Business Continuity Plan Checklist

Costly downtime for your business is unacceptable, no matter how long it lasts. Any event that causes you to lose revenue, productivity, customer confidence or puts people at risk could potentially lead to larger problems in the near future.

Developing and instituting a business continuity plan is crucial to avoiding easily preventable downtime. We have put together a checklist of important steps and factors common to nearly every type or size of business for you to review with your staff and develop a business continuity plan specific to your own organization.

1. Planning

	Not Started	In Process	Complete
Identify and appoint a business continuity (BC) coordinator in your organization.	☐	☐	☐
Identify and appoint a business continuity team to work with your BC coordinator.	☐	☐	☐
Define your organization's business continuity plan in writing and distribute it to staff.	☐	☐	☐
Define specific processes in your organization that are critical, and those that may be able to be paused in the event of downtime to concentrate on critical processes.	☐	☐	☐
Identify issues that can lead to downtime, such as power loss, internet connectivity loss, data loss, inclement weather prohibiting travel, equipment failure, pandemic, physical damage to your facilities, etc.	☐	☐	☐
Identify key employees and stake holders, then develop an escalation list in the event of an incident that can or does lead to downtime. Identify secondary employees in the event the primary is unavailable.	☐	☐	☐
Conduct a Business Continuity Impact Analysis to identify anticipated loss based on your business model. How much money does your organization stand to lose in the event of one hour of downtime? Consider average sales lost, employee compensation, costs of utilities, resolution costs, etc.	☐	☐	☐
Identify a backup site to receive delivered materials (if applicable).	☐	☐	☐
Identify key employees who need company account (credit card, checking, etc.) access to pay for recovery services or materials if key management are unavailable.	☐	☐	☐

2. Technology

	Not Started	In Process	Complete

A. Building

Identify technology currently in place to avoid and/or be impacted by downtime, including building alarms, security cameras, door entry systems, smoke detectors, environmental monitors and sensors, sump pumps, and power generators.	☐	☐	☐
Identify areas of your facilities not currently covered under existing technology and examine to see if coverage should be extended to protect your network, hard goods, and building integrity.	☐	☐	☐

Technology (continued)

	Not Started	In Process	Complete
Visually inspect mechanical and technical equipment to confirm it is in good working order, all cabling is plugged in and secured, sensors are clean and free of dust/dirt, backup technology is on hand in the event a swap is required.	☐	☐	☐
Identify regional causes of potential downtime (i.e. earthquakes, blizzards, tornadoes, hurricanes, typhoons, floods, power grid failure) and determine if your existing monitoring technology provides warning of impact to your facilities and/or automatic corrective response. Causes can include frozen pipes due to cold, high temperatures due to HVAC loss, leaks due to rain or snow melt, river flooding, etc.	☐	☐	☐
Identify technology partners and vendors who would be critical to bringing your network, devices, and facilities back online in the event of downtime. This may include Internet and phone carriers, Managed Service Providers, power company, HVAC, electricians, plumbing, building security, etc.	☐	☐	☐

B. Network

Identify data backup and protection in place. Put offsite backup processes in place if not currently installed. Document data recovery process & test regularly.	☐	☐	☐
Verify backup internet connectivity is in place. Regularly test for failover in the event the primary connection goes down or is not available.	☐	☐	☐
Identify minimum technology required for staff to securely work offsite remotely.	☐	☐	☐
Identify and provide communication tools for staff including soft phones, collaboration software, cloud-based platforms for word processing, spreadsheets, accounting, receivables and more.	☐	☐	☐
Identify key servers and appliances and develop calendar to ensure they are always up to date, patched, targeted for replacement prior to failure, etc.	☐	☐	☐
Develop checklist of key equipment, property and processes that need to be checked in the event of an emergency and person responsible for checking each.	☐	☐	☐
Ensure firewall definitions and any licensing subscriptions are up to date.	☐	☐	☐
Ensure anti-virus software is up to date.	☐	☐	☐
Ensure passwords & login details are accessible to proper staff for systems access.	☐	☐	☐

3. Communications

	Not Started	In Process	Complete
Establish a communications list for all employees and essential vendors. Review it regularly to ensure contact information is up to date.	☐	☐	☐
Provide escalations contact list to employees for assigned responsibilities.	☐	☐	☐
Provide written business continuity plan to key teams and employees. Review and update it regularly.	☐	☐	☐
Provide essential vendors with parts of your written business continuity plan they are directly involved in. This also includes building management (if renting or leasing), facility managers as well as security providers (if applicable).	☐	☐	☐
Provide testing to all facets of business continuity plan to identify any points of failure. This includes remote employee access, data backups, hardware failover, monitoring alerts, etc.	☐	☐	☐

Communications (continued)

	Not Started	In Process	Complete
Provide regular updates to staff on any changes or additions to the established business continuity plan.	☐	☐	☐
Review notifications and alerts generated by environment monitors and security hardware/software to ensure they are being delivered to the correct staff members and vendors.	☐	☐	☐

4. Recovery and Review

	Not Started	In Process	Complete
Determine if an event should trigger any or all of your established Business Continuity Plan.	☐	☐	☐
Determine steps required to ensure business recovery.	☐	☐	☐
Determine, if possible, the ETA to business recovery.	☐	☐	☐
Communicate updates at all times to affected staff and vendors.	☐	☐	☐
Enact previously determined plan to enact either ongoing remote business activity, or full business recovery.	☐	☐	☐
Once business recovery is complete, enact full review of implementation of business continuity plan to identify areas to be revamped for better/faster performance.	☐	☐	☐
Review business continuity plan on a regular ongoing basis and modify based on updated infrastructure, technology, and staff.	☐	☐	☐

Notes

The most important factor in your Business Continuity Plan is the process of constantly and repeatedly reviewing, testing, and revamping to ensure your company will always be protected against costly unexpected downtime.

To learn more about business continuity and protecting your organization against downtime caused by environment factors such as temperature, humidity, water leaks, power loss, smoke and more, please visit RoomAlert.com for more helpful articles, white papers, videos and resources.

AVTECH™

RoomAlert®
We've got this.

AVTECH Software, Inc. • 401.628.1600 • Sales@RoomAlert.com • RoomAlert.com