Accountable Person: Date: Version:

# Control Standard Canvas

## Name

A short, clear name for the standard.

Make it specific enough to distinguish from similar standards.
Bad Name: User Access Removal
Good Name: Analyst Role Removal from FinData

## Risk Event

The Risk Event this standard addresses is to mitigate risk.

Use the Risk Event name from your Risk Identification Canvas for which this Control Standard is for.

## Control Objective(s)

A Control Objective states the expected outcome when a risk control is applied.

List the Control Objective(s) this standard fulfills. If from a framework, cite it (e.g., NIST 800-53, ISO 27001).

## Details

Detailed, measurable rules that satisfy the Control Objective and mitigate the Risk Event.

Treat the standard as a performance contract. Anyone should be able to check if it's met, without needing to know how the process, tool, or system works inside.

Define clearly: what must be done, when, and how.

Ensure the standard is:
- Not procedurally specific.
- Verifiable without knowing implementation details.
- Precise enough to be automated.

Good Example: Terminated Employee Access Removal from OpsSys.
- When: Within 24 hours of HR's termination notice.
- How:
  - Termination approved by HR.
  - Employee Identity removed from OpsSys.

Why is this example good?
- It's specific (removal of employee access from OpsSys)
- It's measurable (24 hours, HR request log, OpsSys user log)
- It's verifiable (compare termination date, HR approval, vs. access data)

What would be a bad example?
A bad Control Standard reads like a procedure, full of step-by-step execution details instead of outcome-focused rules.

Bad Example:
- HR emails IT about termination.
- IT opens OpsSys.
- IT searches the employee record.
- IT clicks "Remove User."
- IT confirms deletion.

Why is this bad?
- Too procedural (describes "how to click" instead of "what must be achieved").
- Not portable (only applies if you have OpsSys and that exact screen).
- Not future-proof (breaks if the system changes).
- Harder to verify (you'd need system knowledge rather than just checking logs).

How to turn a procedure into a standard?
When you see a step-by-step list, ask yourself:
- What outcome do these steps achieve?
- How can I state that outcome in a way that is measurable (time, evidence, record)?
- What's the minimum expectation that must always be met, no matter what tool or process is used?

Good Standard: outcome, measurable, verifiable.
Bad Standard: step-by-step "click path," tool-specific instructions.

**DESIGNED BY:** Bill Bensing & Damon Edwards
The creators of Combined Assurance Blueprinting and the Attestify Combined Assurance Model™.

© 2025 Attestify. All rights reserved.
This canvas may be used internally for organizational design and planning purposes. Commercial use, reproduction, or modification requires explicit permission from Attestify, Inc.
https://napecentral.com/combined-assurance-blueprinting

Attestify