

A • Intended use

What does the system decide or suggest, for whom and where?

B • Foreseeable misuse

How might it be used beyond its intended use?

C • Interested parties

Who influences or is affected? Represent one interested party.

D • Causes

What if the input is wrong?
What if the model or code changes?

E • Existing controls (preventive)

What currently prevents the failure?

Fails if:

Fails if:

Fails if:

“Fails if”: the escalation factor that makes each control fail.

F • Output failure

Start here.
● random • ● systematic

☐

☐

☐

☒

☐

☐

☐

☒

☐

☐

☐

☒

In one group or case?

G • Existing controls (mitigating)

What currently limits the effect?

Fails if:

Fails if:

Fails if:

H • Consequences → objectives

What happens next? To whom?
Timelines • quality • costs • trust

I • What we do not know

What data or evidence is missing for later analysis?

J • Next steps

This session identifies risks. The organisation sets criteria, analyses, evaluates and treats risks through its risk management.

Take to: _____ Date: _____

Templates for these steps: venturalitica.ai/canvas



Worked session

Instructions: on the back

Risk identification session · Assume the system has already failed and ask questions in both directions.

- 1. Fill in the top row: A, B and C.**
Intended use, foreseeable misuse and interested parties.
Each participant represents an interested party.
- 2. Start at the centre: F.**
Write an output failure and mark its type:  random, the baseline error present in any model, or  systematic, an error that follows a pattern.
- 3.  expands to the right, G and H:**
the consequence, the effect and the existing control; record in I what data would show how often it happens. Ask: “Is it concentrated in any group or category?”.
- 4.  expands to the left, D and E:**
the condition or cause and the existing preventive control.
Below each control, write what makes it fail.
- 5. Finish when no failure at the centre has an open branch.**
Then record in I what you do not know and take the canvas to J. Put each completed chain on a record sheet.

Further templates in preparation: criteria, analysis, evaluation and treatment · venturalitica.ai/canvas



The worked session:
venturalitica.ai/canvas/session-organisation
Solution and chain record sheets.

The online payment authentication challenge

Fictional system · Complete both chains.

A · Intended use Scores each online payment and decides whether to exempt it from strong authentication or require it: two of three factors (something you know, have or are). Fraud below thresholds: 0.13 % up to €100; 0.06 % up to €250; 0.01 % up to €500.		B · Foreseeable misuse The threshold is raised for a business target, not measured risk. The score is used to reject payments without allowing authentication, or to block cards.		C · Interested parties Issuers · cardholders · online merchants · the payment processor itself · the supervisor and card schemes.	
D · Causes  start on the right _____ _____	E · Existing controls (preventive) _____ _____ Fails if: _____	F · Output failure Chain 1 ·  random Exempts a fraudulent payment. Concentrated in a group or category? Chain 2 ·  systematic Exempts a run of fraudulent payments split just below the thresholds. What condition causes it?	G · Existing controls (mitigating) _____ _____ Fails if: _____	H · Effect on objectives Which objective is affected? _____ _____	
What if...? _____ _____	_____ _____ Fails if: _____		_____ _____ Fails if: _____	Which objective is affected? _____ _____	
I · What we do not know What data is missing on exempted payments and fraud by band?					