

INSIDER RISK MANAGEMENT PROGRAM

Five services

The services through which an insider risk management program is designed, built, run, and assessed.

A program is built in an order of dependencies, and the order holds wherever the work begins: no measure collects data before the mandate and its lawful basis are in place, no alert reaches an analyst before the procedure that receives it exists, and operation runs on what the other services have set. The services overlap in time: a later one starts its design while an earlier one is still being agreed, and reaches production only once the earlier one has passed its gate. Where a program already runs, the assessment comes first, and the roadmap closes the earliest gap in that order before any other; where the program is being built, the assessment measures it once it runs. Each service ends with documents the organization owns and applies without the engagement.

SERVICE	WHAT IT ESTABLISHES	DELIVERABLES
Program design	The mandate, the lawful scope, and the decision and escalation matrix under which the program runs.	Program charter; Scope statement; Capability model and roadmap; Decision and escalation matrix; RACI, service levels and runbooks
Detection engineering	Detection, prevention, enrichment, triage, and containment, built on the organization's own risks and tools.	Insider risk map; Use case catalogue; Use case implementation; Policy architecture; Tuning record
Investigation and response	A procedure from alert to case closure that is effective, preserves evidence, and is fair to the person.	Triage and enrichment standard; Investigation plan and playbooks; Evidence and chain of custody standard; Interview protocol; Reporting obligations map and consequence framework
Operations and enablement	A function sized, sustained, and trained to run the program on its own.	Operating capacity and cadence; Case records; Analyst training and case simulations; Operational handover
Program assessment	How the program performs against the full set of measures and its own scenarios, whether its controls operate as intended, and what to close next.	Coverage analysis; Control effectiveness testing; Effectiveness indicators; Program review and prioritized roadmap

SERVICE 1 OF 5

Program design

Which mandate, governance, and operating model the program runs under; what it may lawfully observe and mitigate in each jurisdiction, on which populations and on what basis; and who decides, who is consulted, and who is informed at each step, from the activation of a policy to the consequence for a person.

RATIONALE

Programs are often started from the platform: policies run before the mandate is written and the lawful basis is assessed, and no one owns the decisions an incident requires. On the first serious case, material collected without a documented basis may be inadmissible, and the incident waits while the functions dispute who decides. The service sets the mandate, the lawful scope, and the allocation of decisions and escalation before activation, or rebuilds them around a program already in operation.

SCOPE

Mandate; scope and lawful basis; safeguards; decisions and escalation; operating model; capabilities and roadmap; legal entities.

DELIVERABLES

Program charter; scope statement; capability model and roadmap; decision and escalation matrix; RACI, service levels and runbooks.

DECISIONS THAT REMAIN WITH THE ORGANIZATION

Mandate; ownership of the program; lawful basis; agreements; allocation of decisions; residual risk; sources of context.

OUTCOME

The organization holds a charter agreed by the functions it binds and published in its internal regulations; a scope that states, for each jurisdiction, what is observed and mitigated, and on what basis; the notices and agreements that make it lawful; an owner and a threshold for every decision the program produces; and procedures its teams apply without the engagement.

SERVICE 2 OF 5

Detection engineering

What the program is able to detect; which preventive and response controls are in place; and how the tools are configured to detect, enrich, triage, contain, and respond to anomalies and emerging threats.

RATIONALE

Insider risk engines are often enabled with vendor policies and default thresholds: analysts spend their time on volume, and the scenarios that matter remain uncovered. The service designs and configures the whole chain, from the signal to the response, on the organization's own risks and on the tools it already owns.

SCOPE

Risk map; use cases; use case implementation; detection architecture; prevention; enrichment and triage; containment and response; tuning; coverage gaps.

DELIVERABLES

Insider risk map; use case catalogue; use case implementation; policy architecture; tuning record.

DECISIONS THAT REMAIN WITH THE ORGANIZATION

Risk map; lawful scope; enforcement; residual risk; platform changes; device and browser policies.

OUTCOME

The organization holds a map of its insider risks, a catalogue of use cases and their implementation; detection, prevention, enrichment, triage, and containment configured as one chain on its own platform, at thresholds set on its own data; a record of every change and its effect; and a register of what the tools cannot observe.

SERVICE 3 OF 5

Investigation and response

Triage outcomes and escalation criteria; the acquisition of context and the confirmation, containment, assessment, and escalation of an incident; the collection and preservation of evidence; and the obligations and consequences an event triggers, for whom, and by when.

RATIONALE

An insider alert is ambiguous by nature: the same action can be lawful or unlawful depending on context that no log contains, and a decision taken on logs alone can be reversed by the first contextual fact. The service builds an investigative process that is effective, preserves evidence through a chain of custody, is fair to the person, and holds before workers' representatives, a court, or a supervisory authority.

SCOPE

Triage; context and confirmation; interviews; containment and assessment; escalation and coordination; evidence; obligations and consequence; reporting.

DELIVERABLES

Triage and enrichment standard; investigation plan and playbooks; evidence and chain of custody standard; interview protocol; reporting obligations map and consequence framework.

DECISIONS THAT REMAIN WITH THE ORGANIZATION

Ownership of the procedure; limits of investigation; interview of the employee concerned; live response on an active user; senior analysts; notification of a personal data breach; measures concerning the person; referral of possible criminal conduct; acceptance of complex events.

OUTCOME

The organization holds triage outcomes and escalation criteria applied to every alert; playbooks per scenario; containment with authorized, reversible measures; evidence kept to the standard of the proceedings it may reach; an interview protocol and interviewers trained in it; and a map of what it owes, to whom, and by when, from the moment it knows.

SERVICE 4 OF 5

Operations and enablement

How the function is staffed and sustained: its capacity over the day, the month, and the year; its protection from fatigue and turnover; its operating cadence; its case records; the tuning of detection in operation; and the on-the-job training of the team that takes it over.

RATIONALE

Programs are often configured by people who do not run them and staffed on budget without a measure of volume, and insider work produces fatigue and turnover. The service sizes and sustains the function, runs it alongside the team while the team forms, and hands it over when the team runs it alone.

SCOPE

Capacity; sustainability; cadence; case records; tuning in operation; on-the-job training and handover; awareness.

DELIVERABLES

Operating capacity and cadence; case records; analyst training and case simulations; operational handover.

DECISIONS THAT REMAIN WITH THE ORGANIZATION

Staffing, recruitment, and shifts; retention of case records; acknowledgment of the handover.

OUTCOME

The organization holds a function sized on its volume and covered over time, with protections against fatigue and turnover; a stated cadence; case records that withstand audit; a tuning record that explains every rule; analysts trained on the job and tested on insider cases; and every part of the program owned by name.

SERVICE 5 OF 5

Program assessment

What the existing program covers, read against the full set of measures an insider risk management program is built from and against the organization's scenarios; whether its controls operate as intended, with evidence of it; how the program performs, and which metrics and dashboards govern it; and which gaps to close, in which order.

RATIONALE

Programs are often measured by the policies enabled and the alerts handled, while the coverage of the scenarios that matter goes unmeasured and controls are assumed to work because they are configured. The service reads the program against the full set of measures and the organization's scenarios, tests its controls, evaluates its performance, and sets the order in which its gaps close.

SCOPE

Coverage; scenarios; effectiveness; case handling; performance; roadmap.

DELIVERABLES

Coverage analysis; control effectiveness testing; effectiveness indicators; program review and prioritized roadmap.

DECISIONS THAT REMAIN WITH THE ORGANIZATION

Commission and scope of the assessment; confirmation of the facts; metrics and roadmap; risk acceptance and resources.

OUTCOME

The organization holds an evidenced account of what its program covers and of the scenarios it leaves exposed; the results of tests on its controls; the indicators by which its effectiveness is measured and reported, with the dashboards that carry them; and a roadmap that closes its gaps in order.