Business continuity: could you keep working for a week without a key system, supplier or site?

This quarter, list the processes that would do serious harm if stopped for a week, set up a crisis team with deputies and a channel outside your own IT, and give each process a one-page workaround. Then run a tabletop and a technical failover at least once a year, and let the measured recovery times decide what to fix next.

Reviewed	Next review	Version	Written for
5 Nov 2026	**5 Dec 2026**	**1.1**	**IT, security, risk and operations leads in EU organizations of any size, including those under NIS2 or DORA**

Latest version
sheets.einblick.dev/business-continuity/

If you only do five things

1. **List the processes that can't stop for a week.**
   Ask each department what 7 days of downtime would cost, and have management sign off the shortlist. BSI-Standard 200-4 uses such a prefilter to focus the impact analysis[1].
2. **Set up the crisis team first.**
   Name a lead, a deputy for each role and a channel that works without your own IT. BSI's entry stage starts here, because a crisis team allows a basic response before any plans exist[1].
3. **Write a workaround for each critical process.**
   Describe on one page how it runs on paper, by phone or on spare devices. The NCSC says organizations commonly run with limited or no IT for weeks after a disruptive attack[2].
4. **Set recovery targets and measure them.**
   Give each critical process a maximum tolerable downtime, then recovery time and data loss targets for its systems[1]. The backups and ransomware sheets cover restore tests.
5. **Exercise at least once a year.**
   Run a tabletop for decisions and a failover of one top system, and record the times. ENISA advises testing at least annually[5]; the NCSC warns that many plans fail in practice[3].

Run a lean impact analysis

1. **What would hurt within a week?**
   Ask each unit what a 7-day outage would do to safety, operations, legal and contract duties, reputation and finances[1]. Keep those above a threshold agreed with management.
2. **How long can each process stop?**
   Set the maximum tolerable period of disruption, a recovery time objective below it and a recovery point objective for its data[1].
3. **What does it run on?**
   List people, sites, IT systems, SaaS, suppliers and data. DORA requires the analysis to cover third-party dependencies and interdependencies[8]. Note which share a cloud region or identity provider.
4. **What is good enough in a crisis?**
   Set a minimum service level, such as the share of calls answered within a set time[5].
5. **Do your systems meet the targets?**
   Compare each target with the last measured restore time. Close the gap, change the workaround or have management accept it.

Keep working without your systems

- **Check what is critical this month.** Payroll, cash flow, regulatory reporting and peak seasons shift priorities[2]. Note the critical dates.
- **Review workarounds for security.** Private email or a shared spreadsheet can add risk. Review each one before use and give it a review date so it doesn't become permanent[2].
- **Plan how the data gets back.** Decide early how records kept on paper or in spreadsheets will be reconciled with restored systems[2].
- **Keep the inputs on paper.** Print the plan, as ENISA suggests[5], plus contact lists and price lists, and keep a daily offline export of open orders.

Crisis team, decisions and messages

- **Agree when to declare a crisis.** Write criteria such as prolonged downtime, several sites hit or likely public scrutiny[5]. Anyone may escalate; named people declare.
- **Decide authority in advance.** Record who makes strategic decisions, your risk appetite and escalation thresholds[4], and who may stop deliveries or approve emergency spending. The incident response sheet covers the first hours.
- **Prepare messages and channels.** Draft statements for staff, customers and suppliers, and keep channels that work when primary systems are down[4]. The EU security laws sheet has the reporting clocks.
- **Log decisions and times.** Each time the plan is activated, record decisions, steps and the final recovery time[5].

What large outages teach

- **One update can stop all your Windows devices.** A faulty CrowdStrike update on 19 July 2024[13] affected an estimated 8.5 million Windows devices[12], and the manual fix could ask for each BitLocker recovery key[14]. Stage such updates, which customers can now control[13], and make sure the help desk can read keys with servers down.
- **Sign-in and phones are dependencies.** In AWS's October 2025 outage, Identity Center users in us-east-1 couldn't sign in and callers to Amazon Connect contact centers got busy tones[16]. Test emergency access to each cloud console and keep a fallback phone number.

Exercise in this order

1. **Can you reach the crisis team?**
   Run an unannounced alert test after hours over the backup channel, and tell the works council first. BSI's standard requires alert and crisis staff exercises even at its entry stage[1].
2. **Do the decisions hold up?**
   Run a two-hour tabletop: a key SaaS supplier is gone for a week. The NCSC's Exercise in a Box has scenarios[3].
3. **Do the workarounds work?**
   Walk through each with its users, then run one for half a day.
4. **Does failover work under load?**
   Run real work on one top system's secondary site, zone or backup. DORA requires most financial entities to test such switchovers[8,9].

Mistakes that cost the most

- **Treating recovery time as total downtime.** The recovery time objective runs from declaring the emergency, so detection and decision come off the tolerable downtime first[1].
- **Planning around one person.** If only one person knows the workaround, the plan fails when they are away. DORA's scenarios include losing a critical number of staff[9].
- **Trusting the provider's redundancy.** Google says customers must provision failover for zonal resources such as VMs[17]. Ask each critical SaaS provider what its plan leaves to you.
- **Testing only the easy parts.** A tabletop alone doesn't show that a top system runs at the backup site. DORA's tests must challenge the plans' assumptions[9].

What changed in 2026

- **A power failure in one zone slowed a cloud region.** On 20 October 2026, generators at Google Cloud's London zone europe-west2-b failed to start; other zones were affected and some failovers failed for lack of capacity[17]. Test failover at full capacity.
- **The NCSC published guidance on recovering to minimum viable operations:** the lowest level at which you can operate safely, meet legal duties and keep trust[2]. Set one per critical process.
- **Germany's KRITIS umbrella act took effect** on 17 March 2026; registration waits for its scope ordinance, still a draft[11]. Most registered operators outside IT, telecom and finance have 10 months for a resilience plan[10].

What you can skip

- **An impact analysis of every process.** BSI's entry stages start with the most time-critical processes and add the rest in later cycles. If you're regulated, include all regulated processes in the first cycle[1].
- **Certification before the first exercise.** A certificate doesn't show that payroll runs on day three.
- **Runbooks for every system.** Write them for the systems critical processes need. Restore the rest from backup in priority order.
- **Multi-cloud as the plan.** Running everything twice is costly and rarely tested. First prove failover to a second zone or region.

What this looks like at your size

Small team, no security staff

- Unless regulated, follow BSI-Standard 200-4's reactive entry stage: crisis team with deputies, a 7-day shortlist and one-page workarounds[1].
- Print the plan, the phone tree and the BitLocker key steps; keep copies with two people at home.
- Ask your IT provider and key SaaS suppliers how fast they restore and how they'd reach you without email.

Growing, with IT or security staff

- Have process owners set the targets for the shortlist and management sign them off.
- Write runbooks for the top five systems and time one restore or failover each quarter.
- Quick machine recovery's cloud remediation is off by default on managed devices[15]: decide whether to turn it on, and stage EDR content updates.

Enterprise or regulated

- NIS2 requires business continuity and crisis management[6]; point 4 of Implementing Regulation 2024/2690 details it for cloud, managed service and other digital providers[7].
- Under DORA, test yearly; all but microenterprises add cyberattack and switchover scenarios and a crisis management function[8].
- Exercise the loss of a cloud zone and region, and check which SaaS suppliers share them.

Version history

5 Nov 2026, version 1.1 Confirmed that KRITIS registration still waits for the draft scope ordinance.

Sources

1. BSI-Standard 200-4 Business Continuity Management, version 1.0. BSI, May 2023. bsi.bund.de
2. Disruptive cyber attacks: recovery and ongoing investigations. NCSC (UK), 28 Jul 2026, reviewed 1 Oct 2026. ncsc.gov.uk
3. Disruptive cyber attacks: prepare your business continuity. NCSC (UK), 1 Oct 2026. ncsc.gov.uk
4. Disruptive cyber attacks: prepare to make critical decisions. NCSC (UK), 1 Oct 2026. ncsc.gov.uk
5. NIS2 Technical Implementation Guidance, version 1.0. ENISA, 26 Jun 2025. enisa.europa.eu
6. Directive (EU) 2022/2555 (NIS2), Article 21. EUR-Lex, 2022. eur-lex.europa.eu
7. Implementing Regulation (EU) 2024/2690, Article 1 and Annex point 4. EUR-Lex, 17 Oct 2024. eur-lex.europa.eu
8. Regulation (EU) 2022/2554 (DORA), Article 11. EUR-Lex, 2022. eur-lex.europa.eu
9. Delegated Regulation (EU) 2024/1774, Articles 25 and 26. EUR-Lex, 13 Mar 2024. eur-lex.europa.eu
10. KRITIS-Dachgesetz, §§ 4, 8 and 13. BMJV (Germany), checked 4 Nov 2026. gesetze-im-internet.de
11. FAQ zum KRITIS-Dachgesetz. BBK, checked 5 Nov 2026. bbk.bund.de
12. Helping our customers through the CrowdStrike outage. Microsoft, 20 Jul 2024. blogs.microsoft.com
13. Channel File 291 Incident Root Cause Analysis. CrowdStrike, 6 Aug 2024. crowdstrike.com
14. KB5042421: CrowdStrike issue impacting Windows endpoints. Microsoft Support, checked 4 Nov 2026. support.microsoft.com
15. Quick machine recovery. Microsoft Learn, 26 Oct 2026. learn.microsoft.com
16. Summary of the Amazon DynamoDB service disruption in US-EAST-1. AWS, Oct 2025. aws.amazon.com
17. Incident report: multiple services in europe-west2. Google Cloud, 27 Oct 2026. status.cloud.google.com