KAIA-OR · USE-CASE BRIEF

Financial services

Events grouped across sources and matched to your sites, software and suppliers, with corroboration you can brief on, delivered into your own tools.

DOCUMENT ID	UCB-16-FINANCIAL-SERVICES
VERSION	1.0
DATE	3 November 2026
AUDIENCE	Security, resilience and operational-risk teams at financial institutions

At a glance

Who it is for	Security, resilience and operational-risk teams responsible for branches, offices and operations sites, the software their institution depends on, and the suppliers behind it.
Outcome	Physical, cyber and supply-chain events that touch your institution in one shared picture, each with its corroboration status and why it matched, and in your own tools through the API.
Package	KAIA-OR Enterprise

The challenge

Financial institutions often follow physical, cyber and supplier risk in separate teams and separate tools. Reports of the same event arrive through different channels, at different times and with different levels of certainty. Before anyone acts or briefs leadership, someone has to work out whether a report is corroborated, which sites, systems or suppliers it touches, and what it means for the institution.

At the same time, staff are targeted with invoice fraud and executive impersonation: messages that ask to change where a supplier's money is sent, or that claim to come from a senior colleague.

> In a 2026 survey of risk experts, cyber incidents were the top global risk for the fifth year in a row, at 42% of responses; business interruption ranked third, and natural catastrophes fifth, at 21%.[1]

© Kaia Technologies, Inc.

What changes with KAIA-OR

Physical, cyber and supply chain in one picture

Hazards, incidents and disruptions on your branches, offices and operations sites; major breaches and newly exploited vulnerabilities that touch the software you use; and the suppliers exposed to them, in one shared picture.

Corroboration you can brief leadership on

Reports of the same event from different sources are grouped together. Each event carries its severity, confidence, source and corroboration status, and unconfirmed reports are labelled. Hey KAIA answers are checked against the evidence before anyone sees them, and model output never grants authority.

Evidence in your own tools

Send events into your own tools through the API and webhooks, so your security, resilience and operational-risk teams work from the same evidence in the systems they already use.

A second look before anyone pays

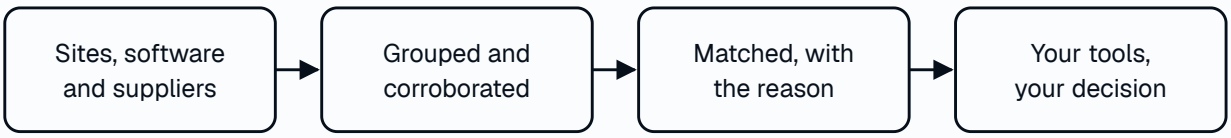
Staff can paste a request to change where money is sent, or a message that appears to come from an executive, to see the warning signs KAIA-OR recognizes. Links stay unopened. You see what looks wrong, when the check can't tell, and a suggested next step, such as confirming through a channel you already trust.

What you see

Item	What it shows
An event on a site	Category, severity, place, time window, confidence, source and corroboration status, and the reason it matched.
A cyber event	A major breach or a newly exploited vulnerability, and the software you use that it touches.
A supplier exposure	The supplier, the event it is exposed to, and why it matched.
An event in your own tools	The same event and its evidence, delivered through the API and webhooks.

© Kaia Technologies, Inc.

How it works



One picture of physical, cyber and supply-chain events, delivered where your teams already work.

1. The resilience team adds branches, offices and operations sites, the software the institution uses and its key suppliers.
2. When official and authoritative sources publish a hazard, an incident, a disruption or a cyber event, KAIA-OR groups reports of the same event and shows how well independent sources corroborate it.
3. When the event touches one of your sites, a piece of software you use or a supplier, it appears in the shared picture with the reason it matched.
4. The event reaches your own tools through the API and webhooks, where your teams handle it under your own procedures.
5. When a member of staff receives a request to change where a supplier’s money is sent, they paste it in and see the warning signs and a suggested next step before anyone pays.

© Kaia Technologies, Inc.

Privacy and control

- The organization sees its sites, software and suppliers, not its people's whereabouts.
- Roles manage membership, not people. Membership never grants access to another member's messages, devices, location or saved places. These boundaries are enforced at the application layer.
- Messages and links that staff check stay on their own device. KAIA-OR checks only what they choose to paste.
- Nothing goes to cloud AI unless each person agrees first, and only that person can give that consent.
- Single-use invitations, each bound to the invited person's account, and dated access reviews keep access accountable.

Honest boundaries

- KAIA-OR does not screen transactions or detect fraud inside payment systems.
- It offers no market or investment views.
- It does not make regulatory determinations. Your institution's obligations remain its own.
- Message and link checks show warning signs, not verdicts, and KAIA-OR is not antivirus.
- Coverage depends on what official and authoritative sources publish. Reports that cannot be corroborated are labelled as unconfirmed.

Editions and related use cases

Financial services is part of KAIA-OR Enterprise. The shared picture is used by the people responsible for your sites, software and suppliers, and each member keeps their own KAIA-OR. KAIA-OR runs on iOS, iPadOS, macOS, Android phones, Android TV, Windows and the web, in English, French (Canada), Turkish and Hebrew. One account works on every platform, with the same features and the same privacy rules.

Related use cases

- Supply chain
- Digital risk and cyber threat intelligence
- Scam and phishing checks

© Kaia Technologies, Inc.

Request early access

> Membership is by invitation. Request early access on the KAIA-OR website and choose Enterprise. Enterprise and government teams can also choose Contact us on the KAIA-OR website.

Sources

1. Allianz Commercial, Allianz Risk Barometer 2026, January 2026. Market context only.

© Kaia Technologies, Inc.

UCB-16-FINANCIAL-SERVICES · Version 1.0 · 3 November 2026

Capability availability depends on the edition and deployment. Capabilities are described as the committed KAIA-OR product scope.