ITMANAGEMENT101.CO.UK

IT disaster recovery plan

Template, runbooks, test log and a worked example for a small business

A business continuity plan keeps the business running. This plan is the IT part of it: how each system and its data come back, in what order, by whom, and the evidence that it works. Fill in the blank pages, print the emergency card and keep a printed copy away from the office, because the systems that hold this document may be the ones that are down.

Three numbers for every system

Number	What it means	Where it goes
Target	What the business needs: the recovery time objective (RTO) and recovery point objective (RPO), taken from the business continuity plan.	RTO and RPO columns
Capability	What your set-up can actually do: how often the data is copied, where the copies live, and how long a restore takes.	Copied every, copies, restore time
Proof	The date someone last restored it and timed it. Without a date, the capability is a guess.	Last test and the Test log

Recover in five layers, in this order

Layer	What it covers	Why it comes here
1. Keys	Admin accounts, the password manager, multi-factor authentication (MFA) devices, the backup console login.	Nothing else can be restored by someone who cannot sign in.
2. Pipes	Internet line, Wi-Fi, firewall, DNS (the internet's address book) and phones.	Restores from the cloud and cloud apps both travel down the pipe.
3. Data	The copies themselves: files, mailboxes, databases, system images.	An application with no data is an empty shell.
4. Apps	Line-of-business systems, cloud (SaaS) services, the monitoring platform.	Apps sit on top of keys, pipes and data.
5. Desks	Laptops, desktops and the people at them: rebuilt, signed in, told what to do.	Last, because a working laptop is no use until there is something to connect to.

How to fill it in

1. Take each system's RTO and RPO from your business continuity plan.
2. Fill in the system register honestly: how often each is copied, where the copies are, and the last time anyone restored it.
3. Write a runbook for each system that has a short RTO or no restore test. Use the rules: a verb, a place, a check, a clock.
4. Test, and write every test in the log. A gap you find in a test is a success.

Latest version, the Excel workbook and the guide: https://www.itmanagement101.co.uk/disaster-recovery-plan-template/

© Garrould Limited · CC BY-NC 4.0 · Share for non-commercial use with a link to https://www.itmanagement101.co.uk/disaster-recovery-plan-template/

1. Plan details and scope

Item	Entry
Organisation	
Plan owner (declares an IT disaster)	
Deputy	
Technical lead / deputy	
Version and date	
Next review date	
Where printed copies are kept	
Business continuity plan (title and location)	

Scope: this plan restores IT systems and data. Keeping the business running while they are down (people, premises, suppliers, workarounds) is in the business continuity plan.

2. When to invoke this plan

• A system on the register will stay down longer than its RTO, or already has.

• Data has been lost, encrypted or deleted beyond what a user can undo.

• Nobody can sign in as an administrator.

• The business continuity plan has been invoked and an IT system is part of the cause.

Only the plan owner, or the deputy if the owner cannot be reached within 15 minutes, declares an IT disaster. Record the time.

3. System register

System	Layer	RTO	RPO	Copied every	Copies / offsite / offline	Measured restore	Last test	Runbook

© Garrould Limited · CC BY-NC 4.0 · Share for non-commercial use with a link to https://www.itmanagement101.co.uk/disaster-recovery-plan-template/

4. Backups: the questions to answer

☐ How many copies of each system's data exist, including the live one? (aim: 3)

☐ Are they on at least two different kinds of storage or service? (aim: 2)

☐ Is at least one away from the office? (aim: 1)

☐ Is at least one offline, or locked so it cannot be changed, and with logins that the everyday admin accounts cannot use?

☐ Is 2-step verification on for every backup account?

☐ Who checks the backup jobs ran, and how often?

☐ When was each last restored, and how long did it take?

5. Access and contacts

Role	Primary	Deputy	Mobile	Personal email
Plan owner				
Technical lead				
Keys holder				
Communications				
Data protection				

Supplier	Support number	Account reference	Contracted response

Emergency admin cards kept at: _____ Password manager recovery kit kept at: _____

© Garrould Limited · CC BY-NC 4.0 · Share for non-commercial use with a link to https://www.itmanagement101.co.uk/disaster-recovery-plan-template/

6. Runbook

One per system or scenario. Write it for the deputy, not for yourself. Every step has:

• A verb: Every step starts with something to do: open, sign in, restore, check, ring.

• A place: Where it happens: the console, the menu path, the cupboard, the phone number.

• A check: What you should see when it worked, so the reader knows to move on.

• A clock: Roughly how long the step takes, so the person running it can tell when something is wrong.

Runbook ID and title	Use it when	Owner / deputy	Last walked through

#	Do this (start with a verb)	Where	You should see	Min
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				

© Garrould Limited · CC BY-NC 4.0 · Share for non-commercial use with a link to https://www.itmanagement101.co.uk/disaster-recovery-plan-template/

7. Test log

Pass means the target was met AND the owner of the data confirmed it was complete.

Date	System / runbook	Test type	Target	Achieved	Pass / fail	What we changed

Test types

Test	How	How often
File restore spot check	Pick a random file or email from last week and get it back. Ten minutes; proves the backup job is still running.	Monthly
Timed system restore	Restore one system to a spare location (not over the live copy), time it from start to a user confirming it works.	By tier: 3, 6 or 12 months
Deputy walk-through	The deputy, not the usual person, follows one runbook step by step. Every question they ask is a missing line.	Every 6 months
Emergency admin sign-in	Sign in with each break-glass (emergency access) account and confirm the alert fired.	Every 90 days and when IT staff change
Scenario exercise	Talk a scenario through with the people named in the plan; for a cyber attack, use the NCSC's free Exercise in a Box.	Once a year

© Garrould Limited · CC BY-NC 4.0 · Share for non-commercial use with a link to https://www.itmanagement101.co.uk/disaster-recovery-plan-template/

EMERGENCY CARD: IT DISASTER

Keep a copy at home and in your wallet or bag. Do not rely on company email or files.

Step	What to do
1. Make people safe	If anyone is at risk, ring 999 first.
2. Stop the damage	Disconnect affected machines from the network. If a cyber attack is suspected, leave them switched on for the investigation.
3. Ring, don't email	Technical lead: _____ Plan owner: _____ Deputy: _____
4. Decide	Does a trigger apply? The plan owner declares an IT disaster and the time is written down.
5. Start the log	Time, what happened, decision, who decided. Every hour: status and the time of the next update.
6. Personal data	If personal data is unavailable, lost or exposed, start the breach decision now. The ICO's 72-hour clock starts when you become aware.
7. Recover in order	Keys, pipes, data, apps, desks. Use the runbooks for the scenario.
8. Ring the insurer	Cyber insurer claims line: _____ Policy: _____

Emergency admin cards: _____ **Printed plan:** _____

© Garrould Limited · CC BY-NC 4.0 · Share for non-commercial use with a link to https://www.itmanagement101.co.uk/disaster-recovery-plan-template/

WORKED EXAMPLE

Harbour Lane IT Ltd: IT disaster recovery plan

Harbour Lane IT Ltd is a 22-person managed IT services firm supporting about 140 small-business clients from one office (fictional). Its business continuity plan set the recovery targets; this plan shows how each system comes back. All names and figures are illustrative.

System register (in recovery order)

System	Layer	RTO	RPO	Copied every	RPO check	3-2-1	Restore	Last test	Runbook
S1 Microsoft 365 admin and emergency accounts	Keys	2 h	n/a	-	n/a	n/a	0.5 h	2 months ago	R1
S2 Company password manager	Keys	2 h	24 h	24 h	Met	Fails 3-2-1	0.5 h	4 months ago	R1
S4 Cloud phone system	Pipes	1 h	n/a	-	n/a	n/a	0.25 h	1 months ago	R2
S3 Office internet (fibre) and 5G backup router	Pipes	2 h	n/a	-	n/a	n/a	0.25 h	1 months ago	R2
S6 Microsoft 365 mailboxes	Data	8 h	24 h	24 h	Met	Fails 3-2-1	UNTESTED	never	R3
S5 SharePoint company files	Data	24 h	24 h	24 h	Met	3-2-1, no offline	3 h	5 months ago	R3
S7 Ticketing system	Apps	2 h	4 h	24 h	Gap	Fails 3-2-1	UNTESTED	never	R4
S8 Remote monitoring platform settings	Apps	8 h	24 h	24 h	Met	Fails 3-2-1	6 h	14 months ago	R4
S9 Accounts and payroll (cloud)	Apps	72 h	24 h	24 h	Met	Fails 3-2-1	1 h	2 months ago	R4
S10 Staff laptops (22)	Desks	24 h	n/a	-	n/a	n/a	2 h	3 months ago	R5

Scenarios

Scenario	Runbooks	Why this order
Ransomware on a laptop that spreads to synced files	R5, R1, R3, R4	Contain first (R5), then make sure the admin accounts are clean (R1) before restoring files (R3) and checking cloud apps (R4).
Office unusable (fire, flood, power)	R2, R5	Everyone works from home on company laptops; the 5G router does not help if the building is shut.
Admin account taken over	R1, R3	Lock the attacker out, then check for files deleted or encrypted while they were in.
Supplier outage (ticketing)	R4	The business continuity plan's workaround carries the service desk; this runbook gets the data back.
Laptop stolen from a car	R5	One person affected; the main risk is personal data on the device.

Actions from the register and the test log

Action	Owner	By
Ask the ticketing supplier for an hourly export or a better restore point; until then, export open tickets every hour	Service desk lead	This month
Restore a test mailbox and time it, once the two missing mailboxes are in the backup	Lead engineer	2 weeks
Re-test the monitoring platform restore (last done 14 months ago)	Lead engineer	1 month
Add an offline copy for SharePoint: a weekly export to an encrypted drive kept away from the office	Ops lead	1 month
Print this plan and the emergency card; keep one copy at home with the plan owner and one with the deputy	Office manager	This week

© Garrould Limited · CC BY-NC 4.0 · Share for non-commercial use with a link to https://www.itmanagement101.co.uk/disaster-recovery-plan-template/

RUNBOOK R1 · LAYER: KEYS

Locked out of Microsoft 365 admin

Use it when: Nobody with admin rights can sign in, or an admin account may have been taken over.

Owner and deputy: as on the Contacts page. The deputy has walked through every step.

#	Do this	Where	You should see	Min
1	Fetch the sealed emergency access card from the office safe (or the managing director's home copy).	Safe; second copy at the MD's home	Card in hand with both emergency account names	15
2	Sign in with emergency account 1 and its passkey from a clean laptop that is not the one suspected of compromise.	admin.microsoft.com	Admin centre opens	5
3	If the trigger was a takeover: block sign-in for the affected account and sign it out of all sessions.	Admin centre > Users > the account	Account shows as blocked	5
4	Reset the affected admin's password and MFA methods; check which mail forwarding rules and app consents it created.	Admin centre; Exchange admin centre	No unknown forwarding rules or apps	30
5	Start an incident report and run the personal data breach decision: the 72-hour clock starts when you become aware.	Incident report template	Decision recorded with the time	15
6	Tell the ops lead and the managing director what was found, and which accounts are back.	Phone, not company email	Both have acknowledged	5
7	Re-seal the emergency card with a new envelope number and log the use.	Safe; Test log	New envelope number recorded	10

Total if every step runs: about 85 minutes (1.4 hours).

© Garrould Limited · CC BY-NC 4.0 · Share for non-commercial use with a link to https://www.itmanagement101.co.uk/disaster-recovery-plan-template/

RUNBOOK R2 · LAYER: PIPES

Office internet down

Use it when: The office has no internet, or it is too slow to work, for more than 15 minutes.

Owner and deputy: as on the Contacts page. The deputy has walked through every step.

#	Do this	Where	You should see	Min
1	Check the router has moved to the 5G connection on its own.	Router admin page from any office PC	WAN 2 (5G) shows as active	5
2	If it has not: switch the WAN over by hand, then ring the internet provider's fault line with the account number.	Router admin page; Contacts tab	Office browsing works; fault reference noted	15
3	Confirm the cloud phone system is receiving calls; if not, switch on the divert to analysts' mobiles.	Phone system web portal	A test call from a mobile is answered	10
4	If 5G is also down: send staff home to work on company laptops and tell the service desk lead.	Contact tree	Every analyst confirms they are online at home	30
5	Log the outage start, the fault reference and the expected fix time.	Incident log	Entry with times	5

Total if every step runs: about 65 minutes (1.1 hours).

© Garrould Limited · CC BY-NC 4.0 · Share for non-commercial use with a link to https://www.itmanagement101.co.uk/disaster-recovery-plan-template/

RUNBOOK R3 · LAYER: DATA

Restore deleted or encrypted company files

Use it when: Files in SharePoint are missing, overwritten or encrypted.

Owner and deputy: as on the Contacts page. The deputy has walked through every step.

#	Do this	Where	You should see	Min
1	Stop the damage: if encryption is spreading, disconnect the affected laptop from the network and suspend its user's sign-in.	The laptop; Admin centre > Users	No new files changing	10
2	Find the scope: which library or folders, and when the damage started.	SharePoint library > version history and activity	A start time written down	20
3	For a few files deleted within 93 days: restore them from the recycle bin.	Site > Recycle bin, then second-stage bin	Files back, opened by their owner	15
4	For a whole library, or anything older: restore from the backup service to a new location, not over the top.	Backup service console (login in the password manager)	Restore job completed	120
5	Ask the file owner to open a sample of the restored files and confirm they are the right version.	Phone the owner	Owner confirms	20
6	Move the checked files back into place and record the restore time on the Test log.	SharePoint; Test log	Achieved time recorded	30

Total if every step runs: about 215 minutes (3.6 hours).

© Garrould Limited · CC BY-NC 4.0 · Share for non-commercial use with a link to https://www.itmanagement101.co.uk/disaster-recovery-plan-template/

RUNBOOK R4 · LAYER: APPS

Cloud (SaaS) application down or data lost

Use it when: The ticketing system, monitoring platform or accounts system is unavailable or missing data.

Owner and deputy: as on the Contacts page. The deputy has walked through every step.

#	Do this	Where	You should see	Min
1	Check the supplier's status page before anything else.	Supplier status page (Contacts tab)	Outage confirmed or ruled out	5
2	Raise a priority ticket and ask two questions: when will it be back, and to what point can you restore our data?	Supplier support line and account number	Ticket reference and both answers written down	15
3	Start the workaround from the business continuity plan (for ticketing: the shared spreadsheet log and this morning's export).	BCP Plan tab	Workaround running	15
4	If data is lost: compare the supplier's restore point with your own last export; key in the gap from email and call logs.	Last export on SharePoint	Gap listed and assigned	60
5	When the service returns: check a sample of records, then switch back from the workaround.	The application	Service desk lead confirms	30

Total if every step runs: about 125 minutes (2.1 hours).

© Garrould Limited · CC BY-NC 4.0 · Share for non-commercial use with a link to https://www.itmanagement101.co.uk/disaster-recovery-plan-template/

RUNBOOK R5 · LAYER: DESKS

Laptop lost, stolen or encrypted

Use it when: A company laptop is missing, damaged beyond use, or showing a ransom note.

Owner and deputy: as on the Contacts page. The deputy has walked through every step.

#	Do this	Where	You should see	Min
1	Disconnect it from the network if you have it; do not switch it off if a cyber attack is suspected.	The laptop	Network cable out, Wi-Fi off	5
2	Block the user's sign-in, sign them out everywhere and reset their password and MFA.	Admin centre > Users	User shows signed out	10
3	Issue a spare laptop from the cupboard and sign the user in; their OneDrive files return on their own.	Spare laptop cupboard	User at work with their files	60
4	Wipe the lost laptop remotely, or re-image the damaged one from the standard build.	Device management console	Wipe or rebuild confirmed	60
5	If personal data was on the device or exposed, run the breach decision and log it.	Incident report template	Decision recorded	15

Total if every step runs: about 150 minutes (2.5 hours).

© Garrould Limited · CC BY-NC 4.0 · Share for non-commercial use with a link to https://www.itmanagement101.co.uk/disaster-recovery-plan-template/

Test log

When	System / runbook	Test	Target	Achieved	Result	What we found and changed
5 months ago	S5 SharePoint files / R3	Timed system restore	24 h	3 h	Pass	Restore took 3 hours, mostly finding the backup console login Console login added to the password manager
2 months ago	S9 Accounts and payroll / R4	Timed system restore	72 h	1 h	Pass	None
2 months ago	S1 Emergency admin accounts / R1	Emergency admin sign-in	2 h	0.5 h	Pass	Second card was in the office safe too Move one card to the MD's home
1 months ago	S3 Internet / R2	Deputy walk-through	2 h	0.25 h	Pass	Router fail-over worked; nobody knew the provider account number Account number added to the Contacts tab
1 months ago	S6 Mailboxes / R3	Timed system restore	8 h	-	Fail	Backup service had stopped including two new starters' mailboxes Add new starters to backup in the onboarding checklist; re-test
this week	S7 Ticketing / R4	Scenario exercise	2 h	-	Fail	Supplier can restore only to the previous midnight Hourly export by the supplier's API; ask about a 4-hour restore point at renewal

Two of the six tests failed. That is the log working: both failures were found on a quiet afternoon instead of during an outage.

© Garrould Limited · CC BY-NC 4.0 · Share for non-commercial use with a link to https://www.itmanagement101.co.uk/disaster-recovery-plan-template/