

Downtime Risk Checklist

How quickly would work stop if your IT went down?

Contents

Page 3

How to use this checklist?

Page 4

What Would Stop First?

Page 5

Everyday Weak Points

Page 6

Hidden Risks You Cannot See

Page 7

Backups and Recovery

Page 8

Network and Internet Resilience

Page 9

Your downtime risk score

Page 10

Your Next Step: The Downtime Risk MOT

How to use this checklist?



This checklist is for hands on businesses that rely on planning, drawings, scheduling or dispatch to keep work moving.

For example: fabrication, engineering, construction, trades, warehousing and similar companies.

Use it to see how quickly work would stop if your IT failed, and where the weak points are.

- Answer each question **Yes** or **No**
- If you are not sure, treat it as a **No**
- Add up your **Yes** answers and use the scoring at the end



If your score worries you or raises questions you cannot answer, the next step is a Downtime Risk MOT.

What Would Stop First?

Would planning, scheduling or job allocation stop if one key PC failed?		
Would drawings, CAD files or machine settings be unavailable if the main PC storing them went down?		
Would dispatch, stock or delivery notes stop if the person who handles them could not log in?		
Would your team on site, in the workshop or in the warehouse be unable to work if email or internet stopped working?		
Do you have a documented plan for how long you can operate if any of these systems fail?		

Everyday Weak Points

Are staff using company devices for work rather than personal laptops or phones?		
Does everyone use the extra login security step (the code to your phone) when signing in?		
When someone leaves, is their access to your systems stopped straight away?		
Are the PCs you rely on for planning, drawings, scheduling or dispatch less than 5 years old?		
Is your Wi Fi reliable everywhere it is actually used, including the workshop, warehouse, office, yard or site areas?		

Hidden Risks You Cannot See

Are all work PCs protected with security software that is up to date and centrally monitored?		
Are security updates checked and installed automatically within around two weeks, without relying on staff to do anything?		
Does everyone use their own login, rather than sharing the same account?		
Is there a separate admin account for installing software, and do staff use normal logins for everyday work?		
Do you have protection in place that blocks fake emails pretending to be suppliers, customers or staff?		
Are you alerted if someone logs into your systems from an unexpected country?		
Is remote access into your systems protected with an extra security step, such as a code to your phone?		

Backups and Recovery

Could you recover your key systems the same day if a PC or server failed?		
Are your backups protected so ransomware cannot encrypt or delete them?		
Is Microsoft 365, such as email, OneDrive and SharePoint, backed up separately?		
Has a full restore been tested in the last 12 months?		
Do you know roughly how long it would take to get your systems back if the worst happened?		

Network and Internet Resilience

Do you have a backup internet option if your main connection stops working?		
Is your router or firewall still supported and receiving security updates?		
Are key systems separated so one infected device cannot bring everything down?		
Do you receive alerts if something on your network behaves unusually, such as devices going offline or large spikes in traffic?		
Is remote access only available through a secure method with an extra login step?		



Your downtime risk score

When you have answered all the questions, add up your Yes answers and use the guide below to see your level of downtime risk.

22 to 27 points: Low Risk

You have strong resilience in place. A few improvements may tighten things further.

14 to 21 points: Medium Risk

You are doing some things well but there are weak points that could cause unexpected stoppages. Most hands on businesses fall here.

0 to 13 points: High Risk

A single failure, such as a PC, a login breach or a backup issue, could stop work for hours or days. You have serious downtime exposure.

If this checklist shows gaps, or if you are worried about any of the questions, the next sensible step is a Downtime Risk MOT.

Your Next Step: The Downtime Risk MOT

A simple, fixed price review that shows what would stop work if your IT failed and what you must fix first to keep jobs moving.

If you do not leave the MOT clearly informed about how an IT failure would hit your business and your top three fixes, **you do not pay. You are the judge.**



What the MOT includes

- Microsoft 365 security review
- Backup and recovery protection check
- Endpoint and email protection audit
- Wi Fi and network continuity review
- User access and admin rights audit
- Day 1, Day 3 and Day 7 downtime impact summary
- Clear priorities for the next 30 days and 90 days

£495
+VAT