

# Cyber Insurance Readiness Checklist

*Verify your policy, technical controls and incident plan*

## 1. Policy

- ☐ Obtain full wording and schedule
- ☐ Check limits, excesses and sub-limits
- ☐ Review exclusions
- ☐ Check business-interruption cover
- ☐ Check social-engineering cover
- ☐ Check cloud and supplier cover

## 2. Application Answers

- ☐ Assign an owner to each question
- ☐ Verify technical answers
- ☐ Retain supporting evidence
- ☐ Recheck previous-year answers
- ☐ Record any assumptions

## 3. Security Controls

- ☐ MFA
- ☐ Administrator protection
- ☐ Supported systems
- ☐ Security updates
- ☐ Endpoint protection
- ☐ Secure remote access

## 6. Ask Your Broker

- What is covered?
- What is excluded?
- Which sub-limits apply?
- Is supplier disruption covered?
- What approval is required during a claim?

## 4. Backups and Recovery

- ☐ Critical data included
- ☐ SaaS backup reviewed
- ☐ Encryption enabled
- ☐ Backup access protected
- ☐ Isolated copy maintained
- ☐ Restore tested

## 5. Incident Response

- ☐ Emergency insurer number recorded
- ☐ Policy number available offline
- ☐ Notification responsibilities agreed
- ☐ IT provider informed of process
- ☐ Alternative communications available
- ☐ Incident plan tested

## 7. Ask Your IT Provider

- Is MFA fully deployed?
- Are all systems supported?
- Are backups isolated and tested?
- Can technical answers be evidenced?
- Who supports an insurer-appointed forensic team?



Scan for the full guide  
itclub.work/knowledge-centre

**Verify the answers. Maintain the controls. Know who to call.**

**IT Club**

Technology Intelligence — Plain-English guidance for business owners

<https://itclub.work/knowledge-centre>