any time.

How READI Closes the Gap with Access Studio & Bot Studio

Safe Delegation by Design
Access Studio surfaces only the data a task requires and nothing more. Delegates act through a focused interface with no exposure to underlying scripts, credentials, or secrets, so non-technical staff run privileged tasks without privileged access.

Move Work to the Business
Access Studio shifts approvals and administration to the owners closest to the work — without weakening governance or losing the trail.

Least-Privileged Execution
Tasks run under RBAC with credentials secured in the READI key vault, triggered via API, REST, or PowerShell.

Compliance Built In
Every task run is captured end to end: who initiated it, what changed, and when. The complete history is retained and available on demand from a single audit log, producing review-ready evidence whenever it is needed.

Scan for more information on
www.readibots.com | Linkedin