OPS TOOLS FMEA

Failure Mode and Effects Analysis to identify and reduce risk before pilot, rollout, and standardization. This template is used as a guide, write it out on a whiteboard in-person with a team is more beneficial.

Purpose

Make risks visible, owned, and testable so the team prevents failures at point of cause and holds the gain through PROVE Loop™ checks.

When to Use

Use this tool anytime you are introducing or changing work in a way that could fail in the real world, including a new product line, a pilot program, a new procedure or process, a new standard, or a new work instruction. Use it before a pilot or rollout to prevent predictable failures. Use it after a risk, near miss, incident, complaint, or audit finding to confirm the mitigation is real and to look for related risks that could still exist.

How to Use

Start by naming the change and its scope guardrails so the team is analyzing the same thing. Identify the key steps and decision points where the work can fail, especially at handoffs, exceptions, approvals, system updates, routing, scheduling, and closeout. For each step, write a failure mode that is observable and specific, then describe the effect in real outcomes such as customer impact, delay, rework, safety exposure, compliance exposure, or cost. Score Severity, Occurrence, and Detection using evidence rather than opinion. List the controls that exist today and are consistently used, then define countermeasures that change the work at point of cause and can be tested. If the countermeasure will become a standard, define the PROVE Loop™ check that will detect drift and trigger escalation.

Rules for Objective Scoring

Use one row per step or decision point that can fail. Write failure modes so they can be seen, measured, or verified, and avoid labels like “poor communication.” Every Severity, Occurrence, and Detection rating must cite evidence, such as Go and See observations, logs, audit results, or incident history. Only list a control as “current” if it exists today and is used consistently; if it depends on memory, reminders, or hero behavior, treat it as weak. If evidence is missing, assign an owner and a short due date to gather it and finalize scoring.

Risk Rules

Calculate RPN as Severity × Occurrence × Detection and use one escalation threshold consistently across teams, like 200 or 300. Treat high-severity items as exceptions even when RPN is below threshold. Prefer prevention controls that reduce Occurrence over detection controls that only improve Detection. A countermeasure is not complete until it has an owner, a test date, and a verification method, and it is not ready to standardize until the PROVE Loop™ check is defined with who checks, how often, and what evidence proves it is being followed.

OPS Tools
ORIGIN PROBLEM SOLVIING

Scoring Anchors

Use the best available evidence. If evidence is missing, plan a quick Go and See sample and score again.

Scale	1–3 (Low) **Evidence rule:** "Pick the score using at least one of: (1) Go and See observation, (2) log/audit count, (3) recent example with date."	4–6 (Medium) **Evidence rule:** "Pick the score using at least one of: (1) Go and See observation, (2) log/audit count, (3) recent example with date."	7–10 (High) **Evidence rule:** "Pick the score using at least one of: (1) Go and See observation, (2) log/audit count, (3) recent example with date."
Severity (S) Impact if it happens	Minor nuisance, easy recovery, low cost, no customer impact. • Internal email typo or formatting error corrected before sending. • A non-customer-facing report is late by a few hours and no downstream work stops. • A small rework loop that costs under 15 minutes and does not recur. • A missed optional meeting note that can be recreated from calendar and attendees	Noticeable delay/rework, recurring defects, customer dissatisfaction. • Shows up a few times a quarter in audits or escalations. • A known "every month" issue at month-end close, scheduling, invoicing, or reporting. • Multiple people report "it happens sometimes" and you can find recent examples.	Major service failure, safety/compliance risk, high cost or reputation impact. • Known daily work-around exists, people expect it. • Shows up every week on a dashboard, board, or escalation log. • You can observe it during a short Go and See sample (one shift, one day).
Occurrence (O) How often without new controls	Yearly or less; rare but plausible. • It happens only during annual peak periods or rare exceptions. • Seen once last year, not seen since. • Requires a specific unusual combination of conditions to occur.	Monthly to quarterly. • Shows up a few times a quarter in audits or escalations. • A known "every month" issue at month-end close, scheduling, invoicing, or reporting. • Multiple people report "it happens sometimes" and you can find recent examples.	Weekly to daily. • Known daily work-around exists, people expect it. • Shows up every week on a dashboard, board, or escalation log. • You can observe it during a short Go and See sample (one shift, one day).
Detection (D) Chance to catch before harm	Built-in and immediate; consistently performed. • System prevents submission if required fields are missing (hard stop). • Barcode or scanning verifies right item, right customer, right location before proceeding. • Automated validation flags out-of-range values instantly and blocks the transaction. • Second-person check is standard, happens every time, and is recorded.	Defined and usually works but not guaranteed. • A daily review catches errors, but only after work is already processed. • A supervisor spot check exists, but not every case is checked. • A report exists, but it is reviewed inconsistently or after delays. • Errors are caught when a customer complains or when a downstream team notices.	No reliable detection until after harm or customer impact. • No one checks until after an escalation, complaint, incident, or audit. • The error is invisible in the system and only discovered by chance. • Detection depends on one experienced person noticing something "feels off." • The first reliable signal is rework, an incident, or customer impact.

OPS Tools
ORIGIN PROBLEM SOLVIING

OPS TOOLS FMEA WORKSHEET

Project / Area		**Date**	
Owner (overall)		**FMEA Type (Process / Product / Project)**	
Problem Statement			

Step or Decision Point	Requirement / Standard	Failure Mode (observable)	Effect (what happens)	Evidence / Source	S	O	D	RPN	Countermeasure + Test	Owner + Due	Sustain Plan (Y/N)

Hints: Write failure modes as "If X, then Y." Cite evidence for S/O/D. Prefer prevention controls. Countermeasures must change the work at point of cause. If adopted, define a PROVE Loop™ check (who, cadence, evidence) for sustainment.