Business Fraud Prevention Checklist

Practical checks for organizations operating in or with Mexico

Use this checklist to review common control areas. It is an educational starting point, not a formal audit, fraud examination or guarantee that fraud will be prevented.

1. Map the risk

- Identify processes involving money, purchasing, payroll, expense claims, inventory, insurance claims, property and third parties.
- Identify who can request, approve, change and release payments or records.
- List high-value, unusual or time-sensitive transactions that receive limited review.
- Assign an owner to each important control and define how exceptions are escalated.

2. Verify vendors and counterparties

- Confirm the legal or trading name, address, business activity and relevant registration details using independent sources.
- Check whether the person giving instructions is authorized to act for the organization.
- Verify material ownership, management or address changes where relevant and legally available.
- Do not rely only on a website, email signature, social profile or document supplied by the counterparty.

3. Control payment changes

- Treat new or changed bank details as a high-risk request.
- Confirm the change using a contact method already on file, not the phone number or link in the change request.
- Require a second approval for sensitive changes where practical.
- Keep a record of the person who verified the change, the method used and the approval.

4. Strengthen internal controls

- Separate payment initiation, approval and release where the size of the organization allows.
- Review unusual transactions, duplicate invoices, repeated exceptions and manual overrides.
- Limit system and account access to what each role needs.
- Review access when employees change roles or leave.
- Use management review and data monitoring proportionate to the organization's risk and resources.

5. Make reporting usable

- Provide a clear route for employees and relevant third parties to raise concerns.
- Explain who receives reports, how they are assessed and how confidentiality is handled.
- Train employees and managers to recognize warning signs and report facts without making accusations.
- Record the report, date, source, initial assessment and next action.

6. Preserve records and respond

- Preserve original emails, messages, invoices, contracts, payment confirmations, system logs and relevant files.
- Keep original files unchanged and use working copies for notes.
- Create a dated timeline and identify what is known, disputed and unknown.
- Limit access to case material and involve appropriate legal, compliance, HR or investigative professionals.
- Do not confront a subject or conduct intrusive checks without considering safety, legal authority and evidence risks.

7. Review and improve

- After an incident or near miss, identify which control failed or was bypassed.
- Update procedures, access rights and training where justified.
- Test whether the revised control works in practice.
- Keep a record of lessons learned and outstanding risks.

A warning sign is not proof of fraud. Verify facts, consider alternative explanations and document limitations.

GrayCat PI | Mexico | +52 55 4519 8742 | GrayCatPI.com
WhatsApp: +52 55 4519 8742

Sources: ACFE, Occupational Fraud 2026: A Report to the Nations, https://www.acfe.com/rttn. ACFE/Fraud Week resources, https://www.fraudweek.com/resources.