How to Prepare an Asset List for IT Recovery

An asset list helps your team identify what must be restored after an outage, cyber incident, equipment failure, or other disruption. This guide focuses on the technology and supporting resources needed to restore IT services. It can be adapted to include physical assets or broader business continuity needs.

A useful list records more than asset names: it shows which business services rely on each asset, who is responsible for it, what it depends on, and how it can be recovered.

1. Set the scope

Decide what the list covers, such as a business unit, office, application environment, or the whole organization. Include the assets needed to keep essential services running, such as:

- Applications, servers, databases, and cloud services
- End-user devices, network equipment, and security tools
- Business data, configuration files, and software licenses
- Connectivity, power, and other supporting services
- Key suppliers or external services

Record the scope, list owner, and date of the last review.

2. Identify critical services

Start with the business activities that must continue or resume quickly. For each service, record what it does, who relies on it, the impact if it is unavailable, and any legal, contractual, or safety requirements.

Identify the assets that support each service. An asset's importance depends on the services it enables and its dependencies, not just its cost or technical complexity.

3. Set recovery priorities

Agree on recovery targets with the people responsible for each business service:

- **Recovery time objective (RTO):** the target time to restore a service before its unavailability has an unacceptable effect on business operations.
- **Recovery point objective (RPO):** the latest point in time to which data must be recoverable after an outage. It determines how much recent data the organization can afford to lose.

Use those targets, the impact of downtime, and the dependencies between assets to group services into recovery tiers. For example, Tier 1 could cover services that must be restored first to protect safety or essential operations; Tier 2 could cover services needed soon afterward; and Tier 3 could cover services that can wait longer. Define the tiers and their target recovery times to fit your organization.

Then identify which assets must be restored first to support each tier. Confirm that foundational services—such as identity, network access, backups, and security monitoring—can be recovered before the systems that rely on them.

4. Record the essential details

Use a consistent template. Create one row per asset, and link assets to the business services they support.

Field	What to record
Asset name and type	Clear name and whether it is an application, device, data set, service, or facility
Identifier and location	Asset tag, hostname, account or tenant, physical location, or cloud region
Business service and priority	The service it supports and the agreed recovery tier
Owner and recovery contact	The person or team accountable for the asset and who can help restore it
Dependencies	Systems, data, suppliers, credentials, network links, or facilities it needs
RTO and RPO	The agreed service restoration target and latest point in time to which data must be recovered, if defined
Recovery method	Backup location, replication, rebuild instructions, replacement process, or supplier support
Access and licensing	Required accounts, permissions, keys, certificates, and license details
Last recovery test	Test date, result, and any unresolved issues
Status and review date	Whether the details have been verified and when they were last checked

Illustrative example

Field	Example entry
Asset and service	Payroll application supporting payroll processing
Priority and owner	Tier 1; Payroll systems lead
Dependencies	Identity service, payroll database, cloud tenant
RTO and RPO	4-hour RTO; 1-hour RPO (illustrative values only)
Recovery method	Restore from a tested backup, redeploy the application, and validate a payroll run

The target values are illustrative only. Agree actual targets with the business service owner.

Do not put passwords, private keys, or other secrets directly in the list. Record where authorized responders can retrieve them securely.

5. Map dependencies and recovery order

For each critical service, trace the chain of assets required to restore it. For example, an application may depend on identity services, network connectivity, a database, cloud access, and a third-party provider.

Use this dependency map to confirm the recovery order. Check whether supporting services can be restored in time to meet the service's RTO and RPO. If the order or targets are not achievable, record the gap and agree on an action.

6. Verify recovery arrangements

An asset is not recovery-ready just because it appears on the list. Check that:

- Backups or replacement resources exist and authorized responders can access them
- Recovery instructions are current and understandable
- Required people, permissions, licenses, and supplier contacts are available
- Restoration steps have been tested at an interval set by your organization's risk and policy requirements
- Test results show that recovery targets can be met
- Gaps have an owner and due date

Record the date and outcome of each test, along with unresolved issues and follow-up actions.

7. Protect and maintain the list

The list may reveal system locations, dependencies, contacts, and recovery procedures. Store it with access limited to people who need it for recovery. Protect offline or independent copies with appropriate access controls, and make sure authorized responders can reach them if the primary storage location is unavailable.

Assign an owner and set a review schedule based on risk, policy requirements, and how quickly the environment changes. Record the chosen review interval. Update the list when systems, suppliers, locations, responsibilities, or recovery arrangements change. Also review it after a recovery test or incident. Ask asset owners to confirm their entries periodically.

8. Use the list during exercises and incidents

During a recovery exercise, use the list to identify assets, contacts, dependencies, and restoration steps. Record what was missing or inaccurate, update the list, and assign follow-up actions. During an incident, use it as a starting point and verify current conditions before taking recovery actions.

Completion checklist

- [ ] Scope, list owner, and review date are recorded
- [ ] Critical services and their supporting assets are identified
- [ ] Recovery tiers, RTOs, and RPOs are agreed where needed
- [ ] Owners, contacts, and dependencies are documented
- [ ] Recovery order is understood
- [ ] Backup or rebuild methods are confirmed
- [ ] Access details are stored securely
- [ ] Recovery tests, results, and open issues are recorded
- [ ] The list is protected and available to authorized responders
- [ ] Review interval, triggers, and follow-up actions are recorded

Reminder: An asset list supports recovery planning; it does not replace tested backups, incident procedures, or business continuity plans.