



Run AI on the data you can't send to AI

Governed AI agents for banks, credit unions and payment firms



Your examiner will ask how your AI agents are governed

Banks aren't missing an agent framework. They're missing the evidence.

AI agents are a model class your model risk process has no shape for. They:

- Act rather than score
- Are non-deterministic
- Call external model providers
- Change when a vendor ships a new version



Option A: don't deploy

Fall behind while vendors and peers ship agents into your workflows anyway.



Option B: deploy outside MRM

Agents run uninventoried and unvalidated, and the gap surfaces at the next exam.



Neody: deploy inside MRM

Every agent chartered, inventoried, monitored, with evidence for each autonomy decision.



Your risk, audit and control teams are already asking

Eleven asks from eight lines of business reduce to three jobs:



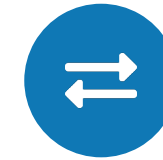
Check it

Review against policy and criteria, QC before sign-off, find gaps, trace each finding to its evidence



Write it

Workpapers, lead sheets, referral narratives and summaries in your approved format



Match it

Combine documents, records and extracts, reconcile them and report the mismatches

And two conditions, from everyone



A human signs. AI prepares; people keep ratings, approvals and sign-off.



It saves reading time. Less repetitive reading, comparing and drafting.



Neody runs your agents, governs them and proves it



Run

Execute any agent on regulated data: PII, cardholder data, MNPI, PHI, including inside PDFs, Word files and email.

COO • CISO • business owner



Govern

Each agent earns autonomy on measured evidence, across every risk domain you already run, and steps back automatically when quality drifts.

CRO • MRM • TPRM • CCO



Prove

One record of what ran, on which data, under whose authority, with what result. Produced as agents run, not assembled before an exam.

Internal audit • examiners



The unit is a business process, not an agent

An Agency owns one capability, with a named human owner

TPRM due-diligence review

KYC Refresh

Disputes

Wire Review

Loan exception handling

First packages in teal



Agents and roles

Human and agent roles in one model, so work shifts over time without redesign



Human checkpoints

Approve, exception, escalate, review: each a named role with an SLA



System connections

Into the core, card, case, GRC and document systems the process touches



Mandate

Its authority, with limits on data classes, spend, purpose and jurisdiction



KPIs and risk tier

Measured ROI, mapped to your internal model risk rating

Autonomy is earned on evidence, and lost automatically

Where most teams start



Promotion gates: decision volume, agreement rate over threshold, no open incidents, independent approver



Automatic demotion: quality drift, an incident, connector errors, anomalous spend, or a model version change



The ladder is your model risk control, built in

SR 11-7 / OCC 2011-12 asks for	What Neody provides
Model inventory	The Agency portfolio: owner, purpose, risk tier and current autonomy level
Documented validation	L1 Shadow: measured agreement with human decisions on live traffic, before anything is applied
Ongoing monitoring	Continuous KPI and drift measurement, with thresholds that fire automatically
Effective challenge	Promotion requires an approver independent of the builder, enforced by policy
Change management	A model version change triggers demotion; an upgrade can't inherit prior authority
Documented limitations	Mandate limits stated in the charter and enforced at runtime



Evidence is produced while agents run, not assembled before the exam.



Your regulated data stays under your control



PII



Cardholder
data



MNPI



PHI



Trade
secrets

Field-level protection

Sensitive values are protected before any model sees them, including inside PDFs, Word files and email.

You approve destinations

A protected value is released only to a destination a named person at your institution approved.

On-premises option

Run the protection service inside your walls for any data class you won't let leave.

Minimum necessary

Each Agency's mandate states which data classes it may touch, for what purpose, and where.



Your vendors' agents are third-party risk

Neody governs any agent: ours, your vendors' or your own

Your core, CRM, HR and ITSM vendors are switching on agents inside your institution. Each one is a model to inventory and a third party acting on your behalf.

“Your control tower knows which agents you have. Neody knows which ones you can trust with what, and proves it.”



At onboarding

TPRM Review Agency checks the vendor's documents against your standards



In production

Govern mode monitors the vendor's agent, with demotion and a kill switch

One TPRM record per vendor



One evidence record answers every risk owner



Model risk

Head of MRM



Third-party risk

Head of TPRM



Operational risk

CRO



Compliance

CCO



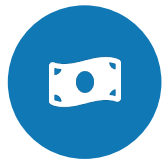
Data and privacy

CDO · CPO



Information security

CISO



Financial governance

CFO



Legal and records

General Counsel



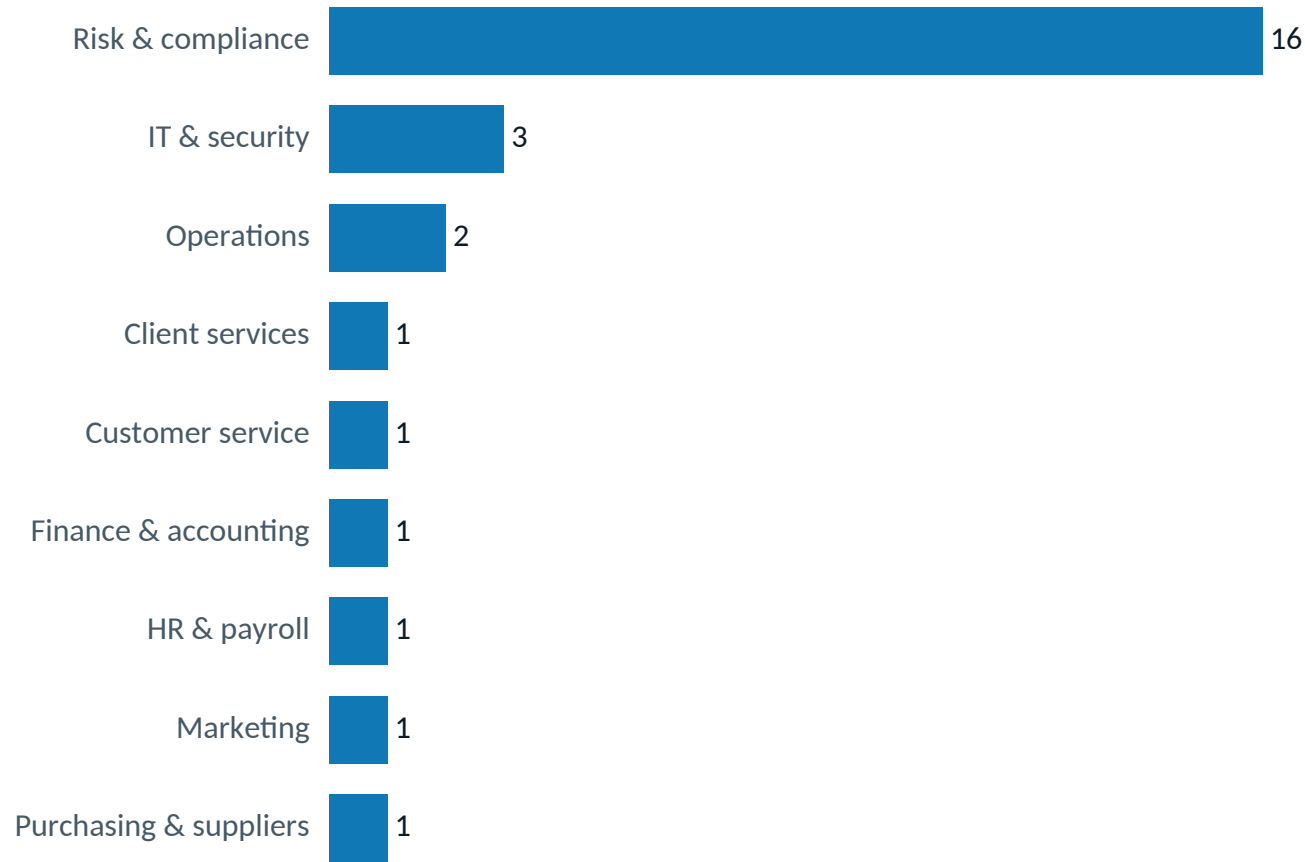
Internal audit

Chief Audit Executive



27 use cases ready for banks and credit unions

Core use cases by department



27

core use cases for this industry

15

high value at low or medium effort

4

more from other industries that also apply

Suggested first: Third-party due-diligence review or KYC document review



We take you from “the board is asking” to production

1

How to use AI

Process discovery,
governance posture
assessment, use-case
catalog, free workflows

2

Your first use case

A chartered, gated Agency
on one process, from guide
to implementation

3

Chat with data and documents

People and agents working
over confidential data, with
protected execution

4

Many agents

Yours, your vendors' and
partners', all governed on
one record

Governance starts at Level 2: your first agent is chartered and gated from day one.



Start with one use case, accepted on your CRO's number



TPRM due-diligence review

Vendor documents against your standards. No cardholder data, no core connection needed. Your CRO owns it.



KYC Refresh

Regulator-driven, high-volume and measurable. PII only.

Second use case costs materially less: the connections, charter templates and approvals already exist.

How acceptance works

1

Before signing, you and your CRO set the agreement threshold and decision volume

2

We build on your systems: L0 Chartered, then L1 Shadow beside your team

3

At L2, an independent validator confirms the threshold was met

4

You keep the evidence pack: inventory entry, validation, monitoring, approvals



Four ways in, priced to how far you go



AI Journey

Per user

Discovery, posture assessment, catalog, and an allowance of governed use cases



Free workflows

Free, with usage credit

Try it on a sample process, including one on protected sample data



Business use cases

Fixed per use case

A how-to guide, then implementation; the guide fee is credited against the build



Hosting

Usage-based, published rates

Run ours, your vendors' or your own agents, with spend caps per Agency



Proposed next steps



01

Posture assessment

Including the model-inventory check: which AI is already running that MRM hasn't inventoried



02

Pick the first use case

TPRM review or KYC Refresh, ranked by value, effort and risk on your processes



03

Agree the acceptance bar

Agreement threshold and decision volume, set with your CRO before anything is signed



04

Start in Shadow

The Agency runs beside your team; nothing is applied until the evidence says so

The governed execution platform for AI agents on regulated data

Bank use-case catalog (1 of 5)

RISK & COMPLIANCE

High risk

ACH originator agreement review

Each business customer's ACH origination agreement, exposure limit and SEC codes checked against the bank's policy; missing or expired agreements chased.

[Intake & extract](#) → [Validate](#) → [Follow up](#)

Value high · effort medium · NACHA Operating Rules

RISK & COMPLIANCE

Medium risk

ACH risk assessment

Volumes, return rates, originator mix and third-party senders pulled together and the annual ACH risk assessment drafted for the board, with the risks ranked.

[Consolidate](#) → [Analyse history](#) → [Draft](#)

Value high · effort medium · NACHA Operating Rules

RISK & COMPLIANCE

High risk

Alert & case triage

Monitoring alerts enriched and prioritised; obvious false positives closed with a reason for review.

[Analyse history](#) → [Route](#)

Value high · effort medium · BSA / AML · SR 11-7

RISK & COMPLIANCE

High risk

Annual ACH audit

The bank's ACH evidence (policies, agreements, return rates, exposure limits, records) gathered and checked against the NACHA rules; gaps chased; the audit report drafted with each finding cited.

[Intake & extract](#) → [Validate](#) → [Follow up](#) → [Draft](#)

Value high · effort medium · NACHA Operating Rules · OFAC sanctions

RISK & COMPLIANCE

Medium risk

Card fraud & velocity monitoring

Card activity watched for velocity, geography and merchant patterns; likely fraud routed to an analyst with the evidence, the rest released.

[Monitor & alert](#) → [Analyse history](#) → [Route](#)

Value high · effort medium · PCI DSS · BSA / AML

RISK & COMPLIANCE

High risk

KYC document review

Customer identity and business documents checked against the KYC standard; gaps chased.

[Intake & extract](#) → [Validate](#) → [Follow up](#)

Value high · effort medium · BSA / AML · GLBA



Bank use-case catalog (2 of 5)

RISK & COMPLIANCE

High risk

Regulatory exam preparation

The examiners' request list answered: documents found and checked, owners chased, open findings tracked to closure before the exam starts.

[Intake & extract](#) → [Validate](#) → [Follow up](#)

Value high · effort medium · GLBA · BSA / AML · NACHA Operating Rules

RISK & COMPLIANCE

Medium risk

Sanctions screening review

ACH, wire and customer screening tested: lists current, matches handled, alerts cleared with a reason; findings drafted.

[Consolidate](#) → [Validate](#) → [Draft](#)

Value high · effort medium · OFAC sanctions · BSA / AML

RISK & COMPLIANCE

Medium risk

Sponsor-bank & program reporting

Program volumes, balances, complaints, disputes and compliance metrics rolled into the sponsor bank's monthly and quarterly reports, checked before they are sent.

[Consolidate](#) → [Validate](#) → [Draft](#)

Value high · effort medium · BSA / AML · Reg E · GLBA

RISK & COMPLIANCE

Medium risk

Third-party due-diligence review

Vendor questionnaires and evidence reviewed against the bank's standard; gaps chased with the vendor.

[Intake & extract](#) → [Validate](#) → [Follow up](#)

Value high · effort high · Third-party risk guidance · SR 11-7

RISK & COMPLIANCE

High risk

Dispute routing

Card and transfer disputes classified, routed and tracked against Reg E deadlines.

[Intake & extract](#) → [Route](#) → [Follow up](#)

Value medium · effort medium · Reg E

RISK & COMPLIANCE

Low risk

Issue closure validation

Evidence that an audit or exam issue is fixed checked before the issue is closed.

[Validate](#)

Value medium · effort medium



Bank use-case catalog (3 of 5)

RISK & COMPLIANCE

Medium risk

Policy Q&A with citations

Staff questions answered from internal policy and procedure, with the section cited.

[Answer](#)

Value medium · effort low

RISK & COMPLIANCE

Low risk

Regulatory change monitoring

New rules and guidance watched; what changes for you summarised with the affected policies.

[Monitor & alert → Research](#)

Value medium · effort medium

RISK & COMPLIANCE

Medium risk

Regulatory report reconciliation

Regulatory reports reconciled to the ledger and source systems before filing.

[Consolidate → Validate](#)

Value medium · effort high · GLBA

RISK & COMPLIANCE

High risk

SAR narrative drafting

Suspicious-activity narratives drafted from the case file for the investigator to edit and sign.

[Consolidate → Draft](#)

Value medium · effort medium · BSA / AML

IT & SECURITY

Medium risk

Access review certification

Who has access to what, compared with their role; managers asked to confirm or remove.

[Consolidate → Validate → Follow up](#)

Value high · effort medium · SOX · GLBA

IT & SECURITY

Medium risk

Internet & electronic banking review

Online and mobile banking reviewed against policy: security, authentication, vendor support and consumer compliance, written up as findings with recommendations.

[Intake & extract → Validate → Draft](#)

Value high · effort medium · GLBA · Reg E



Bank use-case catalog (4 of 5)

IT & SECURITY

Medium risk

Change-record reconciliation

Production changes reconciled with approved change records; unapproved changes listed.

[Consolidate](#)

Value medium · effort medium · SOX

OPERATIONS

Medium risk

Benefits disbursement checks

Each federal or state benefits disbursement file checked against eligibility and the prior cycle before cards are loaded; duplicates and outliers held for a person.

[Validate](#) → [Monitor & alert](#)

Value high · effort medium · BSA / AML · Reg E

OPERATIONS

Medium risk

Technology & operations review

Back office, imaging, process flow, vendor contracts and disaster recovery reviewed; bottlenecks and risks found and the report drafted.

[Intake & extract](#) → [Consolidate](#) → [Analyse history](#) → [Draft](#)

Value high · effort high · Third-party risk guidance

CLIENT SERVICES

High risk

Card program onboarding

A new business, government or fintech card program set up: agreements, program details, KYB documents and sponsor-bank approvals collected, checked and chased until launch.

[Intake & extract](#) → [Validate](#) → [Follow up](#)

Value high · effort medium · BSA / AML · GLBA

CUSTOMER SERVICE

High risk

Cardholder support (balance, card status, lost card)

Cardholders' questions answered from the system of record (balance, transactions, card status); lost or stolen cards locked on request, with anything unusual handed to a person.

[Answer](#) → [Converse](#) → [Execute](#)

Value high · effort medium · Reg E · PCI DSS

FINANCE & ACCOUNTING

High risk

Payroll & benefits card funding reconciliation

Each funding file from an employer or agency matched to the money received and the card loads; short, late or duplicate funding chased before cardholders are affected.

[Consolidate](#) → [Validate](#) → [Follow up](#)

Value high · effort medium · NACHA Operating Rules · Reg E



Bank use-case catalog (5 of 5)

HR & PAYROLL

Medium risk

Training & certification tracking

Required training and licences tracked per person; reminders before they lapse.

[Monitor & alert](#) → [Follow up](#)

Value medium · effort medium

MARKETING

Medium risk

Cash-back rewards offers & settlement

Which offers drive card use, by program and merchant; rewards calculated, settled with merchants and reconciled to what cardholders received.

[Analyse history](#) → [Recommend & optimise](#) → [Consolidate](#)

Value medium · effort medium

PURCHASING & SUPPLIERS

Medium risk

Supplier risk monitoring

Critical suppliers watched continuously for financial, cyber and news risk; alerts with evidence.

[Monitor & alert](#) → [Research](#)

Value medium · effort medium · Third-party risk guidance



Also applies, from other industries

RISK & COMPLIANCE

Medium risk

Security certification evidence (ISO 27001, PCI DSS)

Evidence for each control gathered from systems and owners, checked against the standard, and gaps chased before the auditor arrives.

[Consolidate](#) → [Validate](#) → [Follow up](#)

Value high · effort medium · ISO 27001 / SOC 2 · PCI DSS

IT & SECURITY

Medium risk

Security alert triage

Alerts from monitoring tools enriched, de-duplicated and ranked; the likely-real ones escalated with the evidence, the noise closed with a reason.

[Intake & extract](#) → [Analyse history](#) → [Route](#)

Value high · effort medium · ISO 27001 / SOC 2 · PCI DSS

OPERATIONS

Medium risk

Payment transaction monitoring

Transaction flows on the payment platforms watched for failures, latency and unusual patterns; clients and on-call engineers alerted.

[Monitor & alert](#) → [Analyse history](#)

Value high · effort medium · PCI DSS

QUALITY

Medium risk

Audit-readiness evidence

Evidence for ISO or customer audits gathered and checked against the standard; gaps chased.

[Consolidate](#) → [Validate](#) → [Follow up](#)

Value medium · effort medium · ISO 9001 / IATF 16949

