thirdoctet

IT & Operations

Continuity Checklist

About US

thirdoctet

We are a Managed IT Services provider for small to medium-sized businesses looking to support and empower their employees with IT that enables them to be at their best in today's remote and hybrid work environment.

Our vision is bettering your world through innovative and meaningful technology. We design, implement and manage technology solutions as a means to anywhere access, from any device, from any network, for Work Life Balance, improving engagement, productivity and profit for our clients.

IT & Operations Continuity Checklist

Break the Hero Dependency and Build Business Resilience

Every business has a "hero."
They're the person everyone calls when something breaks. The one who "just knows" how things work. The one who hasn't taken a real vacation in years.
Heroes keep businesses running - but they also create hidden risk. When critical systems, passwords, and processes depend on one person, even a short absence can cause real disruption.
This checklist walks you through how to identify those risks, document what matters, and build coverage that doesn't rely on heroics. It's practical, detailed, and honest about the work involved - because continuity isn't a one-time project. It's a discipline.

1. Identify Your "Heroes" and Single Points of Failure

Who are the go-to problem solvers in your organization? Start by mapping out dependencies:

□ List all employees who are regularly called upon to fix technical issues, troubleshoot systems, or answer "how do I...?" questions
□ Identify critical business functions that rely on a single person (e.g., payroll processing, network maintenance, CRM management, report generation)
□ List vendors and third-party services your business could not operate without for more than 24–48 hours (e.g., internet provider, cloud hosting, payroll processor, payment processor)
□ Note systems or processes where only one person has login credentials, access, or knowledge
□ Document recurring bottlenecks (e.g., "We can't do X until Jane gets back")
□ Ask your team: "If [Person] was unavailable for two weeks, what would stop working?"

IT & Operations Continuity Checklist

2. Map Responsibilities and Create Backup Coverage

For each critical function, ensure multiple people can handle it:

□ Create a responsibility matrix showing who handles each critical task and who their backup is
□ Assign primary and secondary owners for each system, tool, or process
□ Ensure backup personnel are trained and can step in within 24-48 hours
□ Schedule regular knowledge-sharing sessions (monthly or quarterly) where "heroes" teach others
□ Test backup coverage by having secondary owners handle tasks while primary owners are available to support

Sample Responsibility Matrix:

Critical Function	Primary Owner	Backup Owner	Last Reviewed
Payroll Processing			
Financial Reporting			
Network/Wi-Fi Issues			
CRM Management			

If you're realizing how many tasks rely on one person, you're not alone.
Most SMBs discover far more single points of failure than they expected - especially once they start mapping responsibilities.

If you want a second set of eyes, we can walk through your top risk areas together in about 30 minutes and help you prioritize what actually matters.

Schedule a Free Operational Risk Review

thirdoctet

IT & Operations Continuity Checklist

Most SMBs can complete Steps 1–2 on their own. Steps 3–7 are where execution usually stalls - not because they're impossible, but because they require time, coordination, and technical follow-through.

3. Document Critical Systems and Workflows

Create documentation that anyone can follow, even without the "hero" present:

□ List all critical systems (software, hardware, cloud services) your business depends on daily
□ Document login credentials and store them securely (password manager, secure vault)
□ Write step-by-step procedures for common tasks (e.g., "How to reset the printer," "How to pull a sales report")
□ Include screenshots or screen recordings for complex workflows
□ Create an "emergency contacts" list with vendor support numbers, IT support, and escalation procedures
□ Maintain a network diagram showing how systems connect and where data flows
□ Document software licenses, renewal dates, and account ownership
□ Confirm your cyber insurance policy is current and explicitly covers business interruption, data recovery, forensic investigation, and incident response costs
□ Ensure key contracts, agreements, and insurance policies are stored in a secure, shared location that is not dependent on a single system or physical office

This is usually where progress slows down.
Documenting systems, workflows, and access points is critical - but it's also time-consuming and easy to postpone when day-to-day work takes over.

If documentation has been "on the list" for months (or years), we can complete this step for you in 1–2 weeks, using your team's input without disrupting operations.

Learn How Our Documentation Process Works

thirdoctet

IT & Operations Continuity Checklist

4. Establish Sustainable Processes

Move from relying on individuals to relying on systems:

□ Create a centralized knowledge base or shared drive where all procedures are stored
□ Implement a ticketing or task management system to track recurring issues and solutions
□ Set up automated alerts for system failures, low inventory, or other critical events
□ If your business depends on a physical office, is there a documented plan for how operations would continue remotely, including system access, communication protocols, and leadership oversight?
□ Schedule quarterly "continuity drills" where backup personnel handle primary responsibilities
□ Hold regular documentation reviews to ensure procedures stay current (recommend quarterly)
□ Establish an onboarding checklist that includes training on critical systems
□ Create escalation protocols: "If X happens, contact Y, then Z"

5. Technology & Access Management

Ensure critical technology doesn't become a single point of failure:

□ Audit who has admin access to critical systems (email, CRM, accounting software, cloud storage)
□ Ensure at least 2-3 people have admin credentials for each critical system
□ Set up password managers for shared accounts (avoid sticky notes or personal storage)
□ Enable multi-factor authentication (MFA) on all critical accounts
□ Review and update access permissions when employees change roles or leave
□ Create a process for emergency access (e.g., break-glass accounts for true emergencies)
□ Document vendor relationships and contracts in a shared location

Continuity breaks down fast when access isn't clear.
If you're unsure who has admin access, where credentials are stored, or how you'd regain control in an emergency, that's a real risk - not an edge case.

Our Security & Access Review helps you understand who has access to what, where gaps exist, and what to fix first.

Request a Free Security & Access Review

thirdoctet

IT & Operations Continuity Checklist

6. Communication & Culture Change

Build a culture where knowledge-sharing is valued and heroism isn't required:

□ Communicate to your team why continuity planning matters (business stability, reduced stress)
□ Recognize and reward employees who document processes and train others
□ Make it safe for "heroes" to step back without feeling they're letting the team down
□ Set expectations that asking "where is this documented?" is normal and encouraged
□ Schedule regular check-ins to review continuity plans with your team
□ Celebrate when backup coverage works successfully (e.g., someone handled an issue while the primary owner was out)

7. Test Your Continuity Plan Regularly

A plan that isn't tested is just a document. Make continuity part of your routine:
□ Run a quarterly "hero vacation simulation" where key people are unavailable and backups step in, known as "tabletop exercises"
□ Track how long it takes backup personnel to complete critical tasks (aim to reduce this over time)
□ Review and update your documentation after each test—what was missing or unclear?
□ Solicit feedback from backup personnel: "What would have helped you complete this faster?"
□ Update your responsibility matrix and contact lists at least every 6 months
□ Add continuity planning as a standing agenda item in leadership meetings

IT & Operations Continuity Checklist

Your Continuity Action Plan

Now that you've completed the checklist, prioritize your next steps. Use the table below to plan your continuity improvements:

Action Item	Owner	Deadline	Status

Quick Win Recommendations (30 Days)

Week 1: Identify your top 3 "heroes" and list the critical functions they handle alone
Week 2: Document passwords and access credentials in a secure password manager
Week 3: Assign backup owners for your top 3 critical functions
Week 4: Create basic documentation for your most frequently asked "how do I...?" questions

If this checklist feels overwhelming, that's a sign you're taking it seriously.
For most SMBs, completing this work internally takes months - and often stalls once more urgent issues pop up.

Our IT Continuity Planning service completes everything in this checklist within 30–60 days, working alongside your team so nothing lives only in our heads.

Schedule a Free Continuity Planning Call

IT & Operations Continuity Checklist

Final Thought

How Continuity Actually Works in Real Businesses

Business continuity isn't a one-time project - it's an ongoing discipline. The goal isn't to fix everything at once, but to steadily reduce risk where it matters most.

The businesses that make real progress tend to:

- *Start with their highest-risk dependencies, not the easiest tasks*
- *Focus on progress over perfection*
- *Build documentation and backup coverage into normal operations*
- *Review and update continuity plans quarterly, not annually*
- *Celebrate when backup plans actually work*

Whether you handle this internally or with outside help, what matters most is that the work gets done - and kept current.

Contact Us

info@thirdoctet.com
(647) 728-0610
thirdoctet.com

Schedule a Call >

thirdoctet

Guiding Modern SMB

Want more insights like this?

(647) 728-0610 or info@thirdoctet.com

THIRDOCTET.COM

thirdoctet