CrystalSoft worked example

Bounding Agency: Identity, Authority, and Trust in the Age of AI Agents

The AI-IAM Practitioner Series · Book 1 · Rahul Bhardwaj · Arvik Press

This workbook shows every tool as the book fills it in for CrystalSoft Energy's Billing Resolution Agent and Payments Agent. Each sh
reproduces the book's own entries; where the book does not record a value, the cell is left out rather than invented.

*CrystalSoft Energy and its people, agents and systems are fictional, created to illustrate the book. Values marked with an asterisk (*)
illustrative.*

A working diagnostic. Not a certification, audit opinion or compliance attestation.

© 2026 Rahul Bhardwaj. Published by Arvik Press. You may copy and adapt the tools for use within your own organization. They may not be resol
republished.

Table 17.5 — The CrystalSoft Tool Chain

Tool	What it produced for the Billing Resolution Agent	Feeds
AI Agent Inventory	Sponsor, write capability, reversibility, approval mode, authority mode (both), degree of agency (high), delegation capability (Payments Agent only), lifecycle state	All other tools
Identity Readiness Checklist	Sponsor succession missing after the role change	Governance Checklist; 90-Day Plan
Authority & Delegation Assessment	Priya → Billing Resolution Agent → Payments Agent → billing platform; revocation does not cascade across the platform	KAB Worksheet (BUILD)
360° Assessment, KAB Worksheet, Maturity	Mostly ADAPT; two critical gaps; cascade revocation as BUILD	Roadmap
Governance Checklist and Responsibility Matrix	Sponsor-succession and cross-team delegation decision rights	Roadmap; 90-Day Plan
90-Day Action Plan	Week-one escalations; credential work with the vendor	Roadmap
12–24 Month Roadmap	NOW, NEXT and THEN initiatives with gates	Revalidation cycle

Table 4.2 — AI Agent Inventory: Initial Records

Field	Billing Resolution Agent	Payments Agent
Principal / identity type	Workload identity on CrystalSoft's cloud agent platform	Its own workload identity (separate principal)
Name / purpose	Resolve customer billing complaints	Post approved credits and refunds
Sponsor / operator	Head of Customer Operations / platform engineering	Finance* / Finance platform team
Environment / status	Production / active	Production / active
Degree of agency	High: interprets the goal and selects steps	Lower: executes credit requests within policy*
Authority mode	Both: own identity for platform operations; on Priya's behalf for customer-specific actions	Own authority, acting on requests from approved agents*
Delegation capability	Can request credits from the Payments Agent only	None*
Tools / data	CRM (customer PII), third-party billing platform, ticketing, knowledge base, email drafting	Billing platform payment functions*
Read / write	Reads billing history; writes CRM records and tickets; requests credits	Posts credits and refunds
Reversibility	Credits reversible with effort; sent emails are not	Credits reversible with effort
Human approval	Priya approves customer emails; credits above $500 need human approval	Credits above $500 need human approval
Credential pattern	Short-lived, task-scoped*	Short-lived*
Provenance / version	Version and deployment record kept*; model lineage not tracked	Version record kept*
Risk / review	High (customer data, financial action) / quarterly*	High (financial action) / quarterly*
Evidence / confidence	Platform registry + sponsor attestation / high	Finance platform registry / medium*

Values marked with an asterisk are illustrative; the rest come from the scenario as established by Chapter 4.

Table 7.1 — Assessment Example: Billing Resolution Agent → Payments Agent

Field	Value
Delegator → delegate	Billing Resolution Agent → Payments Agent
Purpose / task	Correct this customer's $184.20 duplicate charge
Actor / subject	Payments Agent / Priya, with the Billing Resolution Agent as prior actor
Initial authority	Standing permission to request credits up to $500
Delegated scope	Post one credit, this customer, up to $184.20, this task
Attenuation	Amount, customer, count and time narrowed from the standing permission
Redelegation	Not allowed beyond the billing platform call*
Credential / expiry	Exchanged task token; ten minutes*
Revocation path	Payments Agent introspects each request; the platform token is revoked separately*
Provenance retained	Subject, actors, task ID, amount, decision, timestamps
Cross-domain boundary	Yes, at the billing platform API
Approval	None at $184.20; a human approver above $500
Outcome	Credit posted; recorded against the task

Values marked with an asterisk are illustrative.

Table 14.1 — IAM 360° Readiness Assessment: Row Fields and a Worked Row

Field	What to record	CrystalSoft example
Capability or control	What is being assessed	Finance approval of credits above $500
Spoke / capability	IAM 360° spoke and Chapter 13 capability	Governance & Reporting / Governance & Accountability
Current state	What exists today, in observable terms	Policy exists; approvals happen by email
Evidence source and date	The artifact behind the rating	Policy document (2025); sample of email approvals (Sept 2026)
Confidence / coverage	Evidence strength; share of scope covered	Low; approvals not captured in the workflow
N/A or Unknown	Either, with a reason	—
Stage	Descriptive stage (Section 14.5)	Defined
Target and context	Required stage for this scope, and why	Integrated: financial action, external platform
KEEP / ADAPT / BUILD	Response classification (Section 14.6)	ADAPT: capture approvals in the workflow
Dependency	What this depends on or blocks	Payments Agent workflow change (Finance)
Note	Anything the next reader needs	No above-threshold credit has yet been tested end to end

Figure 14.1 — IAM 360° Assessment Heatmap: CrystalSoft (Illustrative)

IAM 360° spoke	Current	Target (this scope)	Evidence	KEEP / ADAPT / BUILD	Critical gap?
IAM Core Processes	**Integrated**	**Adaptive**	Tested control or log	KEEP · ADAPT · BUILD	Yes
IAM Drivers & Mandates	**Defined**	**Defined**	Configuration	KEEP	No
IAM Enablers & Influencers	**Defined**	**Integrated**	Configuration	ADAPT	No
Future-Ready IAM Trends†	**Initial**	**Defined**	Documented policy or interview	ADAPT (watch)	No
Compliance & Regulatory Alignment	Unknown	**Defined**	None	Unknown: finding	No
IAM Governance & Reporting	**Defined**	**Integrated**	Documented policy or interview	ADAPT	No
Cross-Functional Integration	**Defined**	**Integrated**	Configuration	ADAPT	No
IAM Risk & Threat Management	**Defined**	**Integrated**	Configuration	ADAPT	Yes
Visibility & Analytics (cross-cut)	**Defined**	**Integrated**	Documented policy or interview	ADAPT	No

†Future-Ready IAM Trends assessed for the IAM-for-agents half only. No cell is averaged; critical gaps are outlined. Illustrative results for the CrystalSoft scope.

Table 14.4 — Consolidated KEEP → ADAPT → BUILD Map: CrystalSoft

Spoke	KEEP	ADAPT	BUILD / OPEN / UNKNOWN
IAM Core Processes	Workload identity per agent; task-scoped grants; introspection	CRM write scope; sponsor-change trigger; assistant inventory	Cascade revocation across the billing platform (BUILD)
IAM Drivers & Mandates	Approved use case and purpose	—	—
IAM Enablers & Influencers	Gateway for the ticketing system	Preserve actor and subject beyond the ticketing gateway	End-to-end provenance across the platform boundary (BUILD)
Future-Ready IAM Trends	—	Standards watch list (transaction tokens, agent identity drafts)	—
Compliance & Regulatory Alignment	—	—	Jurisdiction and applicability (UNKNOWN; for the legal department)
IAM Governance & Reporting	Named sponsor; auditor evidence chain	Capture approvals in the workflow; book metrics	—
Cross-Functional Integration	Cross-team delegation rule	Matrix pilot; retirement handoff to Finance	—
IAM Risk & Threat Management	Task grant as injection control	Detection context; privileged third-party credential controls	Detection efficacy (OPEN); SoD between agents (OPEN)
Visibility & Analytics (cross-cut)	—	Reconciliation and coverage reporting	Embedded ticketing agent (UNKNOWN)

Readiness and Governance Checklists — rows the book discusses

Checklist	Domain	Response	What the book records
Identity Readiness (Ch8)	Sponsor	No*	Sponsor succession missing after the role change; the sponsor field went stale while the agent kept authenticating.
Governance (Ch11)	Owner / sponsor	No*	The sponsor seat was vacant when the credit was posted; the auditor sampled the credit three weeks later.
Governance (Ch11)	Evidence / retention	Partly*	Every internal hop reconstructs; the final posting is visible through the billing platform’s audit export, but the evidence is split across a trust boundary and assembling it takes work.
Governance (Ch11)	Regulatory mapping	Unknown*	Jurisdiction and applicability not established; for the legal department.

*Responses marked * are inferred from the book’s account; the book does not state them as checklist answers.*

Responsibility Matrix — the rule CrystalSoft adopted for cross-team delegation (Chapter 12)

The owner of the authority being exercised (Finance) sets its limits.

The owner of the requesting agent (Customer Operations) justifies the need.

IAM implements a grant both can see.

Widening the grant needs both.

In the matrix: Cross-team delegation — A† (the owner of the authority being exercised: Finance), R IAM, C AI engineering and secu
AI governance and risk

Table 15.2 — 12–24 Month Roadmap: Fields and a Worked Entry

Field	CrystalSoft example
Initiative / KAB	Narrow the Billing Resolution Agent’s CRM write scope to the task’s customer / ADAPT
Use case / risk driver	Billing resolution: injected content could steer writes to other customers (Ch10)
Prerequisite	CRM supports record-level scoping, or a gateway enforces it
Accountable owner	Head of Customer Operations (sponsor); IAM implements
Participating capabilities	Trust & Access; Authority & Delegation
Target outcome / evidence	Test showing a write to another customer’s record is denied; policy log
Technology maturity	Established (Chapter 9 legend, as of September 28, 2026)
Standard / technology dependency	CRM vendor capability
Timing window	NOW
Decision gate	Sponsor sign-off on the test result
Status / review date	Planned / next roadmap review

Figure 15.1 — The NOW / NEXT / THEN Capability Roadmap (CrystalSoft)

Capability lane	NOW — visibility and control	NEXT — adapt the IAM stack	THEN — build only what is needed
Identity and inventory	Inventory agents and delegated-access assistants; resolve Unknowns	Federated reconciliation and coverage reporting	Cross-domain registry and verification (BUILD)
Trust and access	Remove shared and long-lived credentials on high-risk paths	Task-scoped tokens; continuous authorization (ADAPT)	
Authority and delegation	Bound high-risk authority (task grants)	Actor and subject context beyond the gateway	Cascade revocation; end-to-end provenance (BUILD); SoD pilot (OPEN) — PULL FORWARD
Lifecycle, PAM and IGA	Name sponsors; privileged third-party credential in PAM	Lifecycle triggers (sponsor, tool, version); JIT	
Runtime assurance	Route denials and signals with identity context	Identity-aware signals joined to authority	Runtime Assurance as an operating capability — PULL FORWARD
Governance	High-risk policy and exception path	Approvals in the workflow; book metrics	
Enterprise integration	Decision rights for high-risk decisions	Responsibility matrix for all agents; retirement handoffs	

Capability logic, not calendar dates. Phases overlap; small organizations may run them together.

Table 16.2 — 90-Day Action Plan: Fields and a Worked Entry

Field	CrystalSoft example
Action	Replace the long-lived billing-platform credential with a shorter-lived or bound one
Purpose	Reduce the blast radius of credential theft (Ch10)
Owner	Finance platform team; IAM supports
Evidence / input	PAM record; vendor capability confirmation; Drift precedent
Output	New credential pattern in production; old credential revoked
Dependency	Billing-platform vendor support
Risk trigger	Third-party credential; long-lived; privileged
Status	In progress (vendor call held)
Confidence / coverage	Medium: vendor answer pending
Next decision	Accept the vendor’s option, or add compensating controls

Table 16.1 — Immediate Escalation Triggers

Trigger	Why it escalates	CrystalSoft, week one
Write or irreversible actions	Consequence cannot be undone (IMDA impact factor)	Payment-plan changes in the held release
Sensitive or regulated data	Exposure is hard to contain (IMDA; Ch10)	Customer account and billing data
External exposure or third-party credentials	Controls stop at the boundary (Ch9, Ch10)	Payments Agent’s credential at the billing platform
Delegated user authority	The agent acts as someone else (Ch7)	Billing Resolution Agent acting for staff
No accountable sponsor	Nobody can accept or refuse the risk (Ch8, Ch11)	Billing Resolution Agent since the role change
Long-lived privileged credentials	Theft gives durable access (Ch10)	The billing-platform credential again