Critical Account Recovery Planning Worksheet

Plan legitimate recovery for one essential account without recording credentials or recovery codes.

How to use these four pages

1. Choose an essential account and the business activity it supports.

2. Identify the authorised owner, recovery process and dependencies.

3. Agree a safe technical check with the appropriate owner or provider.

4. Record the evidence, open questions and next review trigger.

A practical working aid

Use the blank records for your own discussion. Examples are fictional, not client case studies. Print to complete by hand or adapt the prompts in your own document; this PDF is not a fillable form.

Keep completed records confidential. Use references to protected evidence rather than passwords, customer records or sensitive system details.

Online instructions and companion article

Read the guide

Read the article

Source guidance

NIST SP 800-63B-4: Authentication and Authenticator Management

CISA: Implementing Phishing-Resistant MFA

Resource content reviewed 19 November 2026. The source material informs the approach; no endorsement is implied. This worksheet supports planning and record-keeping. It does not authorise testing, certify compliance or replace an agreed specialist review.

Free to use and adapt within your business with the GRCPreneur acknowledgement retained.

A fictional worked example

Illustrative entries only. No real client, vendor result or completed implementation is claimed.

Record	Illustrative entry
Account	Domain administration for a fictional consultancy.
Business dependency	The domain supports access to customer-facing services.
Current arrangement	An occasional contractor holds the listed recovery phone.
Uncertainty	The owner has not agreed the contractor's departure arrangements.
Next step	Authorised administrator proposes a business-controlled recovery route.
Evidence status	Planning only; no transfer or successful recovery is claimed.

Before using the blank pages

Agree who will review the record and what decision it supports. Mark assumptions, proposed actions and unverified claims clearly. Copy pages 3 and 4 when you need more space.

Your working record

Project / record ID: _____ Date: _____

Account, service and owner

Name the account category and authorised business owner; no login details.

Recovery process and dependencies

Provider instructions, responsible people and protected record references.

Unavailable device, person or service

Identify loops or shared dependencies that could prevent legitimate recovery.

Proposed check and authority

Expected result, authorisation, safe transition and technical owner.

Evidence, open items and review

What was demonstrated? What is unverified? Name the next owner and trigger.

Use protected evidence references. Do not enter credentials or confidential customer details.

Recovery checks and follow-up

Related record / requirement: _____ Review date: _____

Dependency / question	Protected evidence reference	Owner / due date	Result / next step

Review before the next decision

- No passwords, tokens or recovery codes appear in this record.
- The recovery process and authorised owner are identified.
- Planned checks remain distinct from completed results.
- Changes have an owner, safe transition and review trigger.

Decision, authority and next checkpoint

Proceed / revise / defer / stop. State the decision scope, conditions, approver and date.

A completed record documents a review. Approval applies only to the stated scope and does not establish that untested work has succeeded.