

Best Practices for Digital Audits

In consultation with Paul Jaroszko, Partner
Prentice, Yates and Clark (PYC) Accountants

How long should corporate records be kept?

a minimum
of 7 years

The following documents must be kept permanently:

- Articles of incorporation
- Corporate by-laws
- Funding agreements
- Mortgage documents
- Capital invoices – for insurance purposes, for the life of the asset
- Board and AGM minutes
- RGI – Member Occupancy agreements until 7 years after moving out

Controls maintained electronically

- Ensure approval information is maintained – either scan approved signed invoices or have an e-signature version attached to the invoice
- The final electronic invoice is best supported by accounting calculation, quotes and other documents
- Include a cheque requisition form

Audit documents – add these to the electronic audit folder

- Deposits, all bank statements
- Bank reconciliations
- Investment statements
- CRA letters
- HST notice of assessments
- Corporate tax notice of assessments
- Property tax bills
- Mortgage statements
- Subsidy funding documents and reconciliations
- Insurance policy
- Capital grant documentation
- Employee wage approvals
- Management contracts
- Budgets
- Signed Board and AGM minutes
- Notice of Change forms
- Change of directors
- Management services contracts – property management, bookkeeping services, maintenance & cleaning

If all documents cannot be scanned, the following should be short listed for the exact selection that the auditor would need once accounting records are made available.

- Invoices – used for sample selection by audit team
- RGI calculations, along with supporting income verification documentation

*It's important to have **BACK-UP** systems as part of your **EMERGENCY RESPONSE** plan*

A good way to back-up your files

Portable hard drive – this equipment can get damaged so keep a second copy off-site.

AND/OR

Back-up to the Cloud – however even a back-up of your cloud information is required in case of data corruption.

Key tips

- Remember to back up often, although a key feature with cloud back-ups, this can be set up automatically
- Test the back-up periodically to ensure you'll be able to recover the information
- Ensure the cloud servers are on Canadian soil and rights to the information stored are maintained within your organization

Password protection is key

All log-ins should be password protected. Consider password protection for sensitive documents as an extra layer of protection.

Key tips

- Maintain a password log in case the manager leaves unexpectedly – the log will allow you to continue to access your vital data
- When staff changes, change the password!



Co-op Cost Cutters recommends cloud-based solutions like Barracuda Backup as a great option for co-ops. For more information, contact [Document Direction \(DDL\)](#), a Co-op Cost Cutters supplier.

