



Community Library

ISO 27001 Payment and Wire Verification

Ten checks that stop fake invoices, swapped bank details, and fake CEO requests.

4

Controls

4

Before you pay

2

If money moves

1.0 · 2026-10

itrygg.com

How to use this checklist

A fake invoice, a swapped bank account, or a message that sounds like the CEO can move money before anyone notices. Give this list to the people who approve payments. Each step also names the proof your ISO/IEC 27001 program should already be able to show.

- 1. Work the parts in order: set the controls, check before you pay, then act if money moves.
- 2. The Proof line is the record your program keeps. If you cannot produce it, the task is not done.
- 3. References point to ISO/IEC 27001:2022 Annex A controls, for example A.5.3.
- 4. Post this where payments are approved. Confirm recovery steps with your bank, insurer, and counsel.

Controls	Before you pay	If money moves
Before a payment is set up	Before the money leaves	After a payment leaves

Set the controls

Two people, a written threshold, the bank's own controls, and protected finance mail.

- ☐ One person sets up a payment and a different person approves it, every time. A.5.3
Proof: The rule, and the names of the person who sets up payments and the person who approves them.
- ☐ Write down the amount above which a payment needs a senior approval, and hold to it. A.5.1, A.5.3
Proof: The written threshold, and a payment above it that shows the senior approval.
- ☐ Turn on dual approval, a payee list, daily limits, and alerts in the banking portal. A.5.3, A.5.15
Proof: The bank settings as they stand, with the date they were checked.
- ☐ Turn on MFA for every finance inbox, and alert when a new forwarding rule appears. A.8.5, A.8.16
Proof: MFA on those inboxes, and the alert for a new forwarding rule.

Before you pay

A known phone number, a pause on pressure, a second channel for a leader, and a look at the address.

- ☐ Verify a new payee, and any bank-detail change, by calling a number already on file. Do not use the number in the email. A.5.14, A.5.19

Proof: The call record: who was called, the number already on file, and the date.

- ☐ Slow down when a request says urgent, confidential, or do not tell anyone. A.6.3

Proof: The rule staff were given, and a note when a payment was paused for that reason.

- ☐ Confirm a leader's payment request on a second channel that you start. A.5.14, A.6.3

Voices can be faked, so agree a code word in advance.

Proof: A record that the code word was agreed and where it is kept, and which second channel was used.

- ☐ Look at the sender address for a look-alike domain, and a reply-to address that does not match the sender. A.6.3

Proof: The check on the request, or the rule that this look happens before approval.

If money moves

The bank is called at once, then security hears what happened and the lesson is shared.

- ☐ Call the bank right away and ask it to recall or freeze the payment. In the United States, report it at ic3.gov. A.5.26, A.5.5

Proof: The bank call, with the time, and the report if one was filed.

- ☐ Tell security, check the mailbox for compromise, and share the lesson with staff. A.6.8, A.5.27

Proof: The event record, the mailbox check, and the lesson shared.

Want the call-back and the approval to live in the program, not on a sticky note?

Trygg keeps the approval, the call-back, and the proof in one place.

[Book a demo](https://itrygg.com/#demo) (itrygg.com/#demo)

[ISO 27001 Preparation Checklist](https://itrygg.com/community/library/iso-27001-preparation-checklist) (itrygg.com/community/library/iso-27001-preparation-checklist)

Portal demos follow a mutual NDA.

isms@itrygg.com

This checklist is guidance, not a substitute for the ISO/IEC 27001:2022 standard. Purchase the standard from ISO or your national standards body. Certification decisions are made only by accredited certification bodies.

© 2026 Trygg, Inc.