Risk Evaluation Canvas

Accountable Person: Date: Version:

Risk Event

[Content Goes Here]

Assurance Action(s)

Assurance Action claims are input data for the Risk Evaluation

Which Assurance Action claims provide the input data for this evaluation?

Risk Tolerance

What level of risk is acceptable?
When does risk become unacceptable?
How much of each Risk Criteria will we accept, and under what conditions?

How much variation is acceptable before escalation?
What is the maximum allowable error/failure rate?
Under what conditions are Low or Medium risks acceptable?
Who is responsible for acting if a High-risk threshold is breached?
What is the escalation path (roles, timing)?

Example:
- Acceptable: We will tolerate Low Risk outcomes (1–2 late removals within 24–168 hours) if corrected within the same quarter.
- Conditionally Acceptable: Medium Risk outcomes (3–5 late removals) may be tolerated only if remediation occurs within 7 days and a root cause is documented.
- Unacceptable: High Risk outcomes (>5 late removals, or any removal beyond 7 days) trigger immediate escalation to the IT Security Manager, who must notify the CISO within 48 hours.

Risk Criteria

Risk Criteria are the rules we use to decide how serious a risk is; they are rules for categorizing risk.

How do we define failure vs. success?
What separates Low, Medium, and High risk?
What thresholds (time, volume, severity) trigger escalation?
Are there compounding factors that raise severity (e.g., repeat issues)?
Is this consistent with the organization's stated risk appetite?

Example
- Failure: Any terminated employee account still active after 7 days.
- Low Risk: 1–2 accounts active >24 hours but <7 days.
- Medium Risk: 3–5 accounts active >24 hours but <7 days.
- High Risk: More than 5 accounts active >24 hours, or any account active beyond 7 days.
- Compounding Factor: Repeat failures across multiple months automatically escalate severity by one level.

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