Can This Legacy Application Be Safely Retired?

A 1-page shutdown readiness assessment for government IT leaders reducing cost, risk, and application dependency

Legacy applications often survive modernization when no one can prove what happens to required information after shutdown. Use this assessment to determine whether the business can safely live without the application.

APPLICATION SNAPSHOT

Application / System: _____

IT Owner: _____

Business Owner: _____

Records Officer: _____

Primary data / records / reports: _____

Last active business use: _____

Annual cost to maintain: $ _____

Reason for review:

☐ Cost ☐ Security ☐ End of support ☐ Modernization

☐ Vendor ☐ Compliance ☐ Other

HIGH-RISK SHUTDOWN SIGNALS

- ☐ No confirmed business owner
- ☐ Unknown reports / workflows / integrations
- ☐ Users still search app for old information
- ☐ Data only makes sense inside original app
- ☐ Metadata, history, or context may be lost
- ☐ Permissions cannot be replicated
- ☐ Retention schedule or disposition rules unclear
- ☐ FOIA, audit, legal, or legislative requests depend on it
- ☐ Kept live mainly "just in case"
- ☐ High annual maintain/support cost
- ☐ Unsupported, insecure, or vendor-dependent

3+ signals = controlled retirement project, not a simple shutdown

SHUTDOWN READINESS TRIAGE

Check Yes, No, or Unknown. Then use the Decision Guide to choose the retirement path.

1. Business Dependency

	Y	N	?
Teams / departments / processes still using app are known.	☐	☐	☐
Reports / workflows / integrations / exports are known.	☐	☐	☐
Business owner confirmed what must remain available.	☐	☐	☐

2. Information Requirements

	Y	N	?
Records covered by a retention schedule are identified, with duration and disposition known.	☐	☐	☐
Metadata, history, relationships, and context can be retained.	☐	☐	☐
Keep vs delete/dispose information can be separated.	☐	☐	☐

3. Post-Shutdown Access

	Y	N	?
Users can search, retrieve, and use information without app.	☐	☐	☐
FOIA, audit, legal, and records requests can be answered.	☐	☐	☐
Permissions and access controls can be maintained/redesigned.	☐	☐	☐

4. Cost and Risk

	Y	N	?
Annual licenses, hosting, maintenance, support, and staff time are known.	☐	☐	☐
App creates security, compliance, vendor, or unsupported tech risk.	☐	☐	☐
Main reason it remains live is access to historical information.	☐	☐	☐

DECISION GUIDE: CHOOSE THE RETIREMENT PATH

Quick rule: Unknown dependency = Discovery Required. No/Unknown in information or access = Access Plan Required. Active critical use = Not Ready.

Ready to Retire

Use when: Mostly Yes; low dependency; required information is understood; access is clear.

Next: Plan validation, sign-off, and shutdown.

Access Plan Required

Use when: App can go, but information must stay searchable, secure, auditable, and usable.

Next: Define what stays accessible, who needs it, and how access works.

Watch out: File exports lose metadata/context; read-only instances keep cost/risk; backups are not searchable or audit-ready. An access plan is not a storage plan.

Discovery Required

Use when: Ownership, usage, retention, permissions, reports, or exports are unclear.

Next: Complete targeted discovery before setting a date.

Not Ready to Retire

Use when: App still supports active processes, reporting, integrations, or critical access.

Next: Document blocker and resolution plan.

FINAL SHUTDOWN READINESS TEST

After shutdown, can required information still be found, accessed, secured, and used to answer audit, legal, compliance, records, or public records (FOIA) requests without recreating the risk the agency is trying to retire?

SHORTCUT CHECK

If the plan depends on a file share, backup, or license the agency still has to maintain, the test fails.

Most applications that fail this assessment fail on access, not shutdown. Solving access first turns a risky retirement into a controlled one.