

FREE RESOURCE — 2026 EDITION

FINTRAC Technology Risk Management Guide

For Mortgage Brokers, Financial Advisors & Insurance Firms in Canada

DSIT Professional Services Inc. | dsitpro.com | Ontario, Canada

Authority	Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) — fintrac-canafe.gc.ca
Applies To	Reporting Entities: mortgage brokers, financial advisors, insurance companies, money services businesses, casinos, real estate brokers
Key Obligation	Reporting Entities must implement compliance programs including written policies, risk assessment, training, and record-keeping
Risk	Non-compliance penalties range from \$1,000 to \$100,000 per violation — criminal charges possible for willful non-compliance

FINTRAC COMPLIANCE PROGRAM — 5 REQUIRED ELEMENTS

- 1. Written compliance policies and procedures — must be reviewed and updated regularly
- 2. Appointment of a Compliance Officer with defined responsibilities
- 3. Risk assessment — assess your clients, products, services, and delivery channels for ML/TF risk
- 4. Ongoing compliance training for all staff with client-facing roles
- 5. Effectiveness review — assess your compliance program effectiveness every two years

TECHNOLOGY-SPECIFIC FINTRAC REQUIREMENTS

- Electronic records must be maintained in a format accessible to FINTRAC — plain text or PDF, not proprietary encrypted formats
- Records must be retained for 5 years from the date of the last transaction
- Identity verification records must be retained for 5 years
- Systems used for identity verification must produce auditable records
- STR (Suspicious Transaction Reports) submitted electronically via FINTRAC's secure reporting system
- Large Cash Transaction Reports (LCTR) submitted within 15 days of transaction
- Third-party determination records retained for all applicable transactions

IT CONTROLS SUPPORTING FINTRAC COMPLIANCE

- Audit logging: all access to client records and transaction data must be logged with user, date, time, and action
- Access controls: client financial records accessible only to staff with compliance need — role-based access mandatory
- Encryption at rest: all client identity and transaction records encrypted
- Encryption in transit: secure transmission for all STR/LCTR submissions to FINTRAC
- Backup and retention: 5-year minimum retention with verified backup and restore capability
- MFA: required on all systems containing reportable transaction data
- Patch management: systems handling FINTRAC-reportable data must be kept current
- Vulnerability management: annual security assessment recommended for systems in scope

RECORD-KEEPING REQUIREMENTS BY TRANSACTION TYPE

- Cash transactions over \$10,000 — Large Cash Transaction Record (LCTR) within 15 days
- Suspicious transactions — Suspicious Transaction Report (STR) as soon as practicable
- Attempted suspicious transactions — STR even if transaction not completed
- Electronic funds transfers over \$10,000 — EFTR within 5 business days
- Virtual currency transactions — specific reporting requirements, consult fintrac.gc.ca
- Client identification records — retained 5 years from last transaction
- Beneficial ownership records — required for legal entities since June 2021

FINTRAC IT COMPLIANCE CHECKLIST

■ Compliance Officer designated in writing	Name, title documented	■ Written compliance policies in place	Reviewed this year
■ Risk assessment completed	Updated annually	■ Staff training program documented	Records on file
■ Effectiveness review scheduled	Every 2 years minimum	■ Audit logging active on all in-scope systems	Logs retained 5+ years
■ Role-based access controls implemented	Audit completed	■ Encryption at rest on all client records	Tool confirmed
■ Encryption in transit for all FINTRAC submissions	HTTPS/TLS verified	■ 5-year backup retention configured	Last restore test dated
■ MFA on all transaction systems	100% of users enrolled	■ FINTRAC secure reporting system access tested	Login credentials current
■ STR submission process documented	Staff know the procedure	■ LCTR submission process documented	15-day deadline understood

■ Identity verification records retained 5 years	Retention schedule set	■ Annual security assessment conducted	Last assessment dated
---	------------------------	---	-----------------------

GETTING HELP

FINTRAC compliance intersects directly with your IT systems. DSIT Professional Services Inc. helps Canadian financial services firms implement the technical controls required for FINTRAC compliance — including audit logging, access controls, encryption, backup retention, and annual security assessments.

- Book a free financial services IT consultation: dsitpro.com/contact
- FINTRAC guidance: fintrac-canafe.gc.ca

DSIT Professional Services Inc. | help@dsitpro.com | (613) 696-5842 | dsitpro.com | Ontario, Canada | © 2026 All rights reserved.