Linux Association of Canada

LINUX ASSOCIATION OF CANADA PUBLIC GUIDE

BACKUPS, BUSINESS CONTINUITY & DISASTER RECOVERY

Keeping Canadian Organizations Operating During Disruptions

PROTECT YOUR DATA
Reliable backups when you need them.

ENSURE CONTINUITY
Keep operations running during disruptions.

RECOVER WITH CONFIDENCE
Restore systems and data quickly and securely.

REDUCE RISK AND IMPACT
Minimize downtime, protect your reputation.

CANADIAN FOCUS COMMUNITY STRONG
Practical guidance for Canadian organizations

About This Guide

Every year, Canadian organizations face disruptions that threaten their operations. Some recover quickly and continue serving their communities. Others struggle for weeks, lose critical data, or cease operations entirely. The difference is not luck—it is preparation.

Why Organizations Fail After Incidents

When disaster strikes, organizations without recovery plans face cascading failures. Lost data cannot be recreated. Critical systems remain offline for days or weeks. Staff cannot access the information needed to serve customers or clients. Financial records disappear. Communication breaks down. What begins as a technical problem becomes an organizational crisis.

The statistics are sobering. Studies consistently show that organizations experiencing major data loss without adequate backups face a high probability of closure within months. Even those that survive often suffer permanent damage to reputation, customer relationships, and financial stability.

Prevention vs. Recovery: Both Are Essential

Many organizations invest heavily in prevention—firewalls, antivirus software, physical security, and access controls. These measures are important and necessary. However, prevention alone is insufficient.

No security measure is perfect. Hardware fails. Natural disasters occur. Human errors happen. Sophisticated attacks bypass defenses. The question is not whether your organization will face a disruption, but when—and whether you will be prepared to recover.

Recovery planning acknowledges reality: incidents will occur despite our best prevention efforts. The goal is ensuring that when disruption happens, your organization can restore operations, recover data, and continue serving your community with minimal interruption.

Why Every Organization Needs a Continuity Plan

Business continuity and disaster recovery planning is not exclusively for large enterprises or technology companies. Every organization—regardless of size, sector, or technical sophistication—depends on digital systems and data. Municipal governments, healthcare providers, educational institutions, non-profits, small businesses, and community organizations all face similar risks and require similar protections.

A continuity plan provides:

- **Clear procedures** for responding to incidents
- **Defined roles** so everyone knows their responsibilities
- **Tested recovery methods** that actually work when needed
- **Alternate operations** to maintain critical services during disruptions
- **Communication protocols** to coordinate response and keep stakeholders informed

Intended Audience

This guide is designed for decision-makers and professionals responsible for organizational resilience:

- Executive directors and senior management
- IT managers and system administrators
- Operations managers
- Board members and governance committees

- Business continuity coordinators
- Anyone responsible for ensuring their organization can weather disruptions

You do not need deep technical expertise to understand and implement the principles in this guide. We explain concepts clearly and focus on practical, actionable steps appropriate for Canadian organizations of all sizes.

Why Recovery Matters

Disruptions affecting Canadian organizations come in many forms. Understanding the range of potential incidents helps organizations prepare comprehensive recovery strategies rather than planning for only the most obvious threats.

Fires

Fire remains one of the most devastating physical threats to organizational infrastructure. A server room fire can destroy hardware, damage facilities, and render entire buildings unusable. Even small fires create smoke damage that can contaminate equipment throughout a facility. Fire suppression systems, while protecting lives and buildings, often cause water damage to electronic equipment.

Recovery from fire requires off-site backups and alternate facilities. Organizations with only on-site backup systems lose both primary and backup data simultaneously.

Floods

Canadian organizations face increasing flood risks from spring runoff, severe storms, and aging urban infrastructure. Basement server rooms are particularly vulnerable. Even minor flooding can destroy servers, network equipment, and backup devices. Water damage often affects multiple floors as it seeps through buildings.

The 2013 southern Alberta floods and recurring Ottawa River flooding demonstrate that Canadian organizations in diverse regions face flood risks. Climate change is increasing both the frequency and severity of flood events.

Hardware Failures

Storage devices, servers, and network equipment eventually fail. Hard drives have limited lifespans. RAID arrays experience multiple disk failures. Power supplies burn out. Cooling systems malfunction, causing equipment overheating. These failures are not possibilities—they are certainties over sufficient time.

Organizations relying on single systems without backup protection will experience data loss when hardware inevitably fails. The question is whether you will lose hours, days, or years of work.

Ransomware

Ransomware has become one of the most significant threats facing Canadian organizations. Attackers encrypt organizational data and demand payment for decryption keys. Even organizations that pay ransoms often cannot fully recover their data.

Recent attacks have targeted Canadian municipalities, healthcare facilities, and businesses of all sizes. Modern ransomware specifically seeks and attempts to encrypt backup systems, making recovery impossible for organizations without properly protected backups.

Immutable and air-gapped backups—discussed later in this guide—provide protection against ransomware by ensuring attackers cannot modify or encrypt backup copies.

Human Mistakes

Accidental deletion, misconfigured systems, and well-intentioned errors cause frequent data loss. An administrator accidentally deletes a critical database. A staff member overwrites important files. A system update goes wrong and corrupts data. A configuration change breaks essential services.

Human errors are inevitable in complex technical environments. Recovery capabilities allow organizations to restore data and systems to known-good states before mistakes occurred.

Power Failures

Extended power outages affect Canadian organizations regularly, particularly during winter storms and summer severe weather. While uninterruptible power supplies (UPS) provide short-term protection, extended outages exhaust battery backup and require system shutdowns.

Power failures can corrupt databases, damage storage systems, and interrupt critical processes. Organizations need both power protection and recovery procedures for systems affected by unplanned shutdowns.

Internet Outages

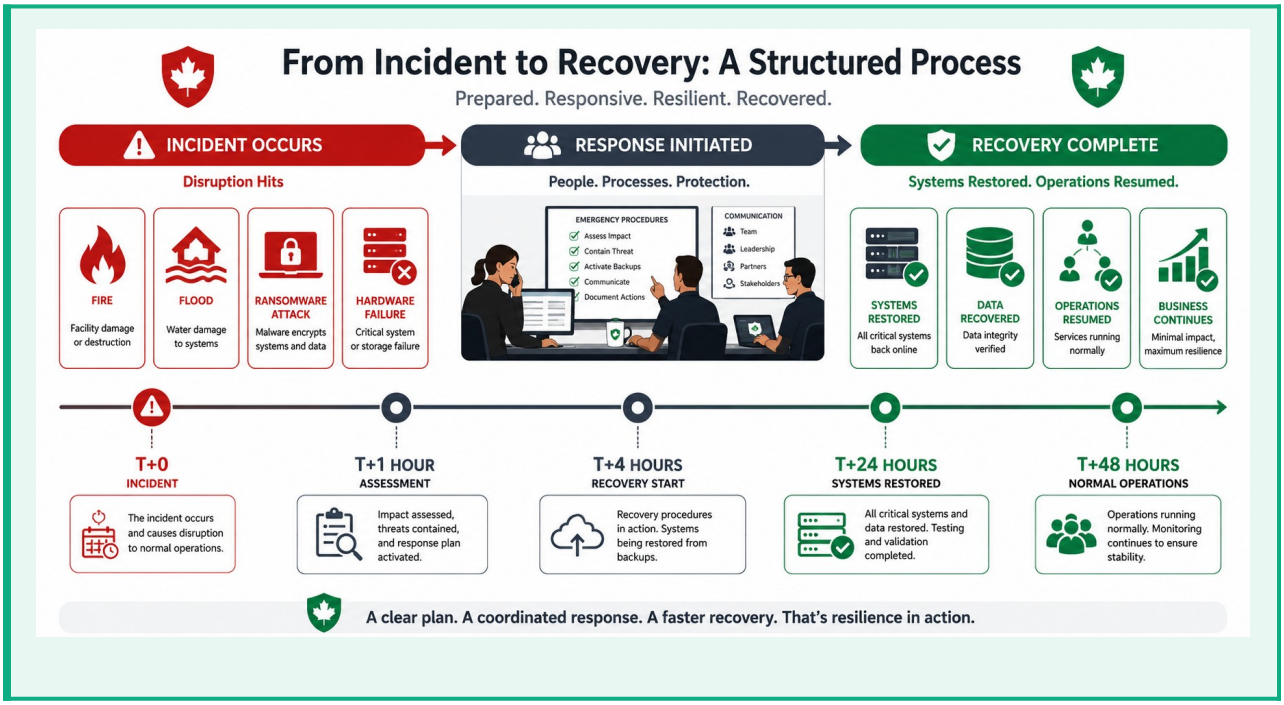
Modern organizations depend on internet connectivity for cloud services, email, customer interactions, and inter-office communications. Internet service provider failures, fiber cuts, and routing problems can isolate organizations from critical cloud-based systems.

Organizations relying exclusively on cloud services without local backup copies may be unable to access essential data during internet outages. Hybrid approaches combining local and cloud backups provide resilience against connectivity failures.

Recovery Planning Is As Important As Prevention

Each of these scenarios demonstrates why recovery planning complements prevention. You cannot prevent all hardware failures, natural disasters, or human errors. You can ensure your organization survives them through tested backup systems, documented procedures, and practiced recovery plans.

The remainder of this guide provides the knowledge and tools to build organizational resilience through comprehensive backup, business continuity, and disaster recovery strategies.



Understanding Risk

Effective recovery planning begins with understanding the risks your organization faces. Not all risks are equally likely or equally damaging. A structured risk assessment helps prioritize recovery planning efforts and allocate resources appropriately.

Operational Risks

Operational risks arise from the day-to-day functioning of your organization. These include:

Process failures: Critical workflows that break down or cannot be completed due to system unavailability. For example, payroll processing that cannot run, customer orders that cannot be fulfilled, or service delivery that cannot be documented.

Capacity limitations: Systems that become overwhelmed during peak demand or cannot scale to meet organizational needs. Insufficient backup storage, inadequate network bandwidth, or processing bottlenecks that prevent timely recovery.

Dependency failures: Reliance on specific individuals who possess unique knowledge or access. When key personnel are unavailable during incidents, recovery efforts stall because no one else knows critical procedures or passwords.

Technical Risks

Technical risks stem from the technology infrastructure itself:

System failures: Servers, storage devices, network equipment, and workstations that fail due to age, defects, or environmental factors. Single points of failure where one component's breakdown disrupts entire systems.

Software defects: Bugs, compatibility issues, and corrupted applications that cause data loss or system instability. Failed updates that break functionality or introduce vulnerabilities.

Cyber threats: Ransomware, malware, unauthorized access, and data breaches that compromise systems and data. Distributed denial-of-service attacks that make systems unavailable.

Data corruption: File system errors, database corruption, and application failures that render data unusable even when storage hardware functions correctly.

Environmental Risks

Environmental risks come from physical surroundings and natural events:

Natural disasters: Floods, fires, severe storms, earthquakes (in some Canadian regions), and extreme weather events that damage facilities and infrastructure.

Utility failures: Extended power outages, water service interruptions affecting cooling systems, and telecommunications failures that isolate facilities.

Physical security breaches: Unauthorized facility access, theft of equipment, and vandalism affecting systems and data.

Environmental conditions: Excessive heat or humidity, water leaks, roof failures, and building infrastructure problems that damage equipment.

Human Risks

Human factors create significant risks despite best intentions:

Accidental errors: Unintentional deletion, misconfiguration, and mistakes during maintenance or updates. Well-meaning actions that have unintended consequences.

Insufficient training: Staff who lack knowledge to properly maintain systems, perform backups, or execute recovery procedures. Gaps in understanding that lead to improper practices.

Social engineering: Phishing attacks, pretexting, and manipulation that trick staff into compromising security or providing unauthorized access.

Malicious insiders: Deliberate sabotage, data theft, or system damage by current or former staff members with legitimate access.

Supplier Risks

Modern organizations depend on external providers, creating additional risk vectors:

Vendor failures: Service providers experiencing their own disruptions, financial difficulties, or business closures that affect your organization's access to critical services.

Cloud service outages: Downtime at cloud providers that makes your data or applications temporarily unavailable. Regional failures affecting entire data centers.

Supply chain disruptions: Inability to obtain replacement hardware, software licenses, or technical support when needed for recovery.

Contractual gaps: Service level agreements that do not adequately protect your organization's recovery requirements or provide insufficient guarantees.

Risk Assessment in Practice

Understanding these risk categories helps organizations:

- Identify which risks are most likely to affect their specific operations
- Determine which risks would cause the most severe impact
- Prioritize recovery planning efforts toward the highest-priority risks
- Allocate backup and continuity resources appropriately
- Develop comprehensive plans addressing multiple risk scenarios

The goal is not to eliminate all risks—an impossible task—but to ensure your organization can recover from the most likely and most damaging scenarios.

PREVIEW — END OF SAMPLE

You've just read the opening of Backups, Business Continuity & Disaster Recovery

This sample covered why recovery planning matters and how to think about risk. The full 192-page guide continues with practical, Canadian-focused guidance your organization can put into action right away.

The full guide also covers:

- ✓ What a backup actually is (and isn't)
- ✓ What should be backed up — and often gets missed
- ✓ The 3-2-1 (and 3-2-1-1-0) backup rule, explained
- ✓ Local, cloud, and hybrid backup strategies
- ✓ Backup types: full, incremental, snapshots & CDP
- ✓ Business continuity planning fundamentals
- ✓ Disaster recovery procedures and testing
- ✓ Ransomware-resilient backup design
- ✓ Compliance considerations for Canadian organizations
- ✓ Step-by-step recovery plan templates

GET THE FULL GUIDE

linuxassociation.ca