



ENERGISE SPECIAL REPORT

The SME Technology Resilience Test

What still works when something fails?

A practical continuity guide for South African SME owners, office managers, finance managers and technology decision-makers.

THE MANAGEMENT QUESTION Not whether every system can be kept fully available, but which business functions must keep working, at what minimum level, for how long, and at what sensible cost.

FACT-CHECKED: 13 AUGUST 2026

EXECUTIVE SUMMARY

Most SME technology failures are not isolated. A fibre fault can affect calls, cloud applications, card payments, remote access, print-and-scan workflows and off-site monitoring at the same time. A later power failure can then disable the router, optical network terminal, switches, Wi-Fi, phones, cameras and access-control components that the backup plan assumed would still be running.

That is why a spare link, a battery or a cloud subscription is not the same as resilience. Redundancy provides an alternative component. Resilience is the tested ability of the business to anticipate disruption, continue essential work at an acceptable level, recover cleanly and adjust the design after learning from failure. This practical framing is consistent with NIST's resilience definition: anticipate, withstand, recover and adapt. [1]

CORE FINDING The weakest point is often not the expensive system. It is the shared dependency underneath several systems: one router, one switch, one power circuit, one mobile network, one identity administrator, one print server, one SIM with an expired data bundle, or one person who knows how the failover works.

What this report asks management to do

- Name the business functions that must continue for four hours, even if service is degraded.
- Map each function to its full chain of power, connectivity, network, cloud, device, supplier and people dependencies.
- Distinguish a duplicated component from an independent, powered, monitored and tested fallback.
- Use a simple downtime-cost range to set sensible priorities - not to manufacture a precise number.
- Run the Four-Hour Business Survival Test and record decisions, owners, limits and evidence.

The aim is not zero downtime. For most SMEs, that would be unaffordable and unnecessary. The aim is controlled degradation: critical work continues, safety is protected, customers receive a credible response, data remains trustworthy, and recovery does not create a second problem.

1 The real question is not uptime. It is survivability.

Technology is normally bought in categories: fibre, phones, Microsoft 365, printers, security and power. The business experiences them as one operating environment. When a dependency fails, several categories can stop together.

South African conditions make this particularly practical. ICASA's March 2026 sector report says national 4G/LTE population coverage rose to 99.5% in 2025, while reported urban coverage by province was between 98% and 100%. That supports mobile backup as a realistic option in many places. Coverage statistics do not prove adequate indoor signal, usable capacity, stable latency, the right public IP behaviour, an active data bundle or working runtime at a particular premises. Those must be tested on site. [2]

The power context has also changed. On 17 July 2026, Eskom reported 427 consecutive days without load shedding since 16 May 2025 and a financial-year-to-date Energy Availability Factor of 65.46%. That is material improvement. It does not prevent local municipal outages, feeder faults, building trips, cable theft, planned maintenance or an internal electrical failure at one office. Resilience planning should therefore move beyond the old assumption that power backup is only a load-shedding purchase. [3]

A BETTER TEST If the office loses fibre at 09:10 and power at 10:10, what can staff still do at 13:10 - and what evidence proves it?

2 Redundancy and resilience are not the same thing

Redundancy is duplication: a second link, a second handset, another switch, a UPS or another supplier. It reduces risk only if the alternative does not fail for the same reason and can take over in the conditions that matter.

Resilience is broader. It includes the ability to anticipate failure, withstand it at an acceptable service level, recover without losing control of data or process, and adapt the design. [1] A resilient service may be deliberately reduced during an incident. For example, LTE may carry voice, email, payments and the finance system while video streaming, large cloud backups and guest Wi-Fi are blocked.

Redundant item	Why it can still fail	What makes it more resilient
Two fibre contracts	May still share the same fibre network operator, building entry, duct, exchange, upstream route or power dependency.	Confirm physical and provider diversity; test one link disconnected.
Fibre plus LTE	Uses different access technology, but may be weak indoors, capped, congested or unpowered.	Survey signal and capacity; power the full network path; prioritise critical traffic.
Cloud PBX	Moves call control off-site, but handsets, Wi-Fi, internet, identity and the provider still matter.	Test inbound redirection, mobile clients, emergency contacts and degraded calling.
Cloud documents	Provider resilience does not make online-only files available when the office is offline.	Keep selected working files offline and test access, edit and later sync.
Inverter or UPS	A battery can be installed but omit the ONT, firewall, PoE switch, NVR or access controller.	Label circuits and measure runtime under the real load.

The commercial point is simple: independence and testability matter more than the number of products on the invoice.

3 Scenario: a 25-person SME loses fibre, then power

Consider a 25-person professional-services and distribution business operating from one South African office. It uses business fibre, a firewall with an LTE SIM, a hosted PBX, Microsoft 365, a networked multifunction printer, eight IP cameras with an on-site recorder, electronic access control and a small inverter. The exact products are not important; the dependency pattern is common.

Time	Event	Operational effect
09:10	Primary fibre fails	The firewall detects a lost link. LTE is configured, but the SIM has not carried full office traffic in six months. Email and web access return slowly; several calls become unstable. Staff are unsure whether large uploads and guest Wi-Fi should be stopped.
09:25	Work splits into three groups	Some staff continue in cached email and locally available files. Others use web-only applications and cannot work reliably. Reception redirects urgent calls manually. A cloud-linked scan workflow queues or fails because the MFP cannot reach its destination consistently.
10:10	Power fails	The inverter powers several desks, but the communications cabinet is on a different circuit. The ONT, firewall, core switch and PoE switch go off. LTE failover is now irrelevant because the router is not running. Desk phones, Wi-Fi access points and IP cameras lose service.
10:20	Security behaviour becomes visible	The front-door lock and internal secure-area lock behave according to their fail-safe or fail-secure design. Staff discover whether door events are recorded locally, whether the controller has battery backup, and whether manual keys and visitor procedures are available. A fail-safe lock unlocks on power loss; a fail-secure lock remains locked, so the correct choice depends on life-safety and security requirements. [4]

Time	Event	Operational effect
11:00	Manual workarounds begin	Managers nominate a mobile contact number, prioritise customer-facing work, use selected laptops and mobile hotspots, record orders and approvals in a controlled outage log, and suspend non-essential bandwidth use.
13:10	Services recover	Power and fibre return. The team must reconcile offline notes, queued email, call records, print jobs, scans and access events. Recovery is not complete until the backlog is checked and one trusted record is confirmed.

WHY THE SEQUENCE MATTERS The first failure tests connectivity. The second tests whether the backup path, network, security and communications equipment were included in the power design. Sequential failures expose assumptions that a single-system test misses.

4 Connectivity: fibre/LTE failover that is ready, not merely installed

Automatic failover can reduce disruption, but it is not magic. The router must detect the right type of failure, change routes cleanly, preserve security policy, provide suitable DNS, and move the applications that matter. Some sessions will reconnect; others may need to be restarted because the public IP address or network path changed.

Questions worth asking before approving a backup link

- Is the backup independent of the primary last mile, building entry, power circuit and provider failure domain?
- Can it carry the critical workload at busy-hour usage, not just pass a speed test on a quiet morning?
- What happens to VoIP quality when cloud backups, CCTV viewing, software updates and guest traffic compete for LTE?
- Does the SIM have the correct APN, data allowance, recharge process, roaming policy and responsible owner?
- Will VPNs, remote access, hosted services or allow-listed systems work from the backup public IP and NAT configuration?
- How quickly is failure detected, who receives the alert, and is recovery to fibre automatic or controlled?
- How often is the failover tested with the fibre physically disconnected?

Business connectivity is often presented as a combination of fibre, LTE and SD-WAN, with automatic failover and application prioritisation. Those are useful building blocks. The management step that is still frequently missed is proving the entire dependency chain under a timed, real-office test - including power, capacity, security rules, supplier contacts and staff behaviour.

PRACTICAL DEFAULT During LTE operation, reserve bandwidth for voice, customer service, payments, finance/ERP access, email and essential collaboration. Pause guest Wi-Fi, bulk sync, software downloads, streaming and non-essential camera viewing unless the risk case says otherwise.

5 VoIP and cloud phones: where the dial tone really depends

Hosted voice can improve flexibility because extensions can work on desk phones, laptops or mobile applications and calls can be redirected. It also creates a dependency chain: handset or app, local power, LAN or Wi-Fi, internet path, DNS, firewall, identity, PBX platform, SIP/PSTN connection and provider support.

A cloud PBX does not automatically keep an office reachable during an internet or power outage. A useful continuity design answers three separate questions: Can customers still reach the business number? Can

selected staff make and receive calls? Can the business see what happened afterwards through call logs, voicemail and recordings?

Minimum viable voice service

- Publish one tested incident contact route and keep an offline copy of critical numbers.
- Define which inbound numbers or queues redirect to which mobiles, and who has authority to activate the change.
- Power the PBX gateway or session border controller, PoE switch, Wi-Fi and handsets that the design relies on.
- Test call quality over LTE while other critical applications are active.
- Confirm emergency-calling and location arrangements with the provider; do not assume a mobile or softphone behaves like a fixed line.
- Keep a manual customer-callback list during the incident and reconcile it when call systems recover.

More advanced survivability exists in some platforms, but it is a designed feature, not an automatic property of 'cloud voice'. Microsoft, for example, documents a Survivable Branch Appliance for specific Teams Phone Direct Routing scenarios when a site cannot reach the Microsoft cloud; it requires compatible architecture and configuration. [5]

6 Microsoft 365 and cloud applications: provider continuity versus office continuity

Cloud platforms are engineered with service-level resilience, monitoring and recovery. Microsoft provides service-health information to administrators and describes continuity measures within Microsoft 365. [6] That does not remove the customer's local dependencies: internet access, power, device health, identity, multi-factor authentication, licences, sync state and user knowledge.

Offline capability must be selected and tested. Microsoft states that OneDrive online-only files cannot be opened without an internet connection, while files marked 'Always keep on this device' are downloaded and remain available offline. [7] Cached Exchange Mode in classic Outlook keeps a local mailbox copy and is intended to support work when the network is slow or unavailable; the current Microsoft support note also states that Cached Exchange Mode is not available in new Outlook for Windows. [8]

A four-hour cloud-app plan

Work area	Degraded method	Control point
Email	Read cached messages, draft responses offline, use a controlled mobile channel for urgent communication.	Test the actual Outlook client and shared mailbox behaviour.
Files	Keep selected current operating files locally available; protect devices and avoid uncontrolled copies.	Check the green always-available state and open files with Wi-Fi disabled.
Teams/collaboration	Use mobile data selectively or switch to a named phone/SMS channel for the incident.	Do not assume meetings, presence and telephony all fail or survive together.
Finance/CRM/ERP	Define the minimum transactions that must continue and an authorised temporary record if the app is unavailable.	Reconcile once; avoid duplicate capturing.
Identity/MFA	Maintain more than one authorised administrator and protected recovery methods.	Test access without relying on one person's phone or memory.

IMPORTANT CONTROL Offline work is still business data. Apply the same confidentiality, device encryption, access control, retention and reconciliation rules that would apply online.

7 Printers and MFP workflows: the device may be on while the process is down

Modern multifunction printers are part of a document workflow, not only a print engine. Common workflows include scanning to email, a local network folder, a document-management system or a cloud service. This is useful functionality, but each destination adds a dependency that must be tested during connectivity and power failures.

A device may still copy locally while scan-to-email, scan-to-SharePoint, pull printing, authentication, address books, print accounting or document-management capture is unavailable. Conversely, cloud print may be available while the local device or building network is not.

Test the workflow, not only the machine

- Print one authorised local document with the internet disconnected. Identify whether a print server, cloud queue or user authentication service is required.
- Scan one document to each critical destination. Record what happens when the destination is unavailable: clear error, local queue, retry or silent failure.
- Define an approved temporary method for urgent documents, including naming, storage, confidentiality and later capture.
- Keep service, meter, toner and support details available without needing the failed cloud system.
- Check that queued print jobs do not all release when service returns, creating duplicate or confidential output.
- Avoid informal USB workarounds unless policy allows them and the device is controlled.

RESILIENCE QUESTION Can the business still create, approve, send, receive, store and later reconcile its critical documents - not merely make a copy?

8 CCTV and access control: continuity must protect both people and premises

IP security systems commonly depend on cameras, door readers, controllers, locks, PoE switches, an NVR or server, storage, the LAN, remote connectivity, time synchronisation, power supplies and batteries. Cloud viewing may fail while local recording continues; local recording may fail while cameras still appear online; access decisions may continue at the controller even if management software is unreachable. The design and configuration determine the outcome.

Door behaviour requires explicit life-safety and security decisions. Axis explains the core distinction: fail-safe locks unlock when power is lost; fail-secure locks remain locked. Either can be correct in the right location, but emergency egress, fire design, local requirements and physical security must be assessed by competent specialists. [4]

Evidence to collect in a controlled test

Test condition	Required observation
Power removed	Which doors unlock or remain locked? Can people always exit safely? Are manual keys and procedures available?
Internet removed	Does local recording continue? Can authorised staff retrieve footage locally? Are alerts delayed or lost?
LAN segment removed	Do controllers make local access decisions? Which cameras, readers or intercoms share the failed switch?

Test condition	Required observation
NVR/storage unavailable	Do cameras buffer locally? How is the recording gap detected and documented?
Recovery	Are timestamps correct, backlogs visible, door events complete and recording retention still within policy?

Never test a lock or power isolation in a way that compromises evacuation, fire systems or personal safety. Coordinate with the responsible security, facilities and fire-safety parties.

9 Backup power: keep the service chain alive

Battery or generator decisions often begin with visible loads such as computers and lights. Technology continuity usually depends on smaller hidden loads in different rooms: the fibre ONT, router/firewall, core switch, PoE switch, Wi-Fi access points, voice gateway, selected phones, NVR, access controller and sometimes the MFP.

Runtime is not the nameplate capacity divided by a guessed load. Battery chemistry, inverter efficiency, age, temperature, startup demand, power factor, depth-of-discharge settings and expansion all affect results. Use supplier calculations, then measure under the intended load and record the result.

A practical power priority ladder

- Tier 1 - life safety and access: required fire, emergency, access-control and security functions as designed by competent specialists.
- Tier 2 - core communications: ONT, firewall/router, core switch, selected PoE, Wi-Fi, voice gateway and incident contact devices.
- Tier 3 - critical work: selected laptops, monitors, finance/customer-service devices and essential document capability.
- Tier 4 - deferrable load: general printing, kitchens, comfort loads, non-essential displays, charging and high-bandwidth systems.

MANAGEMENT DECISION Specify the required service and runtime first - for example, 'keep 10 users, voice, one Wi-Fi zone, core cloud access and security recording operating for four hours' - then size and test the power system against that requirement.

10 Find the single points of failure before they find you

A single point of failure is any one component, supplier, person or process whose loss prevents a critical business function from meeting its minimum service level. The same item can be non-critical in one firm and decisive in another.

Failure domain	Typical SME examples
Physical	One building entry for both fibre links; one comms cabinet; one power circuit; one locked room key.
Network	One firewall; one core or PoE switch; one DNS configuration; one LTE SIM/network; one untested failover rule.
Cloud and identity	One global administrator; one MFA device; one domain/DNS account; one online-only repository; one integration credential.
Voice	One inbound route; one PBX administrator; no current diversion list; desk phones powered from one switch.

Failure domain	Typical SME examples
Documents	One MFP; one print server; one scan mailbox; one approval workflow; no controlled temporary record.
Security	One NVR or storage disk; one PoE switch; one access controller power supply; no manual key process.
Supplier and commercial	Expired SIM/data; unpaid account; SLA without escalation contacts; backup service excluded from support; one vendor holding all credentials.
People	One person knows the passwords, switch-over steps, supplier contacts or reconciliation process.

CISA's dependency guidance makes the wider point: systems and services are interdependent, and co-located operations can be exposed to one disruption. Mapping dependencies is therefore a better investment tool than buying duplicates without understanding what they share. [9]

11 A simple downtime-cost estimate - useful, not falsely precise

Downtime cost is a management estimate. Its purpose is to compare priorities and justify proportionate controls. It is not an accounting fact and should not be presented to the nearest rand as if every minute of work and every delayed sale were known.

SIMPLE FORMULA People materially affected x outage hours x loaded hourly employment cost x estimated productivity loss percentage

Worked example for the 25-person scenario

Input	Assumption	Reason
People materially affected	20	Five people can continue useful work with local files, calls or pre-planned offline tasks.
Duration	4 hours	Fibre fails first; power fails one hour later; normal service returns after four hours.
Loaded hourly employment cost	R220	Illustrative management assumption including salary and employer costs. Replace with the SME's own defensible figure.
Average productivity loss	65%	Some work continues, but customer service, cloud work and coordination are materially impaired.
Estimated productivity exposure	R11,440	$20 \times 4 \times R220 \times 65\% = R11,440$.

It is **more honest** to report this as approximately R11,000 to R12,000 of productivity exposure, before evidenced recovery effort or customer impact, than as an exact loss of R11,440.

Case	Loss factor	Four-hour productivity exposure
Lower disruption	40%	R7,040
Working estimate	65%	R11,440
Severe disruption	80%	R14,080

What may be added - carefully

- Verified overtime or recovery time after systems return.
- Lost contribution margin on orders genuinely lost, not total revenue delayed.
- Contract penalties, emergency supplier charges or outsourced printing supported by evidence.
- A qualitative rating for customer trust, safety or regulatory impact where money would be speculative.

Avoid double counting. If staff cost is already included as lost productive time, do not automatically add their full time again as lost sales. Keep the estimate simple enough that a manager can challenge every input.

12 The Four-Hour Business Survival Test

Run this as a controlled tabletop exercise first. Then perform agreed technical tests in a maintenance window. Do not disconnect safety, fire, security or customer-critical systems without authority, competent supervision and a rollback plan.

Stage	Objective	Test activity	Evidence
Before	Set scope and safety	Name critical functions, incident leader, technical lead, observers, suppliers on standby and stop conditions.	Approved test plan; current contact list
0-15 min	Detect and declare	Simulate or isolate primary fibre. Confirm alerting, incident authority, staff message, customer contact route and outage log.	Timestamps; alerts; named leader
15-45 min	Operate on backup	Verify LTE/secondary path, critical apps, inbound/outbound calls, DNS/VPN, MFP workflow and bandwidth controls.	Screenshots/logs; call test; transaction test
45-60 min	Degrade deliberately	Pause non-essential traffic; confirm who can work offline; document unavailable functions and approved workarounds.	Traffic policy; staff observation
At 60 min	Add power failure	Under an approved method, test loss of normal power to the technology chain or simulate it against verified circuit/runtime evidence.	Circuit list; runtime start; safety observer
1-3 hours	Sustain service	Check router, ONT, switches, Wi-Fi, voice, cameras, recording, access-control behaviour, selected devices and battery trend.	30-minute status log; exception list
3-4 hours	Prepare recovery	Prioritise restoration, protect manual records, communicate expected recovery, and check supplier escalation performance.	Recovery order; customer update
At 4 hours	Restore and reconcile	Return power and fibre in the approved order. Check routes, calls, cloud sync, duplicate records, print queues, scans, footage and access events.	Reconciliation signed by process owners
Within 2 days	Adapt	Record actual runtime, failed assumptions, near misses, commercial decisions, owners and due dates. Update the resilience decision record.	Approved action register

Pass criteria

- No life-safety or access-control outcome is left to assumption.
- The incident is detected and owned within 15 minutes.
- Named customer-facing and financial functions operate at the agreed minimum level.
- Voice and essential data are usable on the backup path under realistic load.
- The full communications and security dependency chain meets the required runtime.
- Manual records are controlled and reconciled once, with no unexplained data loss or duplicate action.
- The test produces decisions and owners, not only technical observations.

13 SME Technology Resilience Checklist

Use Pass only where there is evidence. 'We bought it' or 'the supplier says it works' is not test evidence.

Area	Check	Result	Owner / due date
Business priorities	Critical functions and four-hour minimum service levels are approved.	Pass / Action / Not tested	
Ownership	Incident leader, technical owner, process owners and alternates are named.	Pass / Action / Not tested	
Dependency map	Power, connectivity, network, cloud, device, supplier and people dependencies are mapped.	Pass / Action / Not tested	
Primary fibre	SLA, support path, account status, last-mile/FNO and building entry are known.	Pass / Action / Not tested	
Backup path	Technology/provider diversity, coverage, capacity, data and public-IP behaviour are verified.	Pass / Action / Not tested	
Automatic failover	Fibre has been physically disconnected and recovery tested under realistic load.	Pass / Action / Not tested	
Traffic priority	Critical apps are prioritised; guest Wi-Fi and bulk traffic can be paused.	Pass / Action / Not tested	
Voice	Inbound diversion, mobile/softphone use, outbound calling and call logs are tested.	Pass / Action / Not tested	
Cloud files	Selected operating files are locally available and open with the network off.	Pass / Action / Not tested	
Email	Actual client, cached period, shared mailbox and offline-send behaviour are understood.	Pass / Action / Not tested	
Identity	At least two authorised administrators and protected recovery methods exist.	Pass / Action / Not tested	
MFP printing	Critical print path works or has an authorised temporary method.	Pass / Action / Not tested	
MFP scanning	Each critical destination has been tested for failure, queueing and recovery.	Pass / Action / Not tested	
CCTV	Local recording, remote viewing, retention, clock and outage alerts are tested separately.	Pass / Action / Not tested	
Access control	Fail-safe/fail-secure behaviour, safe egress, keys and visitor process are documented.	Pass / Action / Not tested	
Power scope	ONT, firewall, switches, PoE, Wi-Fi, voice, NVR and controllers are on intended circuits.	Pass / Action / Not tested	
Power runtime	Measured runtime under the real load meets the approved requirement.	Pass / Action / Not tested	
Supplier readiness	Current escalation contacts, response commitments and after-hours authority are available offline.	Pass / Action / Not tested	
Manual control	Outage logs, temporary records, approvals and reconciliation steps are ready.	Pass / Action / Not tested	
Review cycle	Quarterly checks and an annual four-hour test are scheduled with owners.	Pass / Action / Not tested	

SUGGESTED SCORING Pass = evidence is current. Action = a gap is accepted with an owner and due date. Not tested = treat as a gap until proved.

14 Technology Resilience Decision Record

Complete one record for each material decision. Keep the reasoning, not only the chosen product. This prevents the same debate being repeated when suppliers, staff or technology change.

Decision title	
Business function protected	
Decision owner and date	
Failure event in scope	
Minimum acceptable service	
Maximum tolerable disruption	
Current dependency chain	
Single points of failure	
Options considered	
Chosen control or workaround	
Why this is proportionate	
Cost basis and assumptions	
Residual risks accepted	
Test method and pass criteria	
Evidence location	
Action owner and due date	
Next review date	
Approvals	

15 A practical closing: resilience is a management habit

SMEs do not need an enterprise-sized continuity programme to make meaningful progress. They need a clear view of the work that matters, the dependencies underneath it, the minimum acceptable service, and the few failures that could stop too much at once.

The first improvement is often inexpensive: update the escalation list, test the LTE SIM, keep selected files offline, move the comms cabinet onto the intended backup circuit, document phone diversion, label manual keys, nominate a second administrator, or stop guest traffic during failover.

Larger investments should follow evidence. If the Four-Hour Business Survival Test shows that a single switch disables voice, Wi-Fi, cameras and access control, that is a better business case than a generic promise of 'more uptime'. If LTE cannot support the busy-hour workload, the test tells management whether to reduce the protected workload or fund a stronger independent path.

FINAL QUESTION When something fails, can the business continue its most important work safely, communicate honestly, protect its records and recover in control? If the answer is based on a recent test rather than confidence, the business is becoming resilient.

This report is educational and should be adapted to the business's risk, contracts, site, safety obligations and technical design. Fire, electrical, access-control and life-safety decisions require competent professional input.

Sources and fact-check notes

Claims were checked against the authoritative and technical sources below on 13 August 2026. Product documentation is used only to confirm specific platform behaviour; it is not treated as proof of performance at a particular customer site.

- [1] **NIST Computer Security Resource Center - Cyber resiliency glossary; Developing Cyber-Resilient Systems (SP 800-160 Vol. 2 Rev. 1).** [Open source](#)
Supports the anticipate, withstand, recover and adapt framing.
- [2] **ICASA - The State of the ICT Sector in South Africa 2026 report.** [Open source](#)
Reports 2025 national 4G/LTE population coverage of 99.5% and urban provincial coverage of 98%-100%; population coverage does not guarantee service at an individual premises.
- [3] **Eskom - Stronger system performance update, 17 July 2026.** [Open source](#)
Source for the dated load-shedding and EAF figures. Local outage risk is a separate operational consideration.
- [4] **Axis Communications - Fail-safe vs fail-secure: what is the difference and how to choose, 2026.** [Open source](#)
Supports the basic power-loss behaviour of door locks; site decisions must follow applicable safety and security requirements.
- [5] **Microsoft Learn - Survivable Branch Appliance for Teams Phone Direct Routing.** [Open source](#)
Shows that local PSTN survivability is a specific designed architecture, not an automatic property of cloud calling.
- [6] **Microsoft Learn - Microsoft 365 service health and continuity.** [Open source](#)
Supports provider service-health and continuity statements.
- [7] **Microsoft Support - Save disk space with OneDrive Files On-Demand for Windows.** [Open source](#)
Supports online-only versus locally/always-available file behaviour.
- [8] **Microsoft Support - Turn on Cached Exchange Mode.** [Open source](#)
Supports offline mailbox access in classic Outlook and the stated limitation for new Outlook for Windows.
- [9] **CISA - Infrastructure Dependency Primer: Learn and Implement.** [Open source](#)
Supports mapping dependencies, shared failure exposure and continuity measures.