izi Risk

OPERATIONAL-RISK MODEL

From the event register to capital.

How much your organisation can lose in a year from failed processes, people, systems and external events, how likely that is, and which risks drive the loss.



Banks
Basel II/III, event types at all three levels

Companies
Their own categories, no Basel

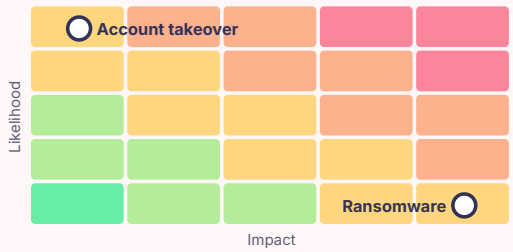
Cyber and IT
Ransomware, data breaches, cloud outages

THE PROBLEM

Loss registers exist. A risk figure, almost never.

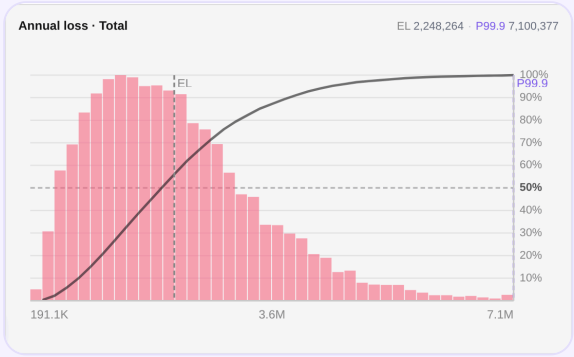
Most organisations record their loss events for the supervisor or for audit, but few turn them into a figure they can defend before a committee.

WHAT A HEAT MAP SHOWS



The frequent-and-cheap and the rare-and-ruinous share boxes of one colour, and nobody knows how much money is at stake.

WHAT THE MODEL SHOWS



The loss of every possible year, in money: the expected one, the 1-in-1,000 year and all in between.

1. **Heat maps**
   They rank by colour, not money.
2. **Historical averages**
   They miss the bad year, the one that puts capital at risk.
3. **Event types in isolation**
   Summing worst cases overstates; ignoring overlap understates.
4. **Registers nobody models**
   What they hold never reaches decisions on capital, insurance or controls.

HOW IT WORKS

The loss distribution approach, in five steps

Reads the register
CSV, Excel, XML or JSON, in five languages. AI sorts out any layout.

Groups
By Basel event type or by your own categories, with breakdowns.

Fits
Frequency and severity per event type, tested against your data.

Simulates
Thousands of years, with the event types correlated.

Measures
Expected loss, VaR at 99.9%, tail and capital by event type.

Bank under Basel II/III
Some 700 events in colones, under Basel event types, with business line, unit, process and product.

Manufacturer
A real-world log with no Basel: plants, several cost columns, insurance and incidents with no loss.

Cyber and IT risk
Security and IT tickets in dollars, under Basel codes. You will see it on the next page.

CYBER AND TECHNOLOGY RISK

Cyber risk is operational risk. And it can be measured in money.

One of the model's three examples: the security and IT tickets of a company that sells online, from 2021 to 2025, with eleven threat categories filed under Basel codes.

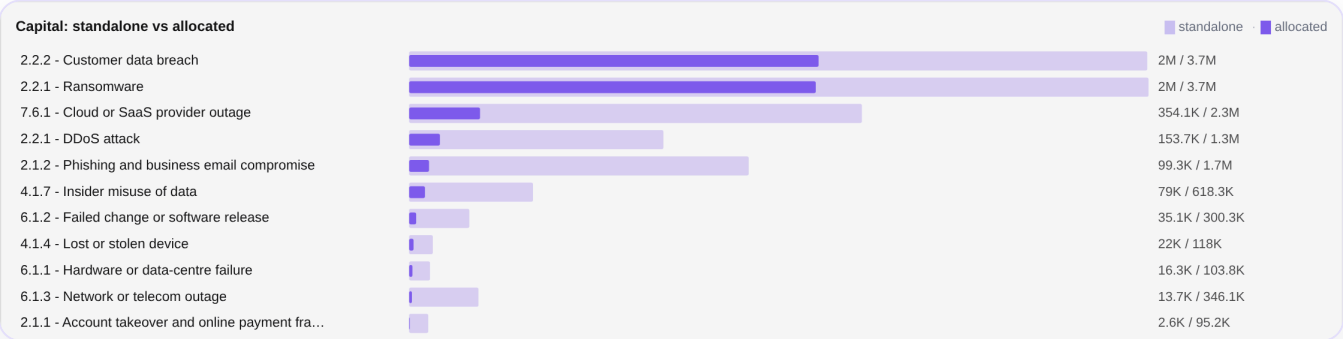
403	US$ 2.2 M	US$ 7.1 M	11
loss events in five years	expected loss per year	VaR at 99.9%: the 1-in-1,000 year	threat categories, each with its own distribution

Risk horizon: the frequent and the ruinous, kept apart



Each bubble is a category: height = events per year, horizontal position = loss per event, area = annual loss at the 80th percentile. Top left, account takeovers; bottom right, ransomware (red) and data breach (yellow).

Where capital concentrates



Light bar: the capital the category would need on its own. Dark bar: its share of total capital. The difference is diversification.

× 7

Six ransomware attacks in five years cost about seven times as much as **nearly two hundred account takeovers**. A heat map would put the account takeovers, for their frequency, in the most visible box.

> 90%

of the capital sits in **three categories**: ransomware, cloud provider outages and customer data breaches. That is where controls, insurance and budget go first.

CAPABILITIES

Every feature answers a committee question

Annual loss distribution
What can we lose in a normal year, and in one in a thousand?

Fit and test
Which distribution describes each event type, and how far to trust it?

Correlation
What happens when the bad years of different risks coincide?

Capital allocation
What consumes capital, and what does diversification return?

Risk horizon
What is frequent and cheap, what rare and ruinous, at any percentile?

Loss horizon
How much can losses add up to over the next few years?

Event register
Register, approval and the supervisor's files in one place.

AI assistance
Imports registers of any layout and explains the results.

5×5 risk matrix
Which cells of the committee's matrix hold the money, and how much?

Risks without history
How to count a risk that has never happened, from expert estimates?

Mitigation
Is each control worth its cost, and how much loss does it avoid?

AI reports
Technical, executive, matrix and mitigation, as PDF or PowerPoint.

What a risk manager gets

- **A defensible capital figure**, read from thousands of years simulated on your own data.
- **Clear priorities:** event types ranked by the capital they consume.
- **A basis for insurance:** the loss at different percentiles guides deductibles and limits.
- **Transparency:** each parameter can be reviewed and changed; the result traces to its events.
- **Committee-ready material:** charts and four AI reports, as PDF or editable PowerPoint, in five languages.

How it fits into existing work

- **Excel:** exports to an iziRisk Quantum workbook (.xlsm) that runs the same simulation.
- **In the browser:** the event file never leaves it; the AI sees only the headers, a summary and the first rows.
- **Register and supervisor:** the Event register tab runs the approval workflow and builds the files.
- **Training and expert support:** courses and a panel of practitioners who answer directly.

Next step: a pilot on your data

We load your organisation's real event register, map it to the event types you choose and return the expected loss, operational VaR, capital by event type and the risks that drive it. Your team sees the method applied to data it already knows.

Fernando J. Hernández
Consulting and Training Manager
IZIRISK, INC
fhernandez@izirisk.com
+506 7253 9597 · phone and WhatsApp

iziriskhub.com