

How resilient is your IT system ?

& 5 levers to strengthen your IT
system's robustness



YOUR TURN!



Q1 – Have you implemented a BCP or DR plan?

- ☒ Yes, tested: Very good reflex, keep going.
- ☐ Yes, untested: To be formalised and tested quickly.
- ☐ In progress: Good approach, to be finalised quickly.
- ☐ No / I don't know: High risk in case of crisis.

Q2 – How do you control your accesses to sensitive data?

- ☒ IAM + MFA: Excellent level of security.
- ☐ By internal roles: To be reinforced with MFA.
- ☐ On a case-by-case basis: Potential vulnerabilities, to be structured.
- ☐ No strategy: Data exposed.

Q3 – What is your resilience based on?

- ☒ Backups: indispensable foundation.
- ☒ Cloud/Redundancy: Very good point.
- ☒ Proactive monitoring: Effective prevention.
- ☒ Team training: Key element to prevent from human errors.
- ☐ No measures: Critical risk.

Q4 – What is your biggest risk?

- Ransomware: Protect your backups.
- Human error: Train your teams.
- Internal leak: Strengthen your access and audits.
- Hardware failure: Implement a disaster recovery plan.
- Other: Integrate it into your overall strategy.

Q5 – How would you rate your preparedness for an IT crisis?

- ☒ Very prepared: Keep testing.
- ☐ Moderately prepared: Consolidate your weak points.
- ☐ Not very prepared/Not prepared at all: React quickly.
- ☐ I don't know: This uncertainty is a risk in itself.

Your answers to the assessment may indicate areas to improve. To help you build action, **here are the key levers to activate for a better protection of your information system protection.**



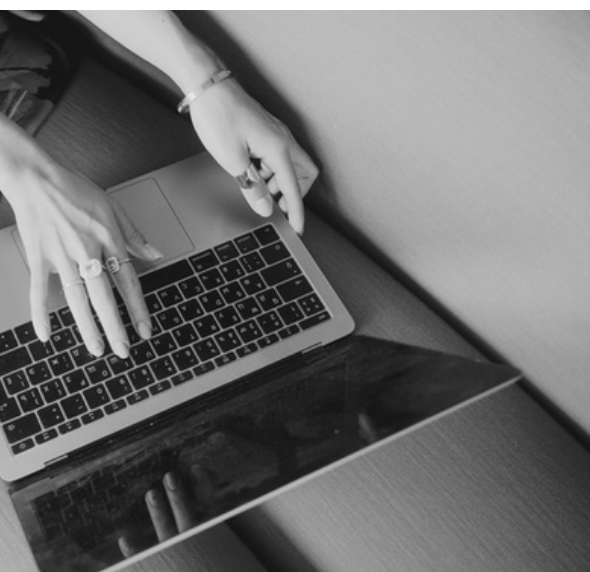
5 levers to strengthen your IT resilience

01 A proven backup strategy

- Apply the 3-2-1 method: 3 copies – 2 different media – 1 off-site
- Regularly test data restoration

02 Simulate an incident to better respond

- Table-top exercises
- Disaster recovery tests
- Cyber and technical scenarios



03

Protect your data beyond your walls

- Table-top exercises
- Disaster recovery tests
- Cyber and technical scenarios

04 Training your users: the human link

- Short sessions (30 minutes to 1 hour) on: phishing, responding to an attack, best practices for passwords
- Simulated testing campaigns

05 Simulate an incident to respond better

- Security audit every 12–24 months
- Vulnerability scanning and penetration testing
- Access verification, updates, and crisis procedures

Need an outside view?

Our team is here to support you every step of the way.

Let us work together to develop a backup strategy tailored to your environment.

You just have to fill this short form: our team will contact you very quickly for a personalised consultation.

[CONTACT US](#)